ID: 321321
Cookbook: browseurl.jbs
Time: 20:43:15
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

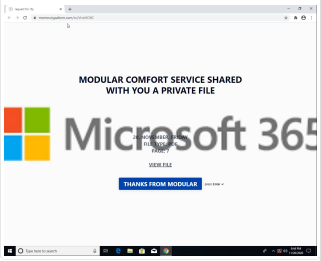
Analysis Report https://mcmms.typeform.com/to/Vtnb9…

Overview

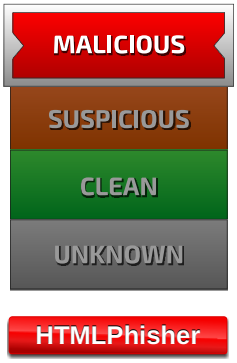
General Information

Sample URL:	http://https://mcmms.typeform.com/to/Vtnb9OBC
Analysis ID:	321321

Most interesting Screenshot:



Detection

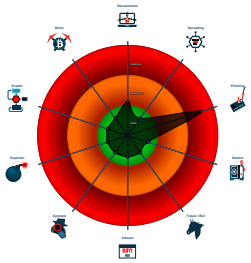


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid 'forgot password' link found
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5896 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://mcmms.typeform.com/to/Vtnb9OBC' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5564 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1620,15715787858784209187,1440343274009636210,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1808 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6068 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1620,15715787858784209187,1440343274009636210,131072 --lang=en-GB --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5040 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1284 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1620,15715787858784209187,1440343274009636210,131072 --lang=en-GB --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=6168 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

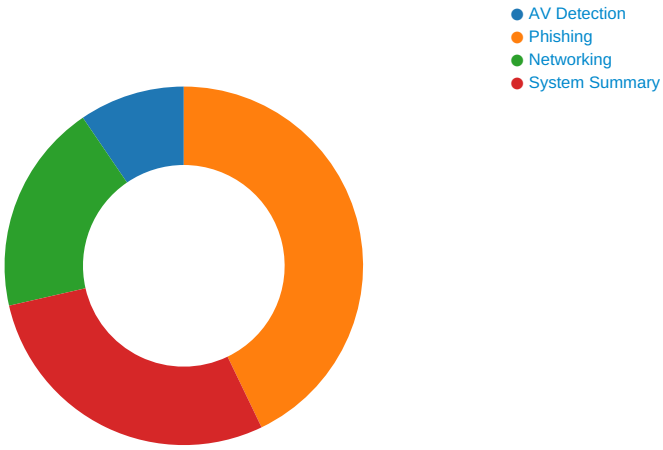
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright null 2020



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 favicon image match)

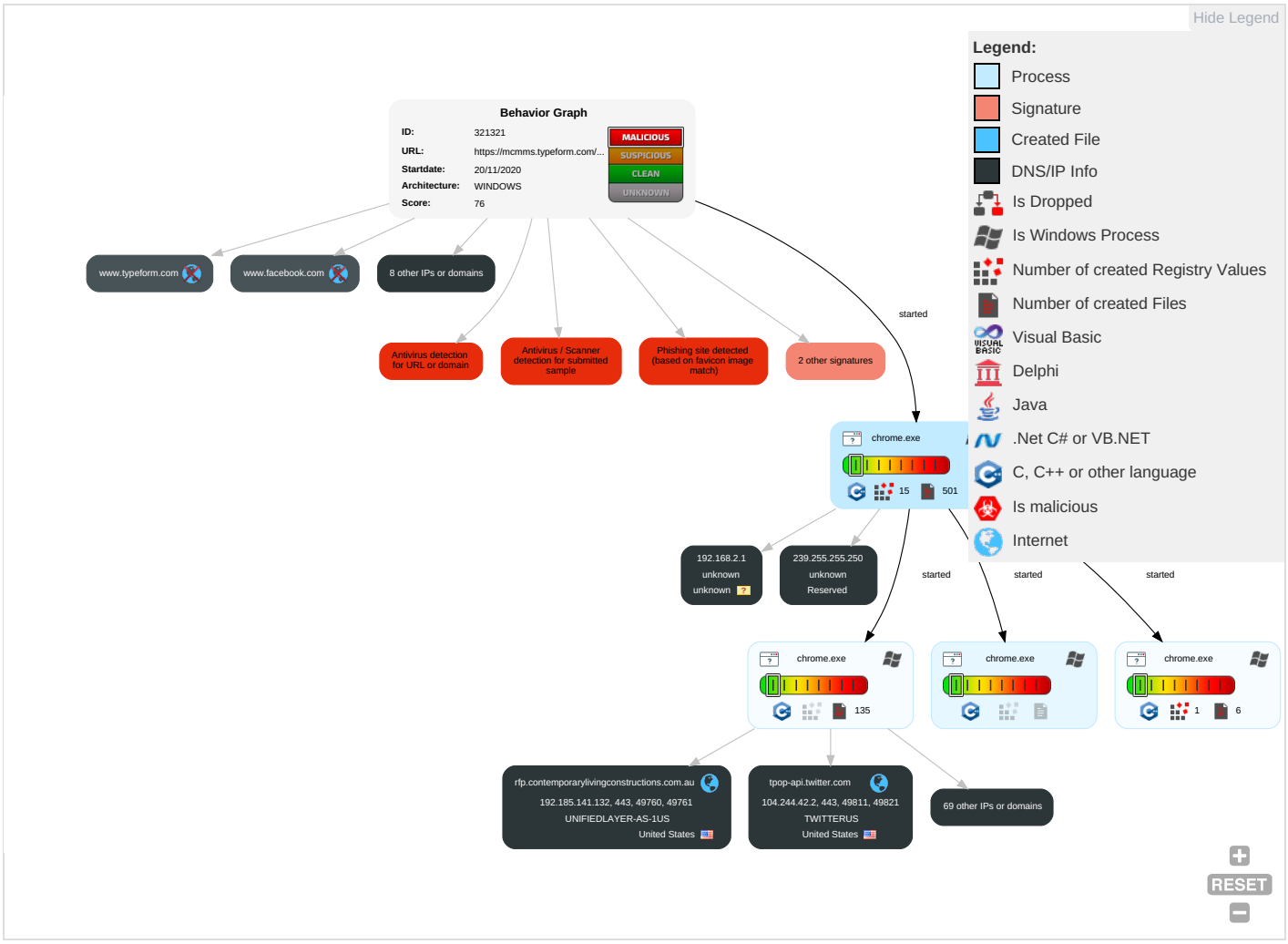
Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

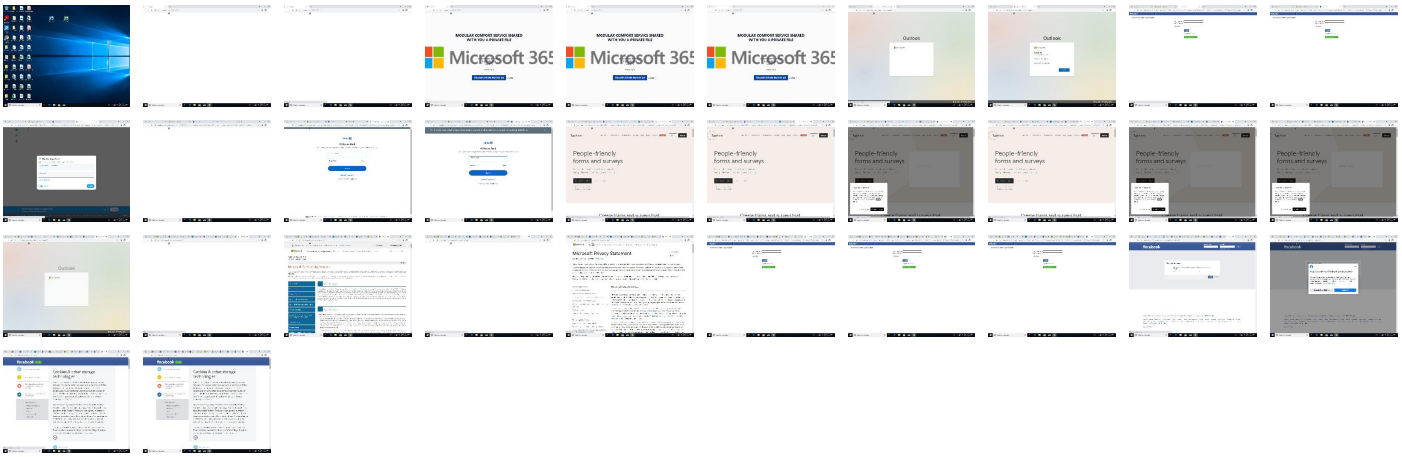
Behavior Graph

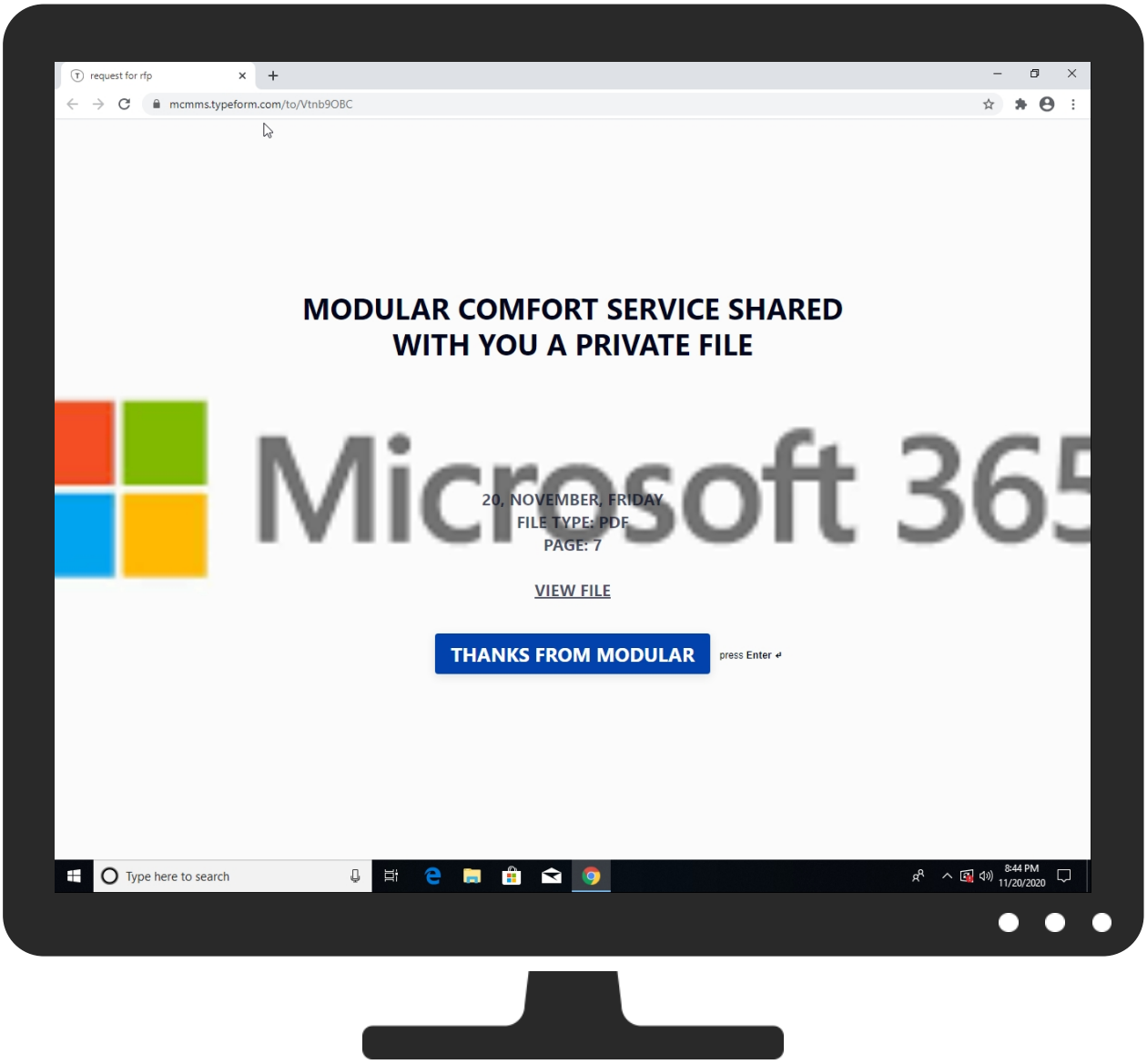


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://mcmms.typeform.com/to/Vtnb9OBC	0%	Virustotal		Browse
http://https://mcmms.typeform.com/to/Vtnb9OBC	0%	Avira URL Cloud	safe	
http://https://mcmms.typeform.com/to/Vtnb9OBC	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://rfp.contemporarylivingconstructions.com.au/ext/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://rfp.contemporarylivingconstructions.com.au/ext/#	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	54.170.224.115	true	false		high
d2citsn5wf4j9j.cloudfront.net	13.224.93.45	true	false		high
tpop-api.twitter.com	104.244.42.2	true	false		high
d296je7bbdd650.cloudfront.net	13.224.100.80	true	false		high
scontent.xx.fbcdn.net	157.240.9.23	true	false		high
t.co	104.244.42.5	true	false		high
twimg.twitter.map.fastly.net	151.101.12.159	true	false		unknown
pagead.l.doubleclick.net	216.58.207.34	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
d1l34lgko5ugnb.cloudfront.net	13.224.93.121	true	false		high
facebook.com	185.60.216.35	true	false		high
api.segment.io	52.38.212.85	true	false		high
polyfill.io	151.101.130.109	true	false		high
cs510.wpc.edgecastcdn.net	152.199.21.141	true	false		high
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
cs531.wpc.edgecastcdn.net	192.229.220.133	true	false		high
twitter.com	104.244.42.65	true	false		high
pagead46.l.doubleclick.net	172.217.22.34	true	false		high
s.twitter.com	104.244.42.67	true	false		high
p13nlog-1106815646.us-east-1.elb.amazonaws.com	34.200.62.85	true	false		high
z-m.c10r.facebook.com	185.60.216.36	true	false		high
dna8twue3dlxq.cloudfront.net	13.224.93.112	true	false		high
d3m6p8tvnbsibq.cloudfront.net	13.224.93.101	true	false		high
www.google.co.uk	172.217.21.195	true	false		unknown
d2nvsmtq2poimt.cloudfront.net	13.224.93.102	true	false		high
googlehosted.l.googleusercontent.com	172.217.16.193	true	false		high
cdn.cookielaw.org	104.16.149.64	true	false		high
geolocation.onetrust.com	104.20.185.68	true	false		high
rfp.contemporarylivingconstructions.com.au	192.185.141.132	true	false		unknown
abs.twimg.com	unknown	unknown	false		high
lnkd.demdex.net	unknown	unknown	false		high
mcmms.typeform.com	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
pixel.facebook.com	unknown	unknown	false		high
api.twitter.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
cdn.segment.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
renderer-assets.typeform.com	unknown	unknown	false		high
cm.g.doubleclick.net	unknown	unknown	false		high
video.twimg.com	unknown	unknown	false		high
platform.linkedin.com	unknown	unknown	false		high
www.typeform.com	unknown	unknown	false		high
dpm.demdex.net	unknown	unknown	false		high
logx.optimizely.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
pbs.twimg.com	unknown	unknown	false		high

Copyright null 2020

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.linkedin.com	unknown	unknown	false		high
static-exp3.licdn.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
images.typeform.com	unknown	unknown	false		high
public.profitwell.com	unknown	unknown	false		high
cdn3.optimizely.com	unknown	unknown	false		high
static.xx.fbcdn.net	unknown	unknown	false		high
analytics.twitter.com	unknown	unknown	false		high
cdn.optimizely.com	unknown	unknown	false		high
font.typeform.com	unknown	unknown	false		high
googleads.g.doubleclick.net	unknown	unknown	false		high
a15381830540.cdn.optimizely.com	unknown	unknown	false		high

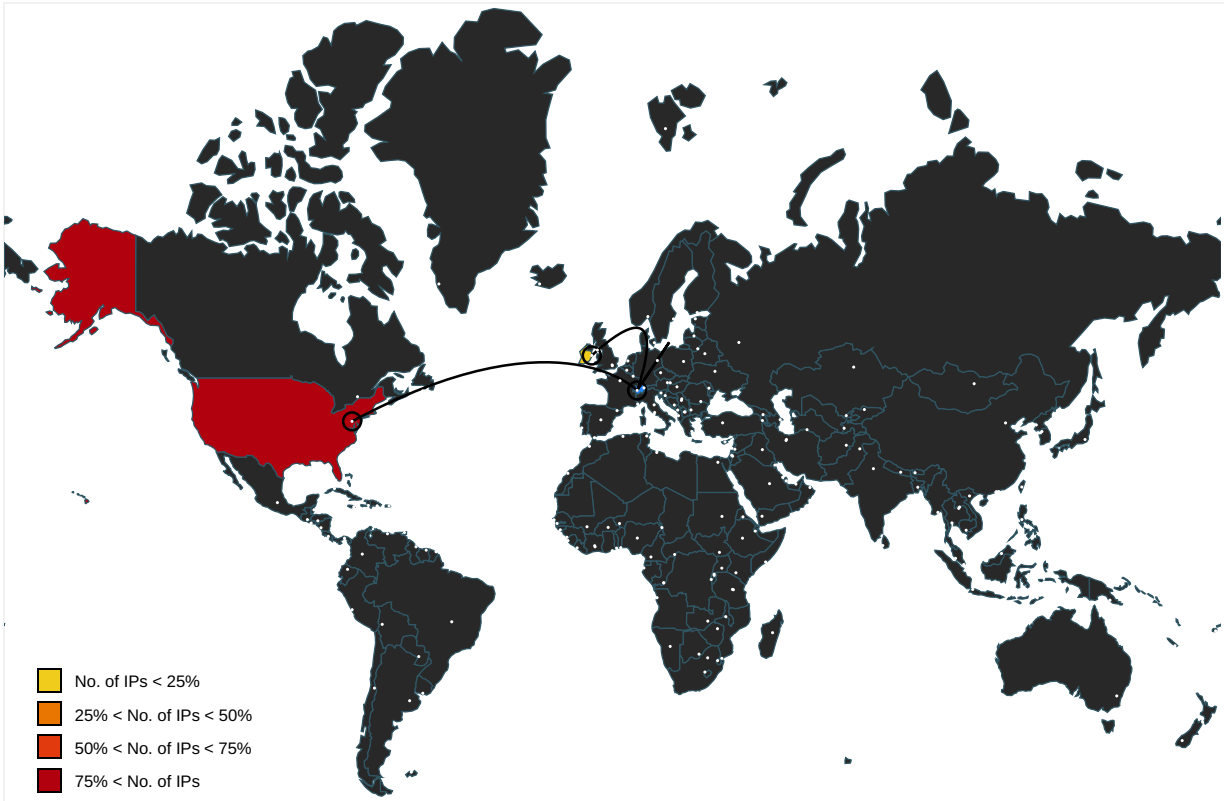
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://abs.twimg.com/responsive-web/client-web/bundle.AdvancedSearch.c0685f75.jsaD	32700fea768255f5_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.FollowerRequests.a85b5405.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.Compose.21b10db5.js.map	5881cbd28e52958c_0.0.dr	false		high
http://https://www.linkedin.com	Current Session.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.UserProfile.154d50c5.jsH	d737c2f83517d1c5_0.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.SettingsTransparency.25	f48d68dc1253f393_1.0.dr, f48d68dc1253f393_0.0.dr	false		high
http://https://support.twitter.com/articles/14606#receipts	34ad44d3f22af904_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.TimelineRenderer.2e4c7825.jsHP	7c3005f6423e7232_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Logout.c63c2d25.js(window.webpackJsonp=window	540335e5006c5433_0.0.dr	false		high
http://https://twitter.com/i/csp_report?a=O5RXE%3D%3D%3D&ro=falsecontent-type:application/javascript;	2cc80dabc69f58b6_0.0.dr	false		high
http://https://www.typeform.com/_next/static/chunks/6770615276bd5da6d0c72e0b9a6c4cc60237862a.23e7894a0300c9	7bfe9e92ce3f3ce1_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.NetworkInstrument.8cd49fb5.jsHP	739b423e13023e5d_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.SmsLogin.2d8ce2d5.jsHP	6741873163f0c1b8_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/sharedCore.f32fe095.jsH	8f92d6477bc30c3f_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.UserMoments.70821155.jsH	ea826d12a65360fe_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/main.79e68875.jsaD	6555571f4de54cf5_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.NotificationDetail.a425e5a5.jsHP	8c31666631e41fcf_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.ComposeScheduling.8cdd2145.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://upload.twitter.com	2cc80dabc69f58b6_0.0.dr, af47be93e4c33dc6_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/shared~bundle.Settings~bundle.SettingsRevamp~bundle.	2cc80dabc69f58b6_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/main.79e68875.js.map	6555571f4de54cf5_1.0.dr, 6555571f4de54cf5_0.0.dr	false		high
http://https://twitter.com/sw.js	000003.log8.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Logout.c63c2d25.jsaD	540335e5006c5433_1.0.dr	false		high
http://https://cards-frame.twitter.com/i/cards/tfw/v1/uc/	315be19845ca6d9d_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/loaders.video.PlayerUi.22f01e2	cdcf2f9caf44f736_1.0.dr, cdcf2f9caf44f736_0.0.dr	false		high
http://https://abs.twimg.com/a/1501527574/img/t1/icon_giphy.png	72a629a9b5d0115e_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/shared~bundle.LiveEvent~bundle	3f6e5ce3c019bb49_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.Topics.d01887a5.js.map	e6dc3e013a43df3c_1.0.dr, e6dc3e013a43df3c_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.SettingsTransparency.25b86025.jsHP	f48d68dc1253f393_0.0.dr	false		high
http://https://t.co/livevideobrowsers	cdcf2f9caf44f736_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-fa.271570a5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.NewsLanding.b7ef3685.jsaD	4e7da4b4942f1dfe_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.UserFollowLists.cca7f4d5.jsaD	1fd589a43e1b46b0_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.MultiAccount.c9d1a0d5.js	2cc80dabc69f58b6_1.0.dr, 0d8674449530216b_1.0.dr	false		high
http://https://www.typeform.com/_next/static/chunks/webpack-eb080e3f091731f228fb.jsaD	7d748ba4e1f95dcd_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.ConversationParticipants.7fec5625.jsH	0371dbd3e818f1f8_0.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.RichTextCompose.3798576	4f6f79ac303317f5_1.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/rollbar.js/2.4.6/rollbar.min.jsaD	3dd0c8e84c33e5ab_0.0.dr	false		high
http://https://cm.g.doubleclick.net/pixel?google_nid=twitter_dbm&google_redir=https://analytics.twitter.com	6555571f4de54cf5_1.0.dr	false		high
http://https://pbs.twimg.com/lex/placeholder_live_nomargin.png	315be19845ca6d9d_1.0.dr	false		high
http://https://npms.io/search?q=ponyfill.	5bfbb46374541e45_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.AudioOnlyVideoPlayer.7ea70755.js	05c1a55dbd54a88d_1.0.dr, 2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.DMDrawer.5b7711a5.jsH	9cb49c311c61d0ad_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3i9Zn4/yn/l/en_GB/anMEAxuISXI.js?_nc_x=Ij3Wp8lg5Kza	1a3eaa7325c8d467_0.0.dr	false		high
http://https://www.hud.gov	d7c11a70674843f7_0.0.dr	false		high
http://https://help.twitter.com/using-twitter/twitter-videos	34ad44d3f22af904_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.MomentMaker.17607ec5.jsHP	5bfbb46374541e45_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.UserMoments.70821155.js	ea826d12a65360fe_1.0.dr, 2cc80dabc69f58b6_1.0.dr	false		high
http://https://twitter.app.link/interstitial_switch_to_app	5bfbb46374541e45_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/icon-svg.9e211f65.svg	af47be93e4c33dc6_0.0.dr	false		high
http://https://twitter.com/home?lang=ca	af47be93e4c33dc6_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.Dropdown.9ec1da45.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://typeform.com/9	5af3e76addb24ee8_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3ijDN4/y-/l/en_GB/_g9V36AHQKV.js?_nc_x=Ij3Wp8lg5Kza	d2f8205d72348c98_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.HoverCard.a0be1c75.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.LiveEvent.2790a865.jsHP	5ba1880186935502_0.0.dr	false		high
http://https://twitter.com/home?lang=cs	af47be93e4c33dc6_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.GenericTimeline.cd7813b5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Topics.d01887a5.js	e6dc3e013a43df3c_1.0.dr, 2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-it.41cbf8e5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/loaders.video.VideoPlayerDefau	4639d15059ef86cd_1.0.dr	false		high
http://https://vmapstage.snappytv.com	2cc80dabc69f58b6_0.0.dr, af47be93e4c33dc6_0.0.dr	false		high
http://https://support.twitter.com/articles/14606#receive	34ad44d3f22af904_1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.TopicPeek.1844ba15.js.m	73ce858764985ae6_1.0.dr	false		high
http://https://twitter.com/home?lang=de	af47be93e4c33dc6_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-bg.905c7245.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs-0.twimg.com/emoji/v2	6555571f4de54cf5_1.0.dr	false		high
http://https://twitter.com/home?lang=da	af47be93e4c33dc6_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.HWCard.4a95ba45.jsHP	315be19845ca6d9d_0.0.dr	false		high
http://https://abs.twimg.com/sticky/default_profile_images/default_profile_normal.png	6555571f4de54cf5_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Search.e76909c5.jsHP	ded311c97ce87860_0.0.dr	false		high
http://https://www.typeform.com/_next/static/chunks/05d954cf.01e8d901e2813d632096.jsaD	8e45b4e4dc728c42_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3i8jc4/yA/l/en_GB/2596_8UTwmn.js?_nc_x=Ij3Wp8lg5Kz	6a2cf1a3d566dd90_0.0.dr	false		high
http://https://www.typeform.com/_next/static/chunks/pages/front-page-004159675a09fbf6e6f4.js	2e7da6200e9bb853_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.ProfileClusterFollow.13222285.jsHP	1d233998e0468f4e_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.UserProfile.154d50c5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.LottieWeb.f4c2aa65.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://mcmms.typeform.com/to/Vtnb9OBCugN0	History-journal.0.dr	false		high
http://https://twitter.com/intent/tweet?url=https%3A%2F%2Fmcmms.typeform.com%2Fto%2FVtnb9OBC%3Ftypeform-ty-	History-journal.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yV/r/cKYG5jgbj2D.js?_nc_x=Ij3Wp8lg5Kz	3bbba9d520641b16_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.FleetMediaDetail.0c6c1df5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Twitterversary.b7212275.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://twitter.com/home?lang=ar	af47be93e4c33dc6_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.DirectMessages.92439335.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://twitter.com/home?lang=bg	af47be93e4c33dc6_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.directMessagesData.73873bc5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.kn.67f5cee5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.MomentMaker.17607ec5.js	5bfbb46374541e45_1.0.dr, 5bfbb46374541e45_0.0.dr	false		high
http://https://help.twitter.com/rules-and-policies/twitter-cookies	28f3f34d076e157c_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.TweetMediaTags.2f63fe95.jsH	287f94cc816febd6_0.0.dr	false		high
http://https://renderer-assets.typeform.com/modern-renderer.1dc96dfb1da55c4cfd25.js	1ded97f6a28d5a09_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.TweetActivity.6a2de005.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Logout.c63c2d25.js	2cc80dabc69f58b6_1.0.dr, 540335e5006c5433_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.TweetActivity.6a2de005.js(window.webpackJsonp	0c7af041f708eb18_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.SettingsRevamp.fd97dd85.jsH	9ad92f9a160a0939_0.0.dr	false		high
http://https://twitter.com/home?lang=bn	af47be93e4c33dc6_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.CarouselScroller.ff07de85.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://www.linkedin.com/	Network Action Predictor-journal.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.ConnectTab.e9081845.js.	12d09362c945a7f3_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.SettingsProfile.a972cdb5.jsHP	739b193de0c3170b_0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.38.212.85	unknown	United States		16509	AMAZON-02US	false
13.224.93.45	unknown	United States		16509	AMAZON-02US	false
192.185.141.132	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
54.170.224.115	unknown	United States		16509	AMAZON-02US	false
13.224.100.80	unknown	United States		16509	AMAZON-02US	false
151.101.130.109	unknown	United States		54113	FASTLYUS	false
185.60.216.35	unknown	Ireland		32934	FACEBOOKUS	false
13.224.93.101	unknown	United States		16509	AMAZON-02US	false
185.60.216.36	unknown	Ireland		32934	FACEBOOKUS	false
13.224.93.102	unknown	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
13.224.93.56	unknown	United States		16509	AMAZON-02US	false
151.101.12.159	unknown	United States		54113	FASTLYUS	false
172.217.21.195	unknown	United States		15169	GOOGLEUS	false
52.48.66.74	unknown	United States		16509	AMAZON-02US	false
172.217.16.193	unknown	United States		15169	GOOGLEUS	false
152.199.23.37	unknown	United States		15133	EDGECASTUS	false
216.58.206.2	unknown	United States		15169	GOOGLEUS	false
34.200.62.85	unknown	United States		14618	AMAZON-AESUS	false
13.224.93.112	unknown	United States		16509	AMAZON-02US	false
152.199.21.141	unknown	United States		15133	EDGECASTUS	false
104.244.42.65	unknown	United States		13414	TWITTERUS	false
104.244.42.2	unknown	United States		13414	TWITTERUS	false
157.240.9.23	unknown	United States		32934	FACEBOOKUS	false
192.229.220.133	unknown	United States		15133	EDGECASTUS	false
104.244.42.67	unknown	United States		13414	TWITTERUS	false
13.224.93.121	unknown	United States		16509	AMAZON-02US	false
216.58.207.34	unknown	United States		15169	GOOGLEUS	false
104.244.42.5	unknown	United States		13414	TWITTERUS	false
104.16.149.64	unknown	United States		13335	CLOUDFLARENETUS	false
104.20.185.68	unknown	United States		13335	CLOUDFLARENETUS	false
172.217.22.34	unknown	United States		15169	GOOGLEUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

Copyright null 2020

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321321
Start date:	20.11.2020
Start time:	20:43:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://mcmms.typeform.com/to/Vtnb9OBC
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:	6
Number of new started drivers analysed:	1
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:	mal76.phis.win@51/561@48/35

Copyright null 2020

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://rfp.contemporarylivingconstructions.com.au/ext • Browse: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fmcmms.typeform.com%2Fto%2FVtnb9OBC%3Ftypeform-ty-screen-ref%3D23ae5f9c-adf7-4d52-808b-5b05db18e22a • Browse: https://twitter.com/intent/tweet?url=https%3A%2F%2Fmcmms.typeform.com%2Fto%2FVtnb9OBC%3Ftypeform-ty-screen-ref%3D23ae5f9c-adf7-4d52-808b-5b05db18e22a • Browse: https://www.linkedin.com/shareArticle?url=https%3A%2F%2Fmcmms.typeform.com%2Fto%2FVtnb9OBC%3Ftypeform-ty-screen-ref%3D23ae5f9c-adf7-4d52-808b-5b05db18e22a • Browse: https://www.typeform.com?utm_campaign=Vtnb9OBC&utm_source=typeform.com-17223155-Premium&utm_medium=typeform&utm_content=typeform-thankyou&utm_term=EN • Browse: https://www.typeform.com?utm_campaign=Vtnb9OBC&utm_source=typeform.com-17223155-Premium&utm_medium=typeform&utm_content=typeform-footer&utm_term=EN • Browse: https://rfp.contemporarylivingconstructions.com.au/ext/# • Browse: https://www.microsoft.com/en-US/servicesagreement/ • Browse: https://privacy.microsoft.com/en-US/privacystatement • Browse: https://www.facebook.com/login.php?skip_api_login=1&api_key=966242223397117&signed_next=1&next=https%3A%2F%2Fwww.facebook.com%2Fsharer%2Fsharer.php%3Fu%3Dhttps%253A%252F%252Fmcmms.typeform.com%252Fto%252FVtnb9OBC%253Ftypeform-ty-screen-ref%253D23ae5f9c-adf7-4d52-808b-5b05db18e22a&cancel_url=https%3A%2F%2Fwww.facebook.com%2Fdialog%2Fclose_window%2F%3Fapp_id%3D966242223397117%26connect%3D0%23_%3D_&display=popup&locale=en_G/reg/?app_id=0&logger_id • Browse: https://www.facebook.com/login.php?skip_api_login=1&api_key=966242223397117&signed_next=1&next=https%3A%2F%2Fwww.facebook.com%2Fsharer%2Fsharer.php%3Fu%3Dhttps%253A%252F%252Fmcmms.typeform.com%252Fto%252FVtnb9OBC%253Ftypeform-ty-screen-ref%253D23ae5f9c-adf7-4d52-808b-5b05db18e22a&cancel_url=https%3A%2F%2Fwww.facebook.com%2Fdialog%2Fclose_window%2F%3Fapp_id%3D966242223397117%26connect%3D0%23_%3D_&display=popup&locale=en_G/# • Browse: https://www.facebook.com/recover/initiate/?ars=facebook_login • Browse: https://www.facebook.com/policies/cookies/
Warnings:	Show All • Exclude process from analysis (whitelisted): qwavedrv.sys, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.147.198.201, 172.217.18.13, 172.217.16.142, 104.18.26.71, 104.18.27.71, 216.58.206.14, 173.194.182.74, 216.58.212.163, 172.217.18.106, 172.217.22.74, 172.217.21.234, 216.58.205.234, 172.217.23.138, 172.217.21.202, 172.217.18.10, 172.217.18.170, 216.58.207.42, 216.58.207.74, 216.58.206.10, 172.217.16.170, 216.58.208.42, 216.58.210.10, 172.217.23.106, 172.217.22.42, 209.197.3.24, 8.241.9.126, 8.241.122.126, 8.241.9.254, 8.253.204.120, 8.241.121.254, 172.217.23.142, 13.107.42.14, 13.107.246.10, 92.122.213.192, 92.122.213.242,

66.102.1.127, 2.20.85.30, 172.217.23.168, 23.37.32.235, 2.17.191.240, 216.58.208.36, 92.122.145.53, 152.199.19.160, 92.122.213.194, 92.122.213.240, 2.18.70.63, 92.122.213.247, 92.122.213.200, 92.122.213.219, 104.108.38.107, 172.217.16.131, 172.217.18.99, 173.194.187.39, 173.194.187.231

- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, r2---sn-4g5e6nsd.gvt1.com, assets.onestore.ms.edgekey.net, clientservices.googleapis.com, i.s-microsoft.com.edgekey.net, a1945.g2.akamai.net, l-0005.l-msedge.net, www.microsoft.com-c-3.edgekey.net, clients2.google.com, random.typeform.com.cdn.cloudflare.net, audownload.windowsupdate.nsatc.net, update.googleapis.com, standard.t-0001.t-msedge.net, www.google.com, statics-marketingsites-eus-ms-com.akamaized.net, watson.telemetry.microsoft.com, www.gstatic.com, li-prod-static.azureedge.net, au-bg-shim.trafficmanager.net, a1778.g2.akamai.net, r2.sn-4g5ednly.gvt1.com, www.google-analytics.com, e10583.dspg.akamaiedge.net, r2---sn-4g5ednly.gvt1.com, content-autofill.googleapis.com, aadcdnoriginneu.azureedge.net, e4343.x.akamaiedge.net, statics-marketingsites-wcus-ms-com.akamaized.net, www.googleapis.com, t-0001.t-msedge.net, od.linkedin.edgesuite.net, assets.onestore.ms.akadns.net, skypedataprdcolcus15.cloudapp.net, c-s.cms.ms.akadns.net, umwatsonrouting.trafficmanager.net, 2-01-2c3e-0055.cdx.cedexis.net, blobcollector.events.data.trafficmanager.net, li-prod-static.afd.azureedge.net, c.s-microsoft.com-c.edgekey.net, clients.l.google.com, privacy.microsoft.com.edgekey.net, r5---sn-4g5e6ns7.gvt1.com, stun.l.google.com, a1916.dscg2.akamai.net, www.googleadservices.com, afd.t-0001.t-msedge.net, i.s-microsoft.com, a1449.dscg2.akamai.net, e5048.dsca.akamaiedge.net, 2-01-2c3e-0069.cdx.cedexis.net, e6640.x.akamaiedge.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, cdn.optimizely.com.edgekey.net, mscomajax.vo.msecnd.net, redirector.gvt1.com, www.googletagmanager.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, r2.sn-4g5e6nsd.gvt1.com, www-linkedin-com.l-0005.l-msedge.net, accounts.google.com, www-google-analytics.l.google.com, cs22.wpc.v0cdn.net, www-googletagmanager.l.google.com, ctldl.windowsupdate.com, wildcard.cdn.optimizely.com.edgekey.net, Edge-Prod-FRAr3.ctrl.t-0001.t-msedge.net, r5.sn-4g5e6ns7.gvt1.com, aadcdnoriginneu.ec.azureedge.net, skypedataprdcoleus16.cloudapp.net, cs2-wpc.apr-8315.edgecastdns.net, c.s-microsoft.com, privacy.microsoft.com, e13678.dscg.akamaiedge.net, cdn.o6.edgekey.net, www.microsoft.com, e13678.dspb.akamaiedge.net, wcpstatic.microsoft.com
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Copyright null 2020

Simulations

Behavior and APIs

Time	Type	Description
20:44:14	API Interceptor	2x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	117872
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	1536:i/LAvEZrGclx0hoW6qCLdNz2p+/LAvEZrGclx0hoW6qCLdNz2pj:UcMqZVCp8pwcMqZVCp8pj
MD5:	DB381E85D86EA4484D20078E9EC667A6
SHA1:	4871FDAF0C2EEC8183FC3CE7710B18FD3C647CEA
SHA-256:	C3520E3A6EB43F6D416852C454414C5D7823A96FB9070BC30301ADDEBB334D4D
SHA-512:	D9E03A617D1D9505D3ADA3C41FC8A53504F4F1C44F92AF00869F2FE150D6677FD4450E85EB1E3D920D32BA01F190E7F14BF130F8CC69EB47D834CCE43CAA765 0
Malicious:	false
Reputation:	low
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,IH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1170916134078785

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Encrypted:	false
SSDEEP:	12:AkPlE99SNxAhUegeTMkPlE99SNxAhUegeT2:AkPcUQU76MkPcUQU762
MD5:	9D01D3687E66C29B6E6EBBB35E4D6E70
SHA1:	228A9F38596CD9D957A5ACE53ED57FD4FA1AC066
SHA-256:	9E3FBA815F63475F8949934D95E2981D1B9FEFFA4FFD7DA92BC9191D80789A6B
SHA-512:	889E7C6BF985CA6BEEDEF1C7E79B304EDB360A35CA136F2D814E913CF3C053C63110103E7657FFD897F2AA4BD87AB082461D97E1CAEC240F22A67BAEB55FB5E5
Malicious:	false
Reputation:	low
Preview:	p..... .....u...(..... .....Y.....$.....8...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...p..... .....\..u...(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0248b757-b876-429b-bed8-d38a0cd22d2a.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):	162578
Entropy (8bit):	6.082636147830395
Encrypted:	false
SSDEEP:	3072:OAEcxY0CaMAdT5OErBbyd3rFcbXafIB0u1GOJmA3iuR5:dJMcxrB+3JaqfIlUOoSiuR5
MD5:	F6EFABFCC0DDC17746C8B6567B11E186
SHA1:	48CEFB3D1FC8F80CEC974AE3B334C06F2D45F29A
SHA-256:	8E1F1A8B7A6AB8958DFA8391A161E7081D18239CFFDE6FB5273FDDC1A7D51C15
SHA-512:	1503533B580BF8187B83723DAF84C317778ABC6EE4D8A9432778C88ECB0B257A6A25B81E95ED0A49A8CE5C09508C21330B9B796691D9FCDD67656EB9773C5F8
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.605901444612482e+12,"network":1.605901446e+12,"ticks":304038233.0,"uncertainty":4293512.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBljSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\0646ab7f-77c6-4419-90dd-e17005e04c5c.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):	162827
Entropy (8bit):	6.082905262533925
Encrypted:	false
SSDEEP:	3072:SdcxY0CaMAdT5OErBbyd3rFcbXafIB0u1GOJmA3iuR5:FMcxrB+3JaqfIlUOoSiuR5
MD5:	B810E4A13216E7D2C3D62A05C27BB70D
SHA1:	35EA3FCCCE6CDE0AE66B500B00BDBC883355FB1A
SHA-256:	06D57CFA3AD9DA44A9D0EF404F8467C4D93C6F500C916B1DA23EE81CD8DC3D35
SHA-512:	9605E95AE4D273F37D75FE3C0A2E1A6B54A00DD7E48E38F65246DB54002C7C8832384480B4B25DBD7417F01B8C7D418C1A9CBE3EDB104F8DC131FACC485ED59
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.605901444612482e+12,"network":1.605901446e+12,"ticks":304038233.0,"uncertainty":4293512.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBljSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715758802"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\502be2ef-baa7-42a2-82c3-43effd57a0e6.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):	162578
Entropy (8bit):	6.082637113341052
Encrypted:	false
SSDEEP:	3072:OizcxY0CaMAdT5OErBbyd3rFcbXafIB0u1GOJmA3iuR5:HGMcxrB+3JaqfIlUOoSiuR5
MD5:	9FCC55C158A7888702B317DC8F095508

C:\Users\user\AppData\Local\Google\Chrome\User Data\502be2ef-baa7-42a2-82c3-43effd57a0e6.tmp	
SHA1:	3365066FEDD97E6B34595A129EA8F1730E8110D7
SHA-256:	AB45664B1D2044590E67F62288D4EB3F2325E03803B63B5D5CF95C0F40F565BE
SHA-512:	BBF954E766B49F1D5A101B32D7134ABCBB892F182561F0F43A01CB0595E5E2EBA8D2705A6B75B61D697155CCEDE4814AD4A5522A1380397A4B2930F7DB008B6
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.605901444612482e+12,"network":1.605901446e+12,"ticks":304038233.0,"uncertainty":4293512.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBljSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\64045fb5-032a-4237-832e-00f2fbedbc59.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):	162580
Entropy (8bit):	6.082635747826904
Encrypted:	false
SSDEEP:	3072:SV+cxY0CaMAdT5OErBbyd3rFcbXafIB0u1GOJmA3iuR5:gzMcxrB+3JaqfIlUOoSiuR5
MD5:	6A48EDA8322CE6C3089A12DAFFB9DAA4
SHA1:	A27598D3BD1BECACB9F5359817F9B42BF95349B7
SHA-256:	E8B696C5407231FC40AA3AAEC54A24164C72259FBFA5BF70057D813B728DD8D5
SHA-512:	16248A64E4AFA0D11C1DDAABC2521788A56511766B5B24B77001359314B206D534F06CCE22C09E0BEC8183A7B6534C116CA57B1F0BBA7472CB5267D20882D16
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.605901444612482e+12,"network":1.605901446e+12,"ticks":304038233.0,"uncertainty":4293512.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBljSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715758802"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\73b5a3b7-496a-4fa4-ad69-0f8df923e8da.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):	162578
Entropy (8bit):	6.082635556897755
Encrypted:	false
SSDEEP:	3072:ORKcxY0CaMAdT5OErBbyd3rFcbXafIB0u1GOJmA3iuR5:MHMcxrB+3JaqfIlUOoSiuR5
MD5:	51E4502040E712927C79331351E751B9
SHA1:	163C4C116B3C253E25DA76D4B93E73C7EA206A32
SHA-256:	E4319A67D84E58617CB8A975332BDDE82166B4F48B1799C03DD30ACA0A7A9C7B
SHA-512:	685CC66FC1C1B244E0E05DD93FBCBB7638130DCB2FF887A441AC0305D2F67394B71573D0F948727667B0113F4E3E0097D35489C7C8EC7DF3476C231289F79B31
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.605901444612482e+12,"network":1.605901446e+12,"ticks":304038233.0,"uncertainty":4293512.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBljSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\86380d6c-40f3-4e2c-a88b-69d1162d0bad.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97400
Entropy (8bit):	3.7515286066566533
Encrypted:	false
SSDEEP:	384:QbkLzxOQ2WaBtVawXSNXrUvDp3kjBQHJgG43ridn5IxUddZcrm7mmyMep3XvwO9I:QeKF9qa8Y0erCd9NoHHO5KbJnxZ
MD5:	0F5E652AC0FAA649DD1E23A39AD16CF5
SHA1:	E2571CD890F9245C356F146392513A73AB186356

C:\Users\user\AppData\Local\Google\Chrome\User Data\86380d6c-40f3-4e2c-a88b-69d1162d0bad.tmp	
SHA-256:	F3DAE5CA65A2111B2C9100469C7C3A578F981E145C816216AF26ECE4C3C13073
SHA-512:	45B891FA8BE7726D5DD3B5DC11A47CA728C6C338DCC445BEC802FAF48065E110CC6F73C5E61BF5D5777771186DC65C7B8ED0F6828442E0DDEB0EA5E38FB89C7
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....)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\8751e8da-f7d2-44c5-ae46-2d2e2309d3e0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.751240075094978
Encrypted:	false
SSDEEP:	384:zbkLzxOQRBWXSNXrUvDp3kjBQHJgG43ridnjxUddZcrm7mmxep3XvwO9F/Nq1vu8:kKF9qtgY0erL9NoHHO5KbJnxu
MD5:	888026EDC35E40FD8E69E0FB644FC835
SHA1:	E61A6D9FD5FE70C945925ED6834BE4E4A6A4FEF3
SHA-256:	2141CAA4AE920739B3C0D78BEAAFEA5FDE54B1993D84E313F2E788B01308C6E9
SHA-512:	6066F2A54519D0871940AF6F731A522891B48BA3650EE405BFEF3A07BAB95680B10A9734EC3B9B2D96534F9354DA32C904544289797599E3B62E425B23A94C14
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\075dcf19-468a-41a6-8a06-45acda3db12f.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):	3289
Entropy (8bit):	5.60438862952317
Encrypted:	false
SSDEEP:	96:ynAB9+UPApU4U6LUiUUMUijyUwUMHKUztU2FUzPeU3UlUYPUg:yAB9+U4pU4U6LUiUUMUiuUwUMHKU5U2/
MD5:	3A3E3C9440874D1EEB237E25CDA0AE64
SHA1:	041E299EC2EC52EE13284DA0AC3C344E26D640C5
SHA-256:	B8A1545F713C15E5B0324537B4DC30E2C795E96CEF26B04CFA36BBF810178A80
SHA-512:	37610A4C5CCA6EDCBDE41748B69263E0DA13E4DE872B75A4A01522B2B4B1503E3F8AF1CE4459C547F498DDA578B79FEE18163CD1117BFD92061D158790EFC08
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\075dcf19-468a-41a6-8a06-45acda3db12f.tmp	
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606506246.817275,"expect_ct_observed":1605901446.817275,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"C5WXbCbt8ZLknJCMf0NV3mm3YVI5dFowQPyp/v9YT50=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606506254.441877,"expect_ct_observed":1605901454.441877,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1605987868.908853,"expect_ct_observed":1605901468.908853,"expect_ct_report_uri":"https://www.linkedin.com/platform-telemetry/ct","host":"tXjOdUMSBgtiUbrbGkl6XP80fiDB8uXOkUbnCf0IKvw=","nik":[]}],"sts":[{"expiry":1637437468.048637,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1605901468.048641},{"expiry":1637437446.817263,"host":"C5WXbCbt8ZLknJCMf0NV3mm3YVI5dFowQ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1440492b-7a13-4caa-a284-83c9c480ab0e.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):	6320
Entropy (8bit):	4.846999525273772
Encrypted:	false
SSDEEP:	192:JzMKxDHGXCOTGH6Uyu/6a0K6W0YLq0G672aRJ6Oe+v6NG+DiEfbBq79iKRnhaFTa:JoKx7GXCOTGH6Uy26a0K6W0YLq0G672q
MD5:	EF3A365C16EAC00174B51FE8155B7193
SHA1:	CCC9FCAB1A26AEC9E5FAAE71A7C27C9D362BEEC2
SHA-256:	81B993391FECD754E5543302E57A98F008CCB214A8BFF03F1C28CCB172776CE3
SHA-512:	0E308E8E1231D7F4932ACE0410879B5F78039744AE37B9906136D056C1A4EBC8E023EF6FEAF77457FE679B868F46401F65D9F96045A878E415AFF5700AEB16C1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://renderer-assets.typeform.com","supports_spdy":true},{"isolation":[],"server":"https://images.typeform.com","supports_spdy":true},{"isolation":[],"server":"https://cdn.segment.com","supports_spdy":true},{"isolation":[],"server":"https://mcmms.typeform.com","su

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\24cae674-2c6c-431f-a4bd-18e1b2b0757d.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):	1876
Entropy (8bit):	5.589417353505067
Encrypted:	false
SSDEEP:	48:Y1PnAjZHt6ezApUM4VwUA6UUhyKUeiYqPeUekUe7BwUYPUeP:ynABRApU4UpUUgKUzHPeU3UlUYPUg
MD5:	DB7E637E1B16409421AAFBC14BBB0F81
SHA1:	9289BA503E9E3B1DDB930A0932D00C48847D45FE
SHA-256:	69ABE81D3E55A811AC7CCFF4A58F7492A0677E59B87BA9B40D124C269539E6F6
SHA-512:	C6296BED8A4136D42291B89348AF4F95E8965886893A655A5D8BE1C7B5CCEB744446D9145EA262B6ECF0D409A137B83261719BA5956191D817C44B16DBD32F3E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606506246.817275,"expect_ct_observed":1605901446.817275,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"C5WXbCbt8ZLknJCMf0NV3mm3YVI5dFowQPyp/v9YT50=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606506254.441877,"expect_ct_observed":1605901454.441877,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","nik":[]}],"sts":[{"expiry":1637437446.817263,"host":"C5WXbCbt8ZLknJCMf0NV3mm3YVI5dFowQPyp/v9YT50=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1605901446.817268},{"expiry":1621681454.441867,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1605901454.441871},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbl1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\73747b13-728e-4195-b928-c8b25a5e518e.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):	5796
Entropy (8bit):	5.603694644373638
Encrypted:	false
SSDEEP:	96:ynA58TXH9UcUHApUIU/LUasieUSUUMKUIzUr3UTUDyUB+UtUoUMdeUpKUzXTUFyd:yA58TXH9UcUgpUIU/LUacUSUUMKUIzU7
MD5:	1B4227ED9B9B36621A2DC99877048DFB
SHA1:	C813AD2925DD4CA75F681FB253827D0B12837CE3
SHA-256:	A3BA0D998F08FFD9367ADB1A10CA52FFDB548163EC12F5D3041B055B5E64C3B4
SHA-512:	405F04C60C1B0A4971F670AEF148BEC70126F368CD0390BFA611B176E23BFAD0C17DCD776951D82815FF601EDA259A7586DE5B2651126D67E522723C892DE856
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\73747b13-728e-4195-b928-c8b25a5e518e.tmp

Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606506246.817275,"expect_ct_observed":1605901446.817275,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"C5WXbCbt8ZLknJCMf0NV3mm3YVI5dFowQPyp/v9YT50=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606506271.566746,"expect_ct_observed":1605901471.566746,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606506278.001758,"expect_ct_observed":1605901478.001758,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"Q2i8+5A3kREMoy37yPuUYKheqKsz3RQ2ENTog6mvPhc=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606506275.422295,"expect_ct_observed":1605901475.422295,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"eMIhdBIeGO0Ugn/hljmbZogTnAA6ZNUajhwz+o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7922196f-0b2e-474a-a708-7ff61bcc51bf.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):	5930
Entropy (8bit):	5.175845636838051
Encrypted:	false
SSDEEP:	96:nBLRw4RIV15k0JCKL8UkG1tYk/IjwbOTlVuHn:nBa4RIjh4KbkG7YkA8
MD5:	E0154DC00A9BBFE0F187C3AF480FCC18
SHA1:	D2AC019BF6C7DA2AD20452D9B981446625453D71
SHA-256:	EB5387F4BD8FDDE44B4707195F81858F62EBF404456E9ED0CD3FD182FF272FF1
SHA-512:	F627AFB19F6AFF829AFBEFAB89457210D50DDECFC424BDB9476937BB00247FF013BCB9A85B191E413E9126A972BB2FE607AC39D4C98BFBC66E8E47260720847 2
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250375042011539","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\79a39a8e-4c26-4fc6-b3ad-9a44d26a3713.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):	5671
Entropy (8bit):	5.167166675432051
Encrypted:	false
SSDEEP:	48:YcLkMkliQMqAcMRqB5gPOW4lYGlQuoTw0hcrf4MqM8C1Nfct/9BhUJo3KhmeSnpk:nBqRw4RIV05k0JCKL8UkG1vbOTlVuHn
MD5:	A0A3603FD5ACB9F23B7D36B8485A46D5
SHA1:	FC8CEDF81EEF25543A45662EA3C1F2C06E507C3F
SHA-256:	175B9DD65C1BA9AD02176B9995C02A99D80779AF2B0FF09A528BA47D6FBCE302
SHA-512:	33F5844E4972D57E5BBB9020AE13F6A6802669452624863333A16D2694D35D16F1237C60EDD5C9A4A914486A381F60A877D1F364E3A3E3910EF94D80B5954BB5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250375042011539","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8e837434-6485-4248-91a9-ac1f11478337.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):	5707
Entropy (8bit):	5.165411263296945
Encrypted:	false
SSDEEP:	48:YcLkMklidMqAcMRqB5gPOW4lYGlQuoTw0hcrO4MqM8C1Nfct/9BhUJo3KhmeSnpk:nBLRw4RIV/5k0JCKL8UkG1vbOTlVuHn
MD5:	AA57086C1151EB29EE11D827329996CC
SHA1:	D4A108DA61370D3F0ADD15E98C2F949B37EB440F
SHA-256:	793B67CB7B26EE23377494F265A4B2A3A1D1F300DE9F9BFDB54D20B8ECE08BF4
SHA-512:	FE70E9EC12DBC4394CAEF835B2FA4C06C4E400F86AF2BCFA880D81F8FA233BE13079421B49CE4258770BA3AF4A763A1DF02978A8E049F9437072B400C7ED5A0 A
Malicious:	false
Reputation:	low

Copyright null 2020

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8e837434-6485-4248-91a9-ac1f11478337.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250375042011539","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9fb099f5-80ba-48a2-8be0-4e401dbcd633.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):	5943
Entropy (8bit):	5.177964153968705
Encrypted:	false
SSDEEP:	96:nBB9w4RIV45k0JCKL8UkG1Kk+1A6TbOTlVuHn:nBo4RIGh4KbkG0k+1td
MD5:	A59319BD41F3BF406134D9B1E220E9C8
SHA1:	F6F6F41C0A51B892919E6AFB15EBD8EC300DC283
SHA-256:	6ED23E01D2437AE1EBB0467993C2F695FCAFC330B78A65B9B5436C93E8144FD1
SHA-512:	EAD2FA850C7B609BDA71BE1CA0FD097300ED4AC709CE9FB26EB1CCCEF908BFFCE38100CFD5B6366C314C9C4C6BE66831E52F952B3F60C855586F3B72AC9E3 62F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250375042011539","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.17015931538159
Encrypted:	false
SSDEEP:	6:3LpVq2Pwkn23iKKdK9RXXTZIFUtwA0gZmwyA0IkwOwkn23iKKdK9RXX5LJ:7pVvYf5Kk7XT2FUtwRg/yRI5Jf5Kk7XH
MD5:	0F1DED5561DE41B726D86E579A1F1780
SHA1:	8C8E9CB0D1C9EEE97C33885958E389A3993157F4
SHA-256:	D16E48030F9D4C60267FAD8AC796F00C0D413E2FD3EC30DB82481587EA3A345D
SHA-512:	14DD43A22835E33109874F80C2A6959D4AB503452BEEFA108082EB3402E063C6CEE98DAD2B0014B91C429FE7E0B9BA9C5ADC40E766FABF5ED59465A24E4C735 1
Malicious:	false
Reputation:	low
Preview:	2020/11/20-20:44:07.872 12c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2020/11/20-20:44:07.873 12c4 Recovering log #3.2020/11/20-20:44:07.873 12c4 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):	5.2025213724859345
Encrypted:	false
SSDEEP:	6:3RQ0Vq2Pwkn23iKKdKyDZIFUtwARHUXpgZmwyARgSIkwOwkn23iKKdKyJLJ:hHVvYf5Kk02FUtwe05g/yezI5Jf5KkWJ
MD5:	C66D0D8D1151AE1C8A3CDB0A6E875B4D
SHA1:	F089553A4C8A5884F73C77E2315B7FBE81673EB4
SHA-256:	923D9B4F998F17F4E2C59C162B6B67BB3FFEA30900EAF363773A666A802BACDF
SHA-512:	3B69768E9CE3AB403980ED85CF48B3177C9C05B2ECB4BEEECE297B7E7DD9A430436467C2D53FBC8FA4C4AB07158039295EC6396580BDBA5067FDE4EB8739C0 68
Malicious:	false
Reputation:	low
Preview:	2020/11/20-20:44:07.865 12c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2020/11/20-20:44:07.868 12c4 Recovering log #3.2020/11/20-20:44:07.869 12c4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

Copyright null 2020

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0044ba13f353fdb5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	198200
Entropy (8bit):	6.075674801506261
Encrypted:	false
SSDEEP:	1536:d55IXGFNZlk/Lu5vMUhT5nmfo+v5nmfNQfaRSTXEedlzrpGaAShzroEY9EVvZJnz:d50GjZR5vDRaPPzFGWzrDvQL3tDLw
MD5:	E30B42C27AA431C5793F4720A783BB1A
SHA1:	44AAA79B74FC4322C3716822B53B6EE739001551
SHA-256:	585FEBE318EA3977A4B9D5FF29436DB3AE4E47F5DB7ECDBF6FFCA60CEBD7FC6F
SHA-512:	0F061B8AAC82B26DC1AD773FDC175C0C5AD8F68E83ED6A3A3A29CD1995E8BB2E3CEF5D1764DA7EF06C25D220FF0EAA3A56BF73C1EF376DE79BD4ED0D8AB0DC49
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...|.....F1D06E9EA1B5FE5CEA0AE0EC2A091E9A9AE78B4A48C71B959B5F3DD35DC47D8A.....'..0....O.....cy.....85.....D...\.....h.....(S.0..`.....L`.....(S...95.`.j.....L`.....Rcp.....0.....Qb.L.....o.....Qb6.....r.....M...R....Qb..m_....p.....QbV..V....t.....Qb.....c.....Qb.....n.....Qb.s.....s.....S...Qb^..g....l.....Qb.....d.....Qb...X....k.....Qb.....h.....Qb..b....y.....Qb.H.....f.....Qb.f./....C.....Qbz9....w.....Qb.N.....A.....Qb^.U@....S.....Qb.y.....x.....Qb*&:.....j.....Qb.....B.....Qb:''.....G.....Qb:O@.....H.....Qb..iU....O.....Qb.....M.....Qb.V.(....q.....Qbj.c.....z.....Qb.}2.....W.....Qb...y....K.....Qb...x....Y.....Qb.j.1....J.....Qb.b.....Q.....QbZ..@....Z.....Qb.d./....X.....Qb&..s....ee....Qb.....te....Qb..8....oe....Qb.k.....ne....Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\01bb8b6526047012_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.62852814156392
Encrypted:	false
SSDEEP:	3:m+lPnRa8RzYkwlAdaJJKNGKYDdK2UUnNLxKX22+H/lHCxlll/21sl+rHxzErmg/R:mMYkXJwyDlWNd2+Hgx/EU+9lg/ZK6t
MD5:	75CACF0B44A90B8D787CF119A2B12DB8
SHA1:	5295E2E410761CBA7CF3F4EF51988B5D63B2C85B
SHA-256:	0CECEF7C908FE03103AABF4C7DCAF7B05ECA468CAF000FDECDE5643E75EC0C73
SHA-512:	085C8A8E7CCAF5A76FE0BFF344879894711BEB16052C543FBDD2E75A15EB79AC3A449713DF90AC1D9CF1A69775B1C4F57E1C35820BE28F6BB337C57C1BEFD3B1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...P"....._keyhttps://static-exp3.licdn.com/sc/h/6jblk5oqhlo45xbkmcr7s4zix .https://linkedin.com/.\.[%./.....SR.+...Ns..#z.-.....y...^....A..Eo.....$.vR.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\02e697c3a9d0c119_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	324024
Entropy (8bit):	6.028766373537068
Encrypted:	false
SSDEEP:	6144:WA71hCHCWZB/kKejnHQktjhAda0zGqZjFTYRnp:B6HC6BMKe7H7tjhF0BZdYRp
MD5:	0A3B81489D75B39EFB050D2BCDA2D5E3
SHA1:	A520B1EBBFEE696367422E77938A43BB9EBC4C54
SHA-256:	94E99B16C59D744988E29E6BDA18A0AD6BC1429BFA6C06C3266CFE486D082455
SHA-512:	7575ADBFD6BA71E630AA313E43493D6683029B391C3598FAB7B8C2DF74083FFCA68C0E0278771C425DBCA340391E8A57152D3F0E10521A58A0B3980E544624A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...w.....8EC0ADCF18CDF28E573D7B1DCC5B06001AF63E5B087E4C9CDA020F3A8FA2D4CB.....'..(....Oa...`...&.{.....(...h1.....4.....X.....`.....\...p.....$.....$.....(S...i1..`.b.....e.L`.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`.....M`.....Qc.....duS9k.....Qb>.....__d...Qdr\P.....GenderConst..(S.,.`.....L`.....I..a2.....Qd.6.)....NOT_A_PERSON`.....Qe.....FEMALE_SINGULAR.`.....QeJ.;S....MALE_SINGULAR...`.....$Qg..\l....FEMALE_SINGULAR_GUESS...`..... Qf..d.....MALE_SINGULAR_GUESS.`.....Qe...y....MIXED_UNKNOWN...`.....Qe..`.....NEUTER_SINGULAR.`.....Qe.....UNKNOWN_SINGULAR`.....Qe.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\05b44c5bd4268000_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.546910319733204
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\05b44c5bd4268000_0	
SSDEEP:	6:mSrgEYkXJwysS3O9RR9NTvmigdOpa78LrRiK6t:98UZwyB+9RzNyiHpZ10
MD5:	AC8E53CF3813A5464EF0403D2A25C15D
SHA1:	DE5441E7A8BDCB8EF5443F3E6AF5F66A6B94BD85
SHA-256:	E8C36C9A2F0142BD3F4401B6213157CF8A607B4A1578D61A9E6719C75AB6364D
SHA-512:	5BD61EFE6ECB0CF6DAFD341DDD81C5C03209BD6AAFB9CCB89100064FDD46DD1020CC3BF9B648B4D5709C9553F08101AF551AD045F75F89AB5CFEFEC26B0FF0D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...EY`....._keyhttps://static-exp3.licdn.com/sc/h/50seqnxcfadh00enh9ffvk85k .https://linkedin.com/a..[%./.....d..YK.....@.....B.7.e.j.....n.A..Eo.....g.P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\07ea641240d07017_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.668796713660854
Encrypted:	false
SSDEEP:	6:mapYk+f2pom0GfVwhmJ2Sacg6+eW5wBcm4ZhK6t:n++amPdwkJ/TWbu6mS7
MD5:	552BCAD45FD5D78F87CD3454B9A9FA0C
SHA1:	72D41F27A81B430DEBA79E0EDCD019F6AE0B44DC
SHA-256:	3050114BCB13C1E7ABF84716D7B05233829731985C4BACDDBD81612E5ACA1E4C
SHA-512:	01BEE32D323BA84E965F702CB4BF3E494CDF944390BE83628FE36030E77A35BD25E65372DACB8FE655CFBB859FB0BF2901CD3F1A0A164135128B3E6FE400AD90
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h... ....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yU/r/l1SacSmrzOr.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.2.\%./.....Q.w....T<,<_...w.Uhp....hi..G.A..Eo.....IVV!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\087a2eed37f66852_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.581077736067478
Encrypted:	false
SSDEEP:	3:m+lcjQ/C8RzYl4JIOkTK5MZKQiJadKTwYsXVRR9LxKLIH/lHCSg/ll5YMl1BGTFb:mwnYLZTTMJmpPNogSgL1gTVnrRZK6t
MD5:	AB304DE1664421A5AA66C00CD7DB48A7
SHA1:	20DA8268132DA804703ED8FE77D9965CB70927D9
SHA-256:	2927A0B040875D14BDD92DDB8C2EF23773AD37624B2DDBB0F23AB5E0DC2050E4
SHA-512:	A757FE6EB3FE4BA22080FA0BD65796A6F3C93FA5DEE2DD636A295EF630E84D95147B1B2FF33B99B6A112DB2A2461B6EABAAEFB6EDD711DCE9FBBD0F58B17BA40
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....F.c...._keyhttps://platform.linkedin.com/litms/utag/checkpoint-frontend/utag.js?cb=1605901200000 .https://linkedin.com/S.[%./.....B.....F{h.....%..%.lE.u.G.^O..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\094e2d6bf2abec98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.53882688869508
Encrypted:	false
SSDEEP:	3:m+lP9Ola8RzYJb9yKIf8QPKxWStHWFvDFYtREa5yv//lHCxtlX3bl58tyGdDmbpD:m3VYyK08fNH1DEzHgxtlXxyL61K6t
MD5:	C49AE5311FA86DA3E722C18AA225813E
SHA1:	9655B8AB0D2E8A05DF4A70B2050D68E4785DD3EE
SHA-256:	918EAE14FD5A5214B341A9E48E2A03C4440EF3157D6C634846570DD83A2844CC
SHA-512:	C68B502CF1E293F744D01CAE52847E030F0CD9705C2FAD3EC245855A7E9FC881CF7CF56AF3D429FE19C8BC5589B74926D52642113D96E5DFC25E4F483DC5AA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js .https://microsoft.com/l/.\%./.....].....=.z-.7.K]..~..=..9.....8...A..Eo.....m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d759eafff2bfe01_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1184
Entropy (8bit):	5.8248736837396375
Encrypted:	false
SSDEEP:	24:1i/LWgnU5TZjekq0+FO6si/LBI4L00Qm7/YMYE6noJm2:4zW5Pik1+cozB5jP/sEF9
MD5:	2AB2D245EE9C3A3234E3530F963751BF
SHA1:	ADCAF9B8493F68E75A867DEF5B886D61EFF7E45D
SHA-256:	4100C4470FBDA5DAC43F9AC418D5B2041D3F1671A8B7950E9068157908347AFE
SHA-512:	F14CD22EE26DA7BD9427B41B0625BBF741C663DFDABDED97CAD637AB80E2C12AD826638E41CE50728EFEFFD8A0AEAC84FCDA6FFD46F595A0CE2E29892D6F DA50
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.typeform.com/_next/static/chunks/b88873b11fb5db9f8fa5a9a1ffacd22835ab0d38.37780e08964bba6db448.js .https://typeform.com/ ..H[%./.....'.....1#../j.....G...%...{f`.G.D..A..Eo.....$x.....A..Eo.....H[%./.P.....'.DB...O.....(.....(S.t..`.....,L`.....Qc.....window. ...Q.`.....webpackJsonp_N_E..Qb*.....push.....`.....L`.....`.....Ma.....`.....a.....Qb.R.....Q8ZgC..Qb.....TcZlC.(S.....Pd.....push.Q8Zg...aN...:.....a.E.@.-....| P.....m...https://www.typeform.com/_next/static/chunks/b88873b11fb5db9f8fa5a9a1ffacd22835ab0d38.37780e08964bba6db448.js...a.....D`....D`....D`.....`....&...&....&. (S.....Pd.....push.TcZl...aH....A.....E..!.d.....`....D.PQr.,w.D...b88873b11fb5db9f8fa5a9a1ffacd22835ab0d38.37780e08964bba6db448.js.map]d..... .a....K`....Dw0.....&....&.(.....|.&.-...(...&.z...&...'..&.}..)&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\10b5ee069081cf02_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1456
Entropy (8bit):	5.756694731269679
Encrypted:	false
SSDEEP:	24:qnVKsd/yUvUle/o86JI0PztnK1cnVKskMu5glggj7yaiYW0iJTkT:q1Ow/o8xgztnnduDm7HOTg
MD5:	769448431EDCBD86285419F4D2AE2F10
SHA1:	91EA2161A88848AAF9DC30BFEB2C3D4B9AF72855
SHA-256:	A7188021C163771577B6484841B58364B0954E3D7A13D5C6F55EDCD389BD3CA7
SHA-512:	90D2F5DDBAABFA30592CCFB1989EA82FF094E69FC487EAAC72DB08E17DBF067995E1AB9A1C9CA61C92E60907BC4BE8EEDA9263170FC95C3F2BC02F8E08145 69A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...|.dn...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yR/r/CiBSy0eOG1U.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...Z%./.....|.@.?...\.4.....ew.X.. ..:.).A..Eo.....A..Eo.....Z%./.....'. .....O....@...".....(S.d..`.....(L`.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`... ...M`.....Qc.).(....52Eas.....Qb>.....__d..$Qg..1X....BanzaiODSWithBanzaiImpl....`.....M`.....Qd.^.....invariant.....QcV\.....Banzai....Qcb.@.....Random....Qb..s.....gkx..(S.. .`.....$L`.....8Rc.....O...Qbz..0....h...a.....I`....Da....0....(S.....Ia.....@..n3..... .I..Q..@.-....\P.a.....M...https://static.xx.fbcdn.net/rsr c.php/v3/yR/r/CiBSy0eOG1U.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`,...D`.....4...`....&...&..!.&..q..D&.(S.....Ia.....I...a.d.....`....DI]d.....A...Qd^b.>...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\113da93680c2e273_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.520648447931774
Encrypted:	false
SSDEEP:	3:m+lP7R6OA8RzYkwIAdaJJKNGKYAMbwdpVV/LxKce/lHCkzlte4Vukz8eBWeap9hD:mYcEYkXJwypUxN7egkzlsDoTyk4nK6t
MD5:	0E594881602C05C0D2DB5D1D16396E8E
SHA1:	894F777498CF09FF5AFBCEBDF017A806094CF480
SHA-256:	581CEE22FF90F03F860117665C85F6A893A217AE25C810A435F6538B1B199785
SHA-512:	F058ADD2A22B084FB0619746EF81566971B9B1ADC7E0CBF415F90FFCAD5862FB20EBC7E38347E7EEBFB01455942C60500614FC276A1143D232C40CCE5928CC1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.....d...._keyhttps://static-exp3.licdn.com/sc/h/eifp0ukycgmm5y0uay3omxuap .https://linkedin.com/.*.[%./.....{.dp.N..U.....\Y+.S.ZN.dV_.....A..Eo..... Xq.m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\11d863c85aaf1b7a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2112
Entropy (8bit):	5.657838957769047
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\11d863c85aaf1b7a_0	
SSDEEP:	24:WnVgpEacDvLUv2UR3J6WEQ0szsF8Xdrg1cnVgAOXAujivRsSfsVGT2tc9B0iJT6w:W4TcDvER5wF2sesSkMhTZMa
MD5:	91E62A87468B77DD1FE3AF91A3CF1536
SHA1:	B923258527E4A9B191D6073601D49A8C6108EA3D
SHA-256:	88C36BD3C538C94B7B860FB721C6396F33D8DE62C2135F86A4CDE2D703CFC0CA
SHA-512:	6BA15C6A852FFBB89E33227EC55850D33FBE603A88F19893B12C62C5CCBD7A26FF147277F3E29F34C6739EE70E12094B427C8B8ED608066DF9119BB5B85EAA8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....1....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yk/r/88TDH0_V0xJ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...Z%./.....x.D{.n..TeG..h.....5 .h.=..c.A..Eo.....4.Q.....A..Eo.....Z%./.....'.....O.....d7.....(S.d..`.....(L`.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....sta rt_js.....`.....M`.....Qc.w.....fjaOu.....Qb>.....__d..$Qg.X.2....BanzaiODSWithFalcoImpl.....`.....$M`.....$Qg...r....OdsWebBatchFalcoEvent.....Qcb.@.....Random....Qb.].....R un...Qd.Q.....clearTimeout..Qb..s.....gkx...Qd.kt>....setTimeout...$Qg*.....unrecoverableViolation...(S...`.....HL` ....`Rc,.....O.....Qbz..0....h.....S...Qbb.....j.....Qb...-....k.....QbZ!Wy....I...f.....I`....Da....J....(S.....Ia....4.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yk/r/88TDH0_V0xJ.js?_nc_x=Ij3Wp8lg5Kz... a.....D`....D`0...D`.....4...`....&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\135cc07817299839_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	76216
Entropy (8bit):	5.856395922200089
Encrypted:	false
SSDEEP:	1536:wRf9vn9tRnsaH4SfB0qollalEtyEog5r+epfxveG:qPFqSoGlsRX9+epfIG
MD5:	8A815CC3A8FCD25341C61F49FB6F179D
SHA1:	1F16EB3FDCAE616C2E83CFD4819955F19D645F9C
SHA-256:	FF361DC2D85892DBCFF370A3D7292B3B77FB808777360172E40BE926E61ECCB0
SHA-512:	96AB4AD9A4F9CB834F6E26CBD9CCC3C8909FC9603D9145CFE5D3AEF83FB9FE1F3A37D13C23FDE6FA25B698EC4B2F72C9450AD0B32028B9FFB2CE7FF752136 20
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....MA....6E023B240D2D91DB42D81F9314B3618D04F999B1515D6DE71B2E96B181E13DEF.....'.....O....x(....@..... .....(.....(S.....`.....q.L`.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`.....M`.....Qc.d|.....kIaGI.....Qb>.....__d...Qe..i.. ...EmojiFormat.bs...(S.\.`n....,L`.....8Rc.....Qbz..0....h...a.....I`....Da.....(S.....Ia.....d.....@.....@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/ v3irQw4/yA/l/en_GB/X40LLUSMcTW.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`b...D`.....`....&...&..!.&....D&.(S...Ia.....d.....@.....M....Q.d.....@.....D&.(S.....Ia ....`.....d.....@.....d.....@.....D&.(S.....Iaj...}.....O...d.....@.....&.(S....`.....,L`.....8Rc.....a.....I`....Daz.....(Qh&4.R....scraperLastPe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\176e7d1d913270bc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.457476583103352
Encrypted:	false
SSDEEP:	6:mwh0lXYGL+MIwJJwMxugSSJilxhm47bK6t:dGlwve1UDGN
MD5:	C88B5C802B2F7B2D2137E1F31A49FC1C
SHA1:	2B1CF7442EDED47FDF4E7DFCFB34AA7806D97307
SHA-256:	501F0C82D45EFDD58862A7B19B9A184435B95A40B17842951B29DA51CAB8008A
SHA-512:	F562A177511D5FEFCBB6CD0DCD609B4701D61CC4C2D96439BFA7289707A58501B1AEDD38AB0BA1D7A8AA9053443383240D0562794D65C2C161C36FC5FD1641 E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.....I....._keyhttps://www.google-analytics.com/analytics.js .https://twitter.com/x..Z%./.....:.&..L...jC...1UR@u<$mz.B...u..A..Eo.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1a3eaa7325c8d467_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6019
Entropy (8bit):	5.718891549356715
Encrypted:	false
SSDEEP:	96:7zHo/ALz3sgoU3hO0owZORKT4LDVF9T82Md3Jszta5:7zHoALzDxcwkRnONOzt2
MD5:	00D1767907FB72F00F427E662B8F9983
SHA1:	CF8BA3A405F90B08D53C4DCDE2FE6A4EAC3475FD
SHA-256:	E20096657972D48937DD8AE9C1AF83A9DEEAEF187B283221215F6EBA744EDC0F
SHA-512:	923736237866E2FA9246C80DE620AEF8E3D5D862E92A36714AAD8C9E341D69455B4D43AA0D674BBD168BD52F15D628D775A3454A81B689079D8D60C3C67A813
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1a3eaa7325c8d467_0	
Reputation:	low
Preview:	0\r..m.....s...v@....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i9Zn4/yn/l/en_GB/anMEAxulSXI.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.u.Z%./.....lY. Os.y.r.B...$.~.@.).....DG.A..Eo.....Lon.....A..Eo.....'.....O.....(S....`j....XL`(.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.. ...Qcz$3.....start_js....`.....M`.....Qc.....Uptn1.....Qb>.....__d...Qe.....HelpLink.react....`.....M`.....Qb.....fbt...Qc.....React.... Qf..;X....TooltipLink.react.....QdV.k.....j oinClasses..(S.x.`.....0L`.....8Rc.....O...Qbz..0....h...a.....I`....Da .....(S....Ia..... ..f..... .... I.....@.-....dP.....X...https://static.xx.fbcdn.net/rsrc. php/v3i9Zn4/yn/l/en_GB/anMEAxulSXI.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`X...D`.....`V...&...&....&..!..D&.(S.\..`r....$L`.....0Rc.....O.`....I`....Da....R....(S.....Ia..... .....,..i.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1b7f01dd400d068b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12183
Entropy (8bit):	5.797562237384016
Encrypted:	false
SSDEEP:	192:X4mqlJh9AHJPYXhsOeezjptWrOSfm765jsxs9y3Ve7SWYXqvoVKepnvBk:/qIsXbmvieeJILWiKeXk
MD5:	512DEBAE69EE95B4D9528B625ED8B322
SHA1:	92D9D401AEE9D64274DA563CA071E27BADFAEF5F
SHA-256:	3B62AE2368BBF49C9A5012C0B2EB798511D60EF38EDF5C5232C07C452F86450C
SHA-512:	57948E1517181E9EC83FDB71183A79DA5F03E0DB789D2B946030564543CCD69654F9AA11CAED7D0F989AC317E65A9ECCF199845EBEA805F8E73310ABECF312F 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....._keyhttps://www.typeform.com/_next/static/chunks/commons.669b84830f35556d6bde.js .https://typeform.com/R[l[%./.....T.....o4PL..h....:....[T.*.V z>.w...A..Eo.....A.....A..Eo.....'.2l....O.....p}?.....d.....(S.....`.....L`.....Qc.....window....Q.`.....webpackJsonp_N_E..Qb*.. ....push.....`.....L`.....`.....Ma.....`.....a.....Qb..k...../0+HC..Qb...J..../GRZC..Qb.....284hC..Qb. .....3r9cC..Qb.i.....48fXC..Qb..7(....4fRqC..Qb.....5fIBC..Qb.... ....5kbpC..Qb:.t!....7eYBC..Qb.E.^....8Kt/C..Qb.....8oxBC..Qbr.y.....8xP1C..Qbj..Z....C+bEC..Qb.....ECySC..Qbv'.x....FYa8C..Qb..1J....GbB8C..Qb.....I2ZFC..Qb...l. ...KckHC..QbJH.....LH/LC..Qb.....LbmRC..Qb..p.....ME5OC..Qb.....O4CFC..Qb.~.....QetdC..Qb.h.....RAsNC..Qb.....T0f4C..Qb.....TAZqC..Qb.....TOwVC..Qb&..... .TqRtC..Qb.~'.....WwogC..QbR.....XuaeC..Qb.....aJjTC..Qbn.....c7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1bf4ec734dbcd926_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7280
Entropy (8bit):	5.864648992365464
Encrypted:	false
SSDEEP:	96:fg2dF4WlTfZBLC68zxpzhmXWuaEO9FZN1z2cRIub9ORfLD1syu/Sz:fDdjHLCdDzhgWuaBTZHz2W9ORn1BuC
MD5:	61995E02C0889FF67EA808A4ADCEB8EB
SHA1:	18A96103050427B7D6DB46363942B8BFEBE32289
SHA-256:	0ABB0F2804194C7A8C6BB703DBD15D7112E9503470FC29925DF261D03C39745D
SHA-512:	3853E3A65BC95762D6D62BF0E82E2B8B2E6F37936CE6E06BC017332E97E8584B3488B2DA1E3DF4F754D0AA15DA2F17A8D3509BDDF15E036C778A16EAFA4D09 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...M.6e...._keyhttps://www.typeform.com/_next/static/chunks/760b9a88.c99a0a27199d7bd13122.js .https://typeform.com/..F[%./.....t.u...<...ov.`..s.)"...7 ..J"=>q..A..Eo.....A..Eo.....'..4....O.....T.....|.....(S.l..`.....$L`.....Qc.....window....Q.`.....webpackJsonp_N_E..Qb*.....push. ....`.....L`.....`.....Ma.... ...`.....a.....Qb.!.....VHu/C.(S.....Pd.....push.VHu/...aQ....4...i.....!q...:.....@.....@...&..@.&.&..@.&.'..@.(.*..@.*.+..@.+.,...@.,.,...@.,-..@.- ....@.....@./.3..@.3.8..@.8.C..@.D.D..@.L.L..@.M.M..@.M.M..@.M.M..@.N.N..@.N.N..@.N.O..@.O.O..@.O.O..@.O.R..@.R.S..@.S.U..@.U.V..@.V.W..@.W.[..@.\.\ ..@.\.]..@.].`..@.`.g..@.g.l..@.l.m..@.m.m..@.m.p..@.p.q..@.q...."@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....3.@.....@.....@.....@.....@.....@

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ded97f6a28d5a09_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.481516146366145
Encrypted:	false
SSDEEP:	6:mvYxRQ3GjXc5pT1HUInGGbI8igB/kPSe/F+8LEK6t:1Q3+c5phUoGqIta9o+d
MD5:	F113F66DB3F6AD0B5FF8E8A1773DBBD1
SHA1:	7BC346899B813237CD051B6BEAF54E427D1A42B2
SHA-256:	723FA20399E039944C8A46353C117B77D48EA1EAF451F5DAA7A330E3D6286A17
SHA-512:	7547351D1ADDEC99D277801F1C0EB771FF4C98E6DD84C5E7307514C98B0C193EDE1FE8D19CD3C01CB46F1C99131AFB55FE61AF753AB9B98A098F8BDE0030D1 B3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ded97f6a28d5a09_0	
Preview:	0\r..m.....g...(.1....._keyhttps://renderer-assets.typeform.com/modern-renderer.1dc96dfb1da55c4cfd25.js .https://typeform.com/.5.Y%./.....3.....INNG.. .#....F.{.T.%...F.f..]...A..Eo.....#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ef7d216b0421f0f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	379
Entropy (8bit):	6.0144457481986136
Encrypted:	false
SSDEEP:	6:m9kYk+f2pomWqKJnV6zhmJ29KFgz2h/mMo0n9FZK6tn+lEnRCOXnny8QqmMo0n6:/++amfKJQzkJQug2h/doYThQEnlXyBqG
MD5:	2648A3FA4B66E0FF1BC169C8CE42D625
SHA1:	477F13AE0D0C3B865BA10490D2A0E240C107782E
SHA-256:	C540DCF72CE72FF5354EC3A87B4E2C6EB92459E3031AF947781583DFCFC55B0D
SHA-512:	5487096B17457141D92076825229753CAFD62C19D72DA2CD9031A58A32105E586E0F0870D48610B1FC8C6C28D220B849161DB9FC159456CA454A60A3F4CBD821
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3id2q4/yE/l/en_GB/BVpZI4bmBYG.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/o..Z%./.....X..;D5O<L.!...C...C...(;.e.\....A..Eo.....I.....A..Eo.....o..Z%./.`...DD6D9B1F4B5A59556C50A8EA9FCA2BA196201425BE43A8C433DD2A7BBB52ADADX..;D5O<L.!...C...C...(;.e.\....A..Eo.....jb..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\20ab2bbebc418a61_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14776
Entropy (8bit):	5.58569115241377
Encrypted:	false
SSDEEP:	192:EvTFUXW91dIq/FPDxwj9ZG3/X7UkRLb3Yv5iwmewoqNVWi9YQoT3rC2cv:Eb19/NFtO/tkhq5JDTeYxcv
MD5:	172DCBA25E3210684AD241986C05DF3C
SHA1:	9FFA825C734CD9886B6B1E3B5064819CB4A13487
SHA-256:	0E4AF9A52E72A50510FC22A30D5BE119C66D8B666CEC6D544378C94867A63BE9
SHA-512:	D9C2188710B10461E8071B28F96E56230D98D5BCB8EDBE4DD1B854A6A25431A8EA3564BC3A0B85749B1A77BE76B0A9F58D3A035467F88EA53ED129B7BC8F83B7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yl/r/1d5nFTij4Ob.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...Z%./.....\.....X../..1..nQ/.gC.'U%..T.....K.A..Eo.....eJ."....A..Eo.....'.83....O.... 8.....(S.....`b.....L`.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`.....M`.....Qc>.....xgfl9.....Qb>.....__d..,Qi.....LitestandStoryInsertionStatus.....`.....M`.....Qd.....ArbiterMixin.(S.l.`.....4L`.....0Rc.....`....I`....Da.....Qc"..)....check.....a.....Qev.9Y....registerBlocker.C..Qdnq.....canInsert...C.(S.....5.a.....M....a.....A.a.....d..... .....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yl/r/1d5nFTij4Ob.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`h...D`.....!....`....&...&....&....D&.(S.....Pd.....a.canInsert.a....W.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22b37a349d2034b2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	20227
Entropy (8bit):	6.060506924924258
Encrypted:	false
SSDEEP:	384:wvtI6tq0r9xzpVHIGVQfwTb2VJDugJRRuiJZL38wZ/uApc0+2eW:wv+6k0r30G/J2L3z476
MD5:	1C145E9A67E53BEB9516C686287EBF1E
SHA1:	EFAC93E75E285BCE7A5002662D6CDB28C9E0BA0E
SHA-256:	57CEFBD5662225DD767C685FEDE7B8949E7EAB431B0B293B0CC191A603759A52
SHA-512:	5BFB1E986683EB1CD1B5DDE14D693EB2F1E71702352F9FDA9E65857154E9203FE0EA6A4DE67E751707EE5631FD60096FB65BA125CC2EC96C77CDBB599A43471
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....H....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iJq44/yd/l/en_GB/eZdBZ6fWkcm.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...Z%./.....^.....)M.0../.z&Y.M.e....T8...EbP.Z..A..Eo.....F..,.....A..Eo.....'.....O....XM....BE.....\.....(S.....`.....L`b.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`.....M`.....Qc..PG....hUh0n.....Qb>.....__d...Qe...e....CalendarUtils.....`.....M`.....Qd.~n.....DateStrings...Qd.....LocalDate....(S...`....LL`"....@Rc.....O.....Qbz..0....h...b.....I`....Da.....(S.....Ia/.....Q..@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iJq44/yd/l/en_GB/eZdBZ6fWkcm.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`^...D`.....`L...&...&..A.&....&.(S...Ia.....Q....q.d.....@.....&.(S....Ia....M.....M...Q..d.....@.....&.(S...IaW.....Qb.9.....c.....d.....@.....&.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\299bc0ffd816811a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\299bc0ffd816811a_0	
File Type:	data
Category:	dropped
Size (bytes):	10536
Entropy (8bit):	5.767627280307833
Encrypted:	false
SSDEEP:	192:BB1zvEMtM0q9QRxZrVRZrmUvL2CiQp/HmN5nV1rduAi:pXlxZTtmUvLLPUhV1xC
MD5:	C2FDAAC759344EF4251A6E596F12802A
SHA1:	5DAFB44966DD33255EC11B27F5EBE03B3AA0071E
SHA-256:	27566E109699ADAB51ADF5333C7B3FE8184F64936263F66114691AACB81E245E
SHA-512:	C92E6DDE194AE6A76E30D127F018CB9D6F92AD52D6C198F6BF8F226C00843586B2B536B5BBC5782870DC271A2E53190A20445A756F5F48308763216C39020C65
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....._keyhttps://www.typeform.com/_next/static/chunks/1acc62d8ce7d026a6eee13d7b40f1eb2588ce752.2f948f86a1985f04d66a.js .https://typeform.com/ .eG[%./..... .....).P.x.-..Q?..Z.)..r.8..^2I..A..Eo.....p.....A..Eo.....'.c.....O....p'...t.....(S.....`.....L`.....Qc.....window....Q.` .....webpackJsonp_N_E..Qb*.....push.....`.....L`.....`.....Ma.....`.....a.....Qb.b.....+VSoC..Qb.....0SfDC..QbF.._....1BAgC..Qb.}.5....1kFSC..Qb..;....4ThwC ..Qb.q.X....6AH7C..Qb.7.....6ZWGC..Qb..4.....78t8C..Qb.....82gjC..Qb...|....8YXYC..Qb.....9uj6C..QbB.....AWprC..Qb.....EMCGC..QbNfw.....EMfcC..QbR[.....FyfSC.. Qb^x.....HFSGC..Qb...B....HL2+C..Qb~.:.....I90/C..Qb..\:....Ibe6C..Qb..x....J8E0C..Qbn.....OPUVC..Qbbj.&....OPXVC..Qb.mZ.....TSYQC..Qb".....U117C..Qb...E.. ..WMsnC..Qb.#.....YZRoC..Qb".....aqg2C..Qb.....cRixC..Qb.E.....cuULC..Qb.{0....dIm

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c32858c83a27761_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5096
Entropy (8bit):	5.896057313568167
Encrypted:	false
SSDEEP:	96:VufACBODjfb+wRbaifFkmzaXsCNeVIPH6HDNu28fTRr/f96Y:Y4aODmw5aiN3zgfeKYgbdrYY
MD5:	96F2036AF31A5AE47B9D4F0EE5A9EEB2
SHA1:	170C499C8DA4E91E32C3D869BBC822B797B70E71
SHA-256:	0D089F75C3CC40E61E4818C03153E4C6118A28F67767D50BFCCC251BE96158B3
SHA-512:	0A84B00497B05EEBF2BDED69DF255C815C2EEF8E33254EF663BD9C50DA59E85A40F0FFD0DBD3663942595F687B10C2D46B90037BE3478398F1B935A9747BA27
Malicious:	false
Reputation:	low
Preview:	0\r..m.....+...._keyhttps://www.typeform.com/_next/static/chunks/07b2ac42de669aab1e26f9dcd6e1211e4d65a4a3.b303d9b5d73a4e58b3b1.js .https://typeform.com/ #"G[%./.....xeV7...uF.6`.....j.0.:...3.\.A..Eo.....A..Eo.....'.....O....8.../.z*.....(S....`.....dL`.....Qc.....window....Q.`..... webpackJsonp_N_E..Qb*.....push.....`.....L`.....`.....Ma.....`.....T..a&.....QbR.].....Dr1XC..Qb.D_.....PftbC..Qb.'#~....cMu5C..Qb...z....dnzcC..QbB..#....k0YDC..Qb.h.. ....kMBYC..Qb.c.v....lbZmC..Qb.U.....pWNRC..Qb>.....u/Y6C.(S.....Pd.....push.Dr1X...aN.....(..g.....@.....@...".....8.l,.....@.....@.....@.....@.....@..... .@.....E.@.-....|P.....m...https://www.typeform.com/_next/static/chunks/07b2ac42de669aab1e26f9dcd6e1211e4d65a4a3.b303d9b5d73a4e58b3b1.js...a.....D`....D`. ...D`.....`....&...&..A..D&.(S.....Pd.....push.Pftb...a&...{y...Y...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2cbf864a87e47638_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270
Entropy (8bit):	5.607870632193611
Encrypted:	false
SSDEEP:	6:mu/XYj018IrAMUowfs21fKYvpMvmugLuoRo4fLnK6t:T1thUU29Juir
MD5:	7BAAA6C1FA7C3BD4AEBD348548614677
SHA1:	633ADFBDFB6AB302957F4CC3C38E383B2D3D4D12
SHA-256:	4A662461B9D7406997F87D99B667A6376A5E7A5F510CAE3548F94CC162E0BD12
SHA-512:	A7439F5975B7E2FF16934B6956035953A630DF6215D982756FA67E4325452724A0FD8952D6E6572608266C463682D161A7D120EC25AF074314E37B96514C9B46
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~ondemand.EmojiPickerData~ondemand.EmojiPicker.c8bd3f05.js .https://twitter.com/..* [%./.....0...j.x.*s.B...'._.f...f.K.:<.R.A..Eo.....q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e7da6200e9bb853_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	383400
Entropy (8bit):	6.0488659348369485
Encrypted:	false
SSDEEP:	6144:wUKxEEBCHac55IVfzh87S44DpI0bFDyw/uKjrE3WHITjO:jdEBkaMI1ziV4BKy

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e7da6200e9bb853_0	
MD5:	8763FF94AD5C98687839E2510EC6AEEE
SHA1:	E40DADD088921249639081431E4638C505FA65C3
SHA-256:	8F5411BC8F4C3BCD7E2D88791D19EC78565CF4E837209121503A0FFF12AB48F2
SHA-512:	51543D89E3762D9EA97BEDE9CF109717320EEB7E1E81C2A669853B45356CC8E5B0FFC9D902B38ABE29CF2BB506D48745AE0C4383ABC4B8C4B60B9A919CDA712B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...k..b....18FD3140031F3A456438F9B5D54F48F30AD826F3494DCF9D0E7ED91A0EA5C7B7.....'.....Os.....d.....l...L..... ..l.....T.....|...P.....(.....t..... .....4.....d.....(S.....`.....L`.....Qc.....window....Q.`.....webpackJsonp_N_E..Qb*.....push..... `.....L`.....`.....Ma....4...`.....`.....L`.....`.....@M`.....Qb.S.....VFsal..... ...(.....$.....a.....Qb..7}....+KjYC..QbJ.....+QRCC..Qb...R....+lk3C..Qb .c%.....+uZHC..QbR&Yj..../bc4C..Qb&!2.....14XmC..QbJW.....1D5qC..Qb...Z....1NkxC..Qb.....1XyrC..Qb.J..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2fe6116701ae5007_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2984
Entropy (8bit):	6.028977956024007
Encrypted:	false
SSDEEP:	48:Cf9dFkgAavfLEfcweNCXpfl5givCcUmawxSLixs0xsL5Z2jxEJt6rwPkImopWop:CaAvzEfcxNil5gxcUOxSLixc5Z+xEJ4G
MD5:	0A59313C7786DDEA9BC777CCA89D0376
SHA1:	6B30917E4F56FCC1037A99014237D76723BE94C2
SHA-256:	5823E82BB6DAA4337F8A1B38D0796E767D53D9CEAFB9DBD68487131852BB5967
SHA-512:	149AB14B5D94A74E8C24E674579DF67DF76B279F557246DD1ED6D484F62CB330157EE198B508B99D9A461FCD513F0FE6F1EB5C41280A03838E67937DA279C655
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yr/r/FZmFG4Q8g6o.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/:..Z%./.....e.....wx.Wj...m1.b..b...|.....a. .d.A..Eo.....+.8f.....A..Eo.....:..Z%./.x.....'.....O....8...U_.....(S....`....0L`.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js..... `.....M`.....QcVA.....5W2Iv.....Qb>.....__d..4Qk.D.6&...ComposerFeatureIntentLoggingDispatcher...(S.<.`2.....L`.....0Rc.....`....I`....Da.....(S.....Iav.....M.. ....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yr/r/FZmFG4Q8g6o.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`F...D`.....(...`....&...&..!.&....&.(S.<..`.....L`.....0Rc..... .....O.`....I`....Da4.....(S.....IaK.....$..g.....@.....@.....@.....M.....d.....@.....Qc.2.....exports...K`....Di....8.....%.....&.%.-.....b.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3054c3c3e5556e82_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	206304
Entropy (8bit):	5.882869362898643
Encrypted:	false
SSDEEP:	3072:zEinItwbM11+93xmfw6O9pL87CZUKOjpWt8uETZpIafobRU7k:ztbYI6O9rUKMwt/UZ7fobi7k
MD5:	4ED93B11CF0048E54D88EEC317D0689B
SHA1:	854BB57BA0061AD17902BEC4E769412889061A63
SHA-256:	E28043353B79D8E86CF3FDDDD08FA4A418238DF01DA87D842B63BBFE480448A3
SHA-512:	1D2C4FD55AB0097934CC0438995C5422734D587DE111E19E972E9B19098F9088E3B756836943D1F26DCE4C8EFE5362989C0F8612D1751F1D5899B9157E43B5B0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....|2....EFA9D4E168229CBFFF0639F08DACC17CDAD0A106AE17AAE0ABB4BCC31304FFBF.....'..1....O@....$.....(....(..... ....T.....(S....(..`.O.....L`.....Qb.H}Z....self..Q.`^. {e....CavalryLogger.....Qcz$3.....start_js.....`.....M`.....Qcv..c....URZlS.....Q.@.....__DEV__..(S.....5.a.....a.....Q.`..X?....emptyFunction...ax...|..IE.@.-....\P.a.... .M...https://static.xx.fbcdn.net/rsrc.php/v3/ye/r/bBkuQPoyW79.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`..... ...`h...&...&...0&...(S....`.....,L`.....8Rc.....M....O.a.. .....I`....DaJ...@.....QbZ.....flat.(S.....la....x.....d.....Q....1d.....(S.....Pd.....Array.flat..a.....I..d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\361ebf4a409f776a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.841178167662218
Encrypted:	false
SSDEEP:	6:mfYeM04ruotgUf1rUXK6tS9qVlJgAdkdlmG51Lku1rUE/:YMwotR1++qqp1Su1l
MD5:	D0D20D07DAF783CBCBEF79EE806FCF1D
SHA1:	2A9376E8B9390B15E680ABE6086E4492D5725070
SHA-256:	DD8AB8C380869F64D3D691A47069CCAB490B177600E7546CD70A530D3E085D19
SHA-512:	A1D6EF0E2E270116B7CDED0551A365037895408C7ADE5C3AEF36FFF74F59288E9A5AC6DC992443A38E64419DA5952648016215D0CDF91375882ADB0E894589500
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\361ebf4a409f776a_0	
Reputation:	low
Preview:	0\r..m.....`....%.k...._keyhttps://code.jquery.com/jquery-3.1.1.min.js .https://contemporarylivingconstructions.com.au/.PZ%./.....K.....r.H.....d4.@AX..K....A ..Eo...../.....A..Eo.....PZ%./..y..EA1D0BC7911F6A59E499C3C8A851C7CCFCC4F4953B3743189817D888FBF1798E.....K.....r.H.....d4.@AX..K....A..Eo.. .....1._L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\370a660deb3efd3b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6688
Entropy (8bit):	5.660496956383748
Encrypted:	false
SSDEEP:	96:ps8xike1yW7/pqqpHCySUhhumZINZJpuBhVNUG2vIvBdcba5AqyHcEs:pBYkcyLYUmZInpy32a35Aq/j
MD5:	78BCED85759B33B4C7C0B5D1B220786F
SHA1:	B7BC61CDFE9550C181AA87B49C5BBEB6B909792E
SHA-256:	30DC2B896B87BDE2665D8DD706FD8CCCD19D12F3AA191B253D6BDAB834A0D2CB
SHA-512:	509A66C6512B2E27F2AE74CCB59340F5CEC42739D49BE88B7DFF8E76F7A57F429093EEA21B305F2B33E7423BC6C8070E65E41AFD2904B7F8080F32F2F297BF1E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....M...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yh/r/sbJIxk8bYkn.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...Z%./.....q.....e0.@LB..]...j.....U.... ddQG...A..Eo.....z.N.....A..Eo.....'.....O.....%.....0.....(S.....`.....L`J.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_j s....`.....M`.....Qc.2....3+aH2.....Qb>.....__d..$Qgn:.u....WorkSwitcherTypedLogger....`.....M`.....QcV\.....Banzai... Qf.F.....GeneratedLoggerUtils..Qd.0k|....nullthrows... (S.D.`D.....L`.....8Rc.....O.....a.....I`....Da,..T....(S.....Ia....E....I..y].....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....I..a..@.- ....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yh/r/sbJIxk8bYkn.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`t...D`.....`....&...&..Q.&..A..D&.(S.P..`V.....L`.....8Rc..... .....O.....a.....I`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\37528fdf671b5653_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8528
Entropy (8bit):	5.6397417269318995
Encrypted:	false
SSDEEP:	192:UIycn+zWgi7iW2MtM7o7atBF9Z7Z7rw7eBkmQQ:U6+zVi7/klaP7oHmN
MD5:	C2E5C77D96E8C06E0BF0A9CA61FFEABC
SHA1:	8909BA409E95359A9F5F7C9C07D0F6DDADD85A38
SHA-256:	B9F2F1B22B56D1E3E5D3273343E72F042C1A4347188789109F3A91C2C39B0F62
SHA-512:	A771A3D6C40276281127C093FBB2DD7FE1C2751232BF4CFBFEA0654AB0C25033DE75D0C46251A7FE85249E83115200260E0CDDE7C54FD2F91639D2DF6A6C874
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.typeform.com/_next/static/chunks/17b61ed54e577e57b19060206cf971f91ca2d519.3c49a1eb6efac428e6b2.js .https://typeform.com/. G[%./.....D.{.....y'.....x.H}A.#.._.aW..A..Eo.....TzV.....A..Eo.....'.....O.....L.7.....(S.....`N.....L`.....Qc.....window....Q .`.....webpackJsonp_N_E..Qb*.....push.....`.....L`.....`.....Ma.....`.....u...a.....Qb.UF1....05uCC..QbfY.....4umIC..Qb^.k.....5D8CC..Qb..2.....6hptC..Qb*.=Z....71 LfC..Qb.lG.....7LKLC..Qb.q.....CSm3C..Qb6."....CrRXC..Qb..,C....D4jQC..QbJ.....E0qHC..Qb.m.....H8DLC..Qbz.....HWy5C..Qb.r.....J2faC..Qb.....J4zpC..Qb.O .....JX7qC..Qb.....KL9zC..Qb~.....NfZxC..Qb.1.o....OcOZC..Qb..n.....PY2iC..Qb...n....V4hiC..Qb..l.....XX6WC..Qb.X.....YSVzC..Qb..h.....bO7iC..Qb.....d/mpC..Qb.K. .....dI71C..Qb.~.y....dwcoC..Qb.'.l....fNrwC..QbZ..S....fzfyC..QbRL.....iTG7C..Qb.>.[....lDWVC..Qb.T

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\38ee049088fe68fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7025
Entropy (8bit):	6.22777345789036
Encrypted:	false
SSDEEP:	96:XV91yLI8pbiV9Kx4902xyg4NYsbOgnhDQZ9SJyRVDJm+B8ulbObpVeUBs+B9gh/C:XDH8AD/e2xu3lySJHuBSjBsM4zG
MD5:	D7BAE7C022E8145083D3205BD02D8B57
SHA1:	FF010F1D58449AADD6FA4159E4262CEFDA250DC8
SHA-256:	5AA1267FB743CD39027CAB1A760C5550F740BDD5473EF2EDF1D503E50B19460F
SHA-512:	558769018D77D1BE3A87047722091F0C752127CA3D32839983FCF4D9E8488E718B3013F60DE20B1E890EAA45CBB1ACA435C994C39B9709A21F59CBAB19740D65
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\38ee049088fe68fe_0	
Preview:	0\r..m.....i.....V....._keyhttps://www.typeform.com/_next/static/chunks/framework.8683c114909ee93ee89f.js .https://typeform.com/.F[%./....."#L<`.6Sv..&.^.j....]5t. ...B.4K.A..Eo.....A..Eo.....'.c.....O.....L.....(S...`....tL`6.....Qc.....window....Q.`.....webpackJsonp_N_E..Qb*.... ..push.....`.....L`.....`.....Ma.....`.....d..a.....Qb.....+wdcC..Qb..^\....16AlC..Qb...2....17x9C..Qb..pW....8L3hC..Qb.d.o....QCnbC..Qbb.f....WbBGC..Qbr.\+....f/k9C ..Qb.|vo....i8i4C..Qb^.....q1tIC..Qb.....viROC..Qb.f.....yl30C.(S.....Pd.....push.+wdc...aP...Q.....@.....@.....@.....@.....@.....@.....@.....@.. ....@...".@.".#..@.#.$..@...~...*..... d.....$.$..@.(.....E.@.-....\P.a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\39b05e5f07e50d94_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.563196823491343
Encrypted:	false
SSDEEP:	6:mD9YxRQ3GjXGLcHh2wFGGUKFgYSyprd7/bK6t:DQ3+cg2oG7KFnrp
MD5:	50811445A68A84E2A5B7B81E680A2596
SHA1:	75093AAF692DB42E672D4336BE348371EEAE1E05
SHA-256:	E37C9A430768AE2764E3D848539EFF67F4EF4998D34A136483BEA590F1419611
SHA-512:	EE56BCF898CAA83EA2B09223A810AD7811621AE0919430BE67AB48E03F7624AF2A36936FC24D4F466BEDE9D1073B9DD61CBE80BFC677CB3AECC581BB15C82C 99
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....._keyhttps://renderer-assets.typeform.com/modern-form.bd689b467237861b9ab3.js .https://typeform.com/...Y%./.....b..f.....2.J..>.....*#..O.*. A..Eo.....p.A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ab30d3a09b5f9af_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2608
Entropy (8bit):	5.98008253239516
Encrypted:	false
SSDEEP:	48:+Atz6bUrHxyxhTtBSurMPY6ryoAt+E5Q/sEqHg:70bUgptBnrMPYN01/ug
MD5:	B276A86FF5335B5A7060F6F553215FC2
SHA1:	4CC00140C629A7CF619D69B516DDAD188497C2A9
SHA-256:	96B5DAFDD024F49058AEE9719E2708761DDE2DF55C43D76B6F5913AAEFFFE5BF
SHA-512:	E57B3A9869DC610DFD13EE8D05AD72CB6D9F699974B68E12230147BEF0F1EFA9464158793683F938D4B71959C793D646539484142B81AFEEAD8D8E890F4E2B37
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...._keyhttps://www.typeform.com/_next/static/chunks/3503bcfd5d0f9a2632fdc11c7503e3f9d7448623.2143d960dc527413dea7.js .https://typeform.com/. .F[%./.....o'.p.O...z_.?~..K.....k? .A..Eo.....w.....A..Eo.....F[%./.....'.XM....O.....(S.l..`.....$L`.....Qc.....window... .Q.`.....webpackJsonp_N_E..Qb*.....push.....`.....L`.....`.....Ma.....`.....a.....Qb.g.'....s/UrC.(S.....Pd.....push.s/Ur...aQ....L.....q.....@.....@ .....@.....@.....@.....@.....@...".@.".0..@.0.2..@.2.@..@.@.@....@.S..@.S....&@.....@.....@.....@.".....0.i.....*....e..... ...|j.....@. .....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@....(.....d.....@.*(....d.....@.(.... .f.....@.....@.**.... .f.....@...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bbba9d520641b16_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2408
Entropy (8bit):	5.677364332241554
Encrypted:	false
SSDEEP:	48:AzhBWEehgguyNFJ0chBtcei0cbMKiCuHhY7c/8NCdA5t9:AznWLx1/nH7fKirhL/GCd69
MD5:	6D3CDD58B58BF706048CF1045E35CB55
SHA1:	062500217CD9D7C3BE840EC89166DC52A338C440
SHA-256:	ADB6E5FBEDC23A2C15F62077765C1FE59C919650A7E1D3675C7E07D9B9AB6C5A
SHA-512:	8C205045C6128A512EFF5EE0FE207D77C82E0B187DFAC562C67DE586E61566BABB1AE8E62D977333EBDC1F65A6C3CE83BD65F4C7B475F1F9BD2C1575FB0504 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....>9....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yV/r/cKYG5jgbj2D.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/|t.Z%./.....J4X..]..<`g+.....sV-L. M...^...A..Eo.....a.....A..Eo.....|t.Z%./.8.....'.....O.....D.....p.....(S....`.....4L`.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start _js....`.....M`.....Qc.|\P....dk1wF.....Qb>.....__d..,Qi.....WebCookieLocaleSelectorHandler.....`.....M`.....,QiR..C....CookieConsentDialogFalcoEvent.....Qdj.m.....IntlUtils.... Qf...O....createArrayFromMixed.(S.L.`R.... L`.....8Rc.....O.....a.....I`....Daf.....$Qgf.....blocking_cookie_banner.....a.....Qb._C.....initC.(S.....Pc.....a.in it..a....o....$..f.....d.....1...q..@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yV/r/cKYG5jgbj2D.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`T... D`.....d...`....&...&..!.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3dd0c8e84c33e5ab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40609
Entropy (8bit):	5.7712357110299
Encrypted:	false
SSDEEP:	768:otrg4WzfQgcOkxcAc4dAvazit/KZjdmjamARAlzWVnpiY9nXl8:yui/ckAvazs/KZj2a1uRWVnb9nV8
MD5:	BE28FBBD5901DF521DC444B999E84738
SHA1:	D794F388632D6BD1365CFDD19BC9BD02B8D4FC8E
SHA-256:	20007EEAA68B88152BC9D7830BF957EBE7102C16436BFB29B28BD843D8156D56
SHA-512:	1BC0DC78289A216391A84F20D041CB5AFD33FA80B48B21CFF4A2E32FA6AE92F14005F7F57ECCC65BBCA5C4F976856E3D27EFC9ED980E9FCF70DB4EE1E3B67 33
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....'b...._keyhttps://cdnjs.cloudflare.com/ajax/libs/rollbar.js/2.4.6/rollbar.min.js .https://typeform.com/v.G[%./.....6.....v.....kR.k%.<'w.3.`...JruU.b..i.A..Eo... .....A..Eo.....'.....O.....i.*~.....(S.....`.....L`<....(S.`.`x.... L`.....@Rc.....Qb.....t.....Qb.A.....e... ..Qb..c\....r...b$.....I`....Da.....(S...`.....L`.....QcV.....exports..$..a.....a....a.....Qb.....id..C..QcJH(.....loaded..H..q...QbN.%x....call.....K`....D}8.....&.%.*..... .&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da....<....a.....e..... P.....@....@.-....TP.A.....F...https://cdnjs.cloudflare .com/ajax/libs/rollbar.js/2.4.6/rollbar.min.js..a.....D`....D`....D`.....a....`,...&...&....&..!.&.(S.-...`.....8L`.....Qc.....window....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4063a03b0f6380ac_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	286
Entropy (8bit):	5.6046937808786135
Encrypted:	false
SSDEEP:	6:myrYj018IrAMUsc5zQcQQc/EMLAaM0qgih/ssgJfFcDK6t:lr1thUsywsMLAUq7rqN4
MD5:	0B8A8E04207BDD388DD07346E8FC2D60
SHA1:	817A0646317144 36A01CEC9EA1204A55E763959A
SHA-256:	193BE619BE696B8BB39219823F58B157A5A937D4FA2053EE84E6FF53D953BA57
SHA-512:	C118C1B5069D0BFCD7A4DBD02544FC856CE5712CB1B53D0DB44BFD600068E70627EF3B906D2F8EB5F12D947324E172DFB6B937DDB9A69071AC004CE8C0BF3 E
Malicious:	false
Reputation:	low
Preview:	0\r..m...../..(...._keyhttps://abs.twimg.com/responsive-web/client-web/shared~bundle.Compose~bundle.RichTextCompose~bundle.PlainTextCompose.c223ed85.js .ht tps://twitter.com/.*.Z%./.....5O..7|d|...;.y._.DFo...CvZA.D3.A..Eo.....y1D].....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\43c236b2b700a11c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	290
Entropy (8bit):	5.6486172019415966
Encrypted:	false
SSDEEP:	6:mvEYj018IrAMUscQQc0HNy1x6TZMBGFgZexKnk9k4JlbK6t:0w1thUsjUH56ex9kilN
MD5:	002D8827167D80A77C5FFD771EC37DDB
SHA1:	C5F5BC4C00337DD48DC328F49443093672767A93
SHA-256:	4CDCC66D62E30139B7D8CBDDAB251ED1C1F049EE27BE9E4EC6A56463F0A47456
SHA-512:	CF05B3AC3439C61F33A4D7D96CBD8F44ED884D246BEA314A33449ECE9B298E7EF8647B88E62801A825DA352271C283F72D3BBD0B10BEFDE15BDF8A188301E6 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~bundle.RichTextCompose~bundle.DMRichTextCompose~ondemand.RichText.d a96bfd5.js .https://twitter.com/q%.Z%./.....7.....[e...&..3A.....C.S.. o..\C....A..Eo.....j..k.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4676ba12e6de301b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.8560168025875035
Encrypted:	false
SSDEEP:	6:m1EYGL+MIwJJ+GG1ugmLFPm4wRK6tF8JVV2JMLFPm4E:uslwv+GbR8Pj7c8
MD5:	8B354CA0BEB1A67487D644BDBA74CF22

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4676ba12e6de301b_0	
SHA1:	80DF9AC26F83ED3ED69525631382EFA97A9A8F28
SHA-256:	494F301C126640BF126C7BABBACE37E55200707D29D780779DE7A1474991E370
SHA-512:	CCCE6FB0270E088518AEC2913C822C86C48A69DBF76947D2D72ADF590DA6DE8779FA88AC881010C119ADAF960CAAAE012D7FD4427C80CD5FDFFF8C6945556E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...U....._keyhttps://www.google-analytics.com/analytics.js .https://typeform.com/x..Z%./.....k.....`)7...>.6._.sf$.G..i.)...%.L.=.A..Eo.....A..Eo.....x..Z%./.....732130D86EE8ABF8C98155B67B74C0DE8362732BE66D6B208CE5EBB4C701EEEA`)7...>.6._.sf$.G..i.)...%.L.=.A..Eo.....E.]L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\47662fdbda55be63_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9952
Entropy (8bit):	5.5388774713623175
Encrypted:	false
SSDEEP:	192:1s1f4J4fctjStM0IwGEbOhTyiKq1hoCA7JAsYEGHzB8:qQhZIG5V8JPN
MD5:	9158DC38C3E1328A4C62BAFA043D179C
SHA1:	276910080905DC9BFA0DF2098152F25315240CC0
SHA-256:	C5C3854F8058451F03A4E97DDD35EBB180D438B5D4F0475DE95A3D4112A78154
SHA-512:	F778092F7A4D325D19E95AE7D95F95A8E72026BF8AA27F132191C927D0ED451E7467BACE72727922B8D06D86846EB04B5C2DC845E166D8AE30E11FCD3C2A6A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....._keyhttps://www.typeform.com/_next/static/chunks/b536aedf98901fb9a37b620c8ac87fff5fe747be.794682bf43ea45cdb3e4.js .https://typeform.com/.dG[%./.....&0..Q.!.K. i....U~.w6....A..Eo.....WU.....A..Eo.....'.....O....0%.....,.....(S.M...`N.....L`.....Qc.....window....Q.`.....webpackJsonp_N_E..Qb*.....push.....`.....L`.....`.....Ma.....`.....a.....Qb...c....+vXQC..Qb. ...../F7NC..Qb...1..../tXRC..Qb.^PE....0WpPC..Qb..{.....40oJC..Qb.~.....5ETAC..Qb..}`....5Qd4C..Qb"..L....7whZC..Qb.)r....A9a0C..Qb..K.....BRsNC..QbF.t.....BfU5C..Qbz.N.....BnagC..Qbf.....By1PC..Qb6.....C61uC..Qb.%.....CYMqC..Qb";.....ENu8C..Qb..?.....EbDIC..Qb.....FgkJC..Qb.[1B....GRewC..Qb.....GhSpC..Qb..!|....GrlXC..QbN.....IjbiC..Qbb_."....JRS9C..Qb^iy.....M5dzC..Qb6.....N4c9C..Qb.._.....Oa1hC..Qbv.hW....P2sYC..Qb>.....QbLZC..Qb.`.....RIqPC..Qb639.....S4vAC..Qb..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4da09bbce288333a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	379
Entropy (8bit):	6.0565689136853145
Encrypted:	false
SSDEEP:	6:mmll/6EYk+f2pomWihKVTzLMzhmJ2AFgdAhptTjbeZK6tmPyh0VMyaESS3hUtTj5:T/b++amzK5OkJrF9pleTk6GVM7xS3Ol
MD5:	8BE98DB071986BE980A1F18AABB87F3F
SHA1:	BD1BCD3334EB56487F827C321CD3B4840B8A65A2
SHA-256:	B40B91B41719124CB27280FA3D4481F8C97AF392DFD391814F17D10E45B91166
SHA-512:	970B8B0C1F37854113AF02A78147A5899CEEDC97A0EAFF41C6BDBDC1002004CEF432562679714BB6D0E012372C820369DBF3A766B46CCB01EB8E8B89D975308
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....OM....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3io9g4/yE/l/en_GB/IQ6TzhnCbxW.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...Z%./.....-..2v..5..b.'Z..*..}.....PK!.A..Eo.....(.....A..Eo.....Z%./.....5B8FD52BE7253E877E339D1787D47FC19644389FF83C94CD428F17DE06EDB88F-..2v..5..b.'Z..*..}...PK!.A..Eo.....jvL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4e9e7be729fbeec3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.508824130426089
Encrypted:	false
SSDEEP:	6:mUi/XYj018IrAcg0pMrtg7rH8ZEal+GgppY9/bK6t:pin1ttg0itIGGG
MD5:	1BAB032A88A2A0C5F57A9F1C536D16DA
SHA1:	FFF648D214180F702407806B627F8F9E44D04E7D
SHA-256:	A57B2964025D8936539D4DDDD3263C42C0E28CA6E05CD681808CD827904F762F
SHA-512:	37691D66ED784B2F7DC7B2515FDF8B05DDC32DCC17409984CC908B973AB5742A1126740AB8702AEDFECF175B3D54941E6A18CB2481870375FD9E1D343623D57
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k.....7...._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.IntentPrompt.a67fe455.js .https://twitter.com/dx.Z%./.....b...n..%.a..Q....i.7..cl...i$...A..Eo.....R.>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\508797177f1f805e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5048
Entropy (8bit):	5.943252983072014
Encrypted:	false
SSDEEP:	96:3YVEdEdQf4lUTT1D0oXIoK9CRDY2KbH8e4MR5XrbvwUDksvPcAWc:38EdJwlUTT1D0oEARsN/lvvwnUkC
MD5:	3DE4E851FA11318EB02FE240EC3C91EB
SHA1:	61B45F2CB8B926401039B2EBFD25DC0B08523F88
SHA-256:	E1D1CE711561F6E11C7E7A26B6CF7D7FBFF7836E702BCCEF0490CA281263F03A
SHA-512:	2697A37CCD0103198FE1F1C4FB96833CB214631FE48029CBD13D28716E7FCD9D11EA4B50ECD5E1651D8CCB354D48E289E46A8A9C1B49DE0EB727FDCB663510 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....a....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yU/r/WNPbD2XSPbr.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...Z%./.....M.....U.m.L...8".V..... .h.)....A..Eo.....z_.&.....A..Eo.....'.....O....(.....p.....(S.....`.....pL`4.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`.. ....M`.....Qc..5n....KuTXi.....Qb>.....__d..$Qg:2?H....AdsValidationIconType.....`.....M`.....Qb..v>....ix....QcZJ.....asset....(S..``....xL`8....t..a6.....Qcv.....ERROR...C..Qe .#.q....ERROR_REDESIGNEDC..Qe..a^....ERROR_GEODESIC..C..QdN.....ERROR_IMAGE.C..Qd.....ERROR_WHITE.C..Qdv..b....LARGE_IMAGE.C..Qd.3..... .MID_IMAGE...C..Qd.v?+....SMALL_IMAGE.C..Qc.[.....SUCCESS.C..Qe..q!....SUCCESS_IMAGE...C..Qc.B.....WARNING.C..Qd..o....WARNING_BIG.C..Qe>.K.....WAR NING_IMAGE...C..Qc.[.....22263.....Qc.:R.....1347204...!...Qc.}L.....1253191.....Qc.\.....22276.....Qc.[.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\51cb0f2b00a1e340_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7216
Entropy (8bit):	5.80460219099177
Encrypted:	false
SSDEEP:	192:7mt08U3xyQw+DjtZKAhMiMSAsvQJ6PPm8o2d2iIaS+CqY:7yjI4Q1tA4AsvjPPmTA2
MD5:	491863D1AB2790F84964BA83554FA398
SHA1:	C7937C7D32EBF32FD87DB6A54955AFBC505748F6
SHA-256:	98C6DDF8FA7D7DA41ED488C3AF30FC32C060EE7B5DBD69F560BD2BA5481D5BC1
SHA-512:	7499DAD05240CDD191BC659372F213C71C280243B7AC933DC01D271F3265A9FC6A2DD8A6B3C117CDEA7F41BBF89897FDD105840672836C5426D66C675E04E18
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....s...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y0/r/Rp16dPXRld4.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/h..Z%./.....Z.....F.V.Q.. ..O.$.R.n..!.Z.. ..X..A..Eo.....[ZH.....A..Eo.....'..3....O.....;.....0.....(S.....`.....L`R.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`..... .M`.....Qc.0.X....y0wcR.....Qb>.....__d...Qcj<=7....curry.....`.....M`.....(S.P.`V.....L`.....Qc.2.....exports...K`....Dn ...8.....&.]...&..&...&.]...&..&.[....&.&.%.-.....(Rc.... .....I`....Da...:.....c.....@.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/y0/r/Rp16dPXRld4.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`f...D`.....`....&. ..&....&.(S...`.....<L`.....8Rc.....O.a$.....I`....Da....@.....Qc...X....Toggler...Qd^b.>....subscribe.....`.....M`.....Qbv1.a....show..Qb.I.....hide.(S.....Ia.....I.....d.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\51f6903b9051e337_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	54031
Entropy (8bit):	5.72828505577187
Encrypted:	false
SSDEEP:	768:SO1PGFAZ88N85IyN3LazTJd3kbQf7aS/V5MwDux/pCjrNSBLRVl4vUzYA0Pv:7GFAZ8x5jN3uzNSjS/VoB89SBLR0vezy
MD5:	CC0D613EAD9779BFB10F860FAF5C6F45
SHA1:	649237F1DD7711D5D4FEB792E28A0F639903C711
SHA-256:	0AFF300F59DB867F9F941FF94F386DD01A6A4A50B7297195FD5D36488F92F887
SHA-512:	1D0DA2EFBB525F9DF23EC2CC7AF5FDE70CB636362860C2B33414A06ABEB9EA88AFED783F72B3814EEDB6D850154F1D1BA4C00C7A593EEC26F38A02DF0E357 9E1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o.....h....._keyhttps://public.profitwell.com/js/profitwell.js?auth=3e9cfb440db56df5e327e141de27a4f6 .https://typeform.com/).P[%./.....8.....Z.V..^B...?..... B...,...Z.X....A..Eo.....A..Eo.....'.....O....@....~.....t.....(.....(S.0..`.....L`.....(S.=..`.....L`N.....RcL..... .....Qb.....t.....Qb.A.....e.....Qb'*j.....n.....Qb..c\....r.....S...Qb...<....o.....QbZE.....s.....Qb.O=....l.....Qb.._2....h.....Qb.....f.....Qb>.{.....p.....Qb..1Z....d.....Qb.....m.....O. ..Qb2a.....x...n.....l`....Da....Pq...(S.....IaPd..Je.....d.....@.+..0.i.....@.....@.....@.*.....d.....@. .....@.-....`P. q.....T...https://public.profitwell.com/js/profitwell.js?auth=3e9cfb440db56df5e327e141de27a4f6a.....D`....D`6...D`.....U....`....&...&....&.(S..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5af3e76addb24ee8_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\5af3e76addb24ee8_0	
Size (bytes):	32408
Entropy (8bit):	5.817076010912362
Encrypted:	false
SSDEEP:	384:CKW5Qm8/8OjKa/f1kfKL8WKAFENZQXmP0/C9YZgZpM18zuS/VQPIIBkU9GpOvFh/:dF/xFdrFUEmPWCWZUprYjZ5XpxCLlA
MD5:	12F9A987EB0A8729BE1DCAC6C666A2FF
SHA1:	6CA5AA5A079F56AC69E7BFCFCF09803FA9E0236A
SHA-256:	B78C1355266454E779DE0AC740E26C22CB12886A8B630F0031F44E2C873EDFC4
SHA-512:	D3FBA884AA6E1A335BAE548FBA10FE1973B1713576A90C8649AF0A55AE01A31077E7BD55429A49568F766ECD8EB169CFECE9B7F9CB50C32FF131E5980E6DC1B9
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.typeform.com/_next/static/chunks/f6078781a05fe1bcb0902d23dbbb2662c8d200b3.5cbe69385ec32cbd615a.js .https://typeform.com/9.G[%./.....?.dB3:{~..&)...uT.5.H....N....A..Eo.....iy".....A..Eo.....'..\....O.....|..E.f.....t.....(S.-...`.....L`n.....Qc.....window....Q.`.....webpackJsonp_N_E..Qb*.....push.....`.....L`.....`.....Ma....&...`.....af.....Qb...../jkWC..Qb...Z....0BsmC..QbV.....3WeDC..QbJ.....6D7lC..Qb.cy.....7KCVC..Qb..B.....AroEC..Qb.Q.....PqPUC..Qb.L.....S3mdC..Qb&.....X24+C..Qbz.?.....YTqdC..Qb*9.....dZ6YC..Qb.....elygC..Qbf.S....g/15C..Qb..8.....ggucC..Qb.2.h....hS4mC..Qb.....kl55C..Qbf..k....mxvIC..Qb.....nOHtC..Qb.....pSHOC..Qb...{....q722C..Qb.....qOIgC..Qb.....qVT1C..Qb.....vJKnC..Qb.x7.....wkBGC..Qb2N.....zoAUC.(S.<.`4.....L`.....0Rc.....Qb"*j.....n...`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5b4c207083ca8268_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	5.6178158520489205
Encrypted:	false
SSDEEP:	6:mhYEfLcJJrmYeDWS4yKv3UGGPtFgaIgfNzchjoDK6t:If4vr4KxxEG8FhbNwa
MD5:	CB8EF53F95DEB78FE1EE44AA157A4599
SHA1:	7895A27D2603C5099C040D32D435A5CB106E703A
SHA-256:	EFB486983BDBAAB900E48293F545914FFDAE7C47872FC1F1046546697A52CC0D
SHA-512:	0404711314B41B292D7D35C037E9D494FFAC548A78AB3AB2F23606E4D84F2896EEA70596E6808CDEBC21CFDBCCFAF262F06E759F924675EBA9237D5C766231D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t...ie....._keyhttps://cdn.segment.com/analytics.js/v1/9at6spGDYXelHDdz4r0cP73b3wV1f0ri/analytics.min.js .https://typeform.com/}..Y%./.....l...../v...%]m*..0vi...$.+...^....A..Eo.....o.].....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5c7581f9c707e823_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	368
Entropy (8bit):	5.962656652496377
Encrypted:	false
SSDEEP:	6:m8vnYk+f2pomYHO5xzhmJ2hgttC1FLjH47K6tcDRxDhKLTnunk1FLjH4BU:TD++amYuXkJ4K8jHqkRxDhKLTnokfjHF
MD5:	C60CDB2FABB08E4B7DBA09C8E0B1A83C
SHA1:	1CF3A8A7F9D0055035042ED0932E80819C3ABEA6
SHA-256:	2B5F7C8171BF662E0ACCFF0B68EAF07F1E23CFBF6ECFC109F0D433EDF0534C58
SHA-512:	4575F18410BD8CD97B80F6D5592786F09DCDFAA886B002081AE6DE1FBAA4131F7BECD65A3075CF6072960DE7A04DD69DDAD9AEF9D6FA98CFBEF57B866DDE5B84
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...b....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/ye/r/bBkuQPoyW79.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/:..Z%./.....'.....e.a%....^.rL9..I..e..x.V..=.A..Eo.....$.~j.....A..Eo.....:..Z%./.8%..EFA9D4E168229CBFFF0639F08DACC17CDAD0A106AE17AAE0ABB4BCC31304FFBF.....e.a%....^.rL9..I..e..x.V..=.A..Eo.....8..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\606b26b45375e153_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4243
Entropy (8bit):	5.624307896896584
Encrypted:	false
SSDEEP:	96:hfhu/LflDtVB3+V0rnq9m4wmfv14b35vmGtYtkG:hfhQftDl+V0rnq9Km1m5OKG
MD5:	65BEA45B2C6BFA7A74F36832BB9E67DA
SHA1:	975D8715873C710CAEF923A414D33D8EFF3977FD
SHA-256:	F326C86FD348EE1E9E6644024801D6DBBD8C25FE295CE08F440839FC4ADB6265

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\606b26b45375e153_0	
SHA-512:	6FA13FDAF5E5E3ABE3DC025B2A1885FE2ED6736A26E8ADB27DDE8CEC6BEC879621CDECFFC6E99B7F24B0AE8E9598F1589183C7B7DA2AFB4D5249CDD4765C E6BF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....<....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iUjN4/yn/l/en_GB/LeGL-TZeQw2.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..s]%./.....S.....~.N U.%).z<I.L=..[.jmG.UTe..u..A..Eo.....a..M.....A..Eo.....s]%./.X.....'.....O.....(S...`.....4L`.....Qb.&.....self..Q.`.@W.....Caval ryLogger.....Qc.....start_js.....`.....M`.....Qc...n....4F5NG.....Qb.<....__d..$Qg.+.r....KeyboardShortcutToken.....`.....M`..... Qf.dj.....KeyEventController...(S.@.`8.....L`.....0R c.....O.`....I`....Da.....(S.....Ia.....D..n3.....d..... ...I.....@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iUjN4 /yn/l/en_GB/LeGL-TZeQw2.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`R...D`.....`T...&...&....&.....D&.(S...`.....L`N....8Rc.....S....O.a$.....I`....Da.....$.....ab.....Qc .z....._arbit

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\614139e555332f20_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.56161253799221
Encrypted:	false
SSDEEP:	6:mKYj018IrAMiGQMO1tgaezcEi1+4anK6t:r1tLiXReNjp
MD5:	86D29170155162B8F6D29AC131CE2E68
SHA1:	4167FB774D186D8122FD5349A8677FBD96FBA803
SHA-256:	0CCA4DE2D47B2A325B4F48964BFDE6709D66CC48080B3EC1DFF9C046A09A649E
SHA-512:	0464563F23964FFA812AAEE5AD645ABC0AE866B8B7C023240728AFED41C68D8EFCDEF53F6B772E8859F946F07169D92E466DE6BE88FD2A9DB37380C718797DF F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....._keyhttps://abs.twimg.com/responsive-web/client-web/vendors~main.fd096c95.js .https://twitter.com/.S.Z%./.....QS..224..m.....G..A ..Eo.....h.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\618edefdd9017502_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.529577972367014
Encrypted:	false
SSDEEP:	6:mxkXYj018IrAE8epMoLKFgZ/m0BJBdQnctbK6t:r1tgeIFY/LBPRtN
MD5:	D8BAFF6146008756464505C384418308
SHA1:	CC978B07BA30ADD41F4624BCCE3939A2CEB819EB
SHA-256:	B3AB59EC8E9D91995D4F44451A87DE50C2567ABA7AF9FA3BAE67D144FEFE2CAE
SHA-512:	3D747378786F31DEA91B2666FE0706861E272DA8FDDF6D5DEA333CE3223069CF1C8E087026139AE386828BC8BE24E696B775279B29E6D30C32F8A97DAC9038B4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....1.k...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.AppModules.390af3e5.js .https://twitter.com/oK.Z%./.....k.u.|..d.E02.\...i k.,.+ .$.>.3.A..Eo.....2.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6382582473ab2618_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	406
Entropy (8bit):	5.524077034079808
Encrypted:	false
SSDEEP:	6:mwEPYEKJTlVFGGRdgU2L5xrYd2RK6tWwEPYEKJTlVFGGrgUleL5xrYdGbK6t:doKJLFGQ6dYUnoKJLFGsidYE
MD5:	D85B4FFFE5E207BA07859BE379F20841
SHA1:	5BA9DAD4B5741CC2D822A802EE83B3D41F055AAF
SHA-256:	9649EE20FE18167871B0584E478D845BCA6D314248DC2DF7DD2C63EB5DD9B0C3
SHA-512:	267E8FD62BC940AE892BA995E4E80449A19DD6FBAEBE32AFCC162957E6CF7683D1A9ABA25CECA23EEE87EA1A09778829414803E31AB4F41D72DAFFDB145D07 7C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G....o....._keyhttps://cdn.optimizely.com/js/16131550068.js .https://typeform.com/.l[%./.....N.....d.C.dm..!.L....U.....]J..A..Eo.....].....A..Eo.....0\r. .m.....G....o....._keyhttps://cdn.optimizely.com/js/16131550068.js .https://typeform.com/..[%./.....~*.....d.C.dm..!.L....U.....]J..A..Eo.....B.=u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\67537b0d7c8393c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.651957016834427
Encrypted:	false
SSDEEP:	6:mEPYk+f2pomDuXGXy4zhmJ23igTOgtlU8q4PsG4K4TdK6t:J++amDJzkJiiurqK43
MD5:	B56D040596488977E46139FE9E7C3FB4
SHA1:	D9F1BD11FAFF8204381C248FCB7B13003552D252
SHA-256:	C7D2FDC4ACEF1EFC2C2C4D879099F7B18B04E51C5900BAEBD7CF18CEB75B4955
SHA-512:	CD8C95762C84BBEA75613E66DC00D30AF9A9D8D1485584603D6B133B5D5C91518E886A4DCC9CEE462E345D8E890CB7A9B47C16DD01C91BC4BC1EED696E9AF E3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....3EG...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yG/r/PryRG-VngUg.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.B.]%./.....6.....q.-#%....y~k.o..''.. .h.l.v.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6a2cf1a3d566dd90_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	30587
Entropy (8bit):	6.156221493461877
Encrypted:	false
SSDEEP:	384:seMlIDe0Zbd1USoysOtzU3rZalHJ+nrlpLE54DMT7Wx4xMEwS3tbWtmlEM05iG9i:sGDrd1gRcD+pp6v78UrwodlERJo
MD5:	0CAF8FBAC17A2137AC89CF7F0D3ECF50
SHA1:	C9F54B982F89F2E03D05E714AC9CAB06D4ADCE82
SHA-256:	9AA2BBB0C57FD54C0D65B6563816A00532A8ACBC39C67CE18C98936996EE25B2
SHA-512:	9E27AF4BEFE7B3948D2CB1869E73DBC5236AD50E94752BB24A1B10CE59ED5BD53253D2DB28996D7B74F49A574EBEA856AF4D5039D8FF7A3D58C5DA60DCB79 C60
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i8jc4/yA/l/en_GB/2596_8UTwmn.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..s]%./.....V.....Ps}.D.....hw Y.....*..olr.....A..Eo.....R.....A..Eo.....'.....O.....u....1.....0.....(S.i...`.....U.L`.....Qb.&.....self..Q.`.@W.....CavalryLogg er.....Qc.....start_js.....`.....M`.....QcZ.....pXZHP.....Qb.<.....__d..8Ql..{.,...ReactComposerNestedActionDispatchTypedLogger...`.....M`.....QcJ.....Banzai... Qf".(j.. ..GeneratedLoggerUtils..Qd...F....nullthrows...(S.D.`D.....L`.....0Rc.....O.`....I`....DaV.....(S.....Ia....'....T..sH.....@.....@.....@.....@.....@.....@.....@.. ....@.....@..I..!..@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3i8jc4/yA/l/en_GB/2596_8UTwmn.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`D...D`.....`....&...&....&.....D&. (S....`.....DL`.....Rc@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6d4e90c1ebbfcf5d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	68592
Entropy (8bit):	6.1527016534953995
Encrypted:	false
SSDEEP:	1536:J1RRVyqKv5kkacBJTcXSM6BG24KlBK2GdakZnN6:AqKxxBblcvdakH6
MD5:	5521D52499D83EBE11A42B5175C74023
SHA1:	8E6E4CDF4AA7BD3BCA93486A8D69385237FFEE99
SHA-256:	B49918A19AE20D71C8F08B9A2218F66754381F938D04836F8A66D5CAE2D8C6D3
SHA-512:	334101A39CF717CEAF1D4B31ECEC4E6E75C11F82AEF23DBC936024B76FC34AE330930B374CD3874588725DD5D8D0182361F1030A44072FC2368EE2E75219A91
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...P.sJ....175EA989576D48C4A902DDDB944F7E098EA5294E01EB8BCADEB05B2D298BE598.....'..9....O.....Z..... ...`.....(.....(S.Y...`j.....L`r.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`.....M`.....Qc".....HY2C6.....Qb>.....__d...Qe.`. ....NullBu sinessID...(S.0.`.....L`..... Qf*.@.....personal-business.....Qc.2.....exports...K`....Df....8.....&.%.-.....(Rc.....I`....Da....".....b.....@.-....dP.....X...https:/ /static.xx.fbcdn.net/rsrc.php/v3irQL4/y9/l/en_GB/EPq8xrc6Uk8.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`B...D`.....u....`6...&...&...,&.(S.D.`D.....L`.....0Rc.....O.`.... I`....Da.....(S.....Ia.....A.....@.... ..@.....@.....@.....@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\715089b76a7507ad_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	637
Entropy (8bit):	5.387231258369863

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\715089b76a7507ad_0	
Encrypted:	false
SSDEEP:	12:eyDQLH6kGFhhykPpoMKl0xXc8HNC1Ngw97wekYzU2FSD6/Za:eykShQklxXc8tCTIYzUVP
MD5:	29546FC04129EAE86E530F17B6BDB398
SHA1:	002EECCCA6BF7F31504503117A808A8AE7B2578D
SHA-256:	CBB0F06E77A573FB4AA8C412BD6CEE61212E4C15E3F36749A82E84FB360D9149
SHA-512:	25B890AFB71FD043B6739CE4963732A3FBA0308F2C0C43417F4579A4FA1AF99BB2A7E34B69EF1725A425584A1B2DA220F4073FAF44F8B41D4A3D53D273FF44AA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....=k....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/b2-7087f0/ea-1a640b/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/50-f1e180?ver=2.0&iife=1 .https://microsoft.com/..>\%./.....L.....h4'....:..<`yt.....,!...j0...@..A..Eo.....a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\77c4908df82ba25a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16697
Entropy (8bit):	5.985276877087924
Encrypted:	false
SSDEEP:	384:0pnMrB3+AlyAJ3L9R2S6oWPKgmVOL/Vfa:0yl3XJ39kRa
MD5:	A86C172731E9689538C92EE49341DB5A
SHA1:	65162201D2700BC16FBD2E8E2966A36A3699B483
SHA-256:	84ABC3D521708B8426E9B2924252D62ABE0FB5EB66B060568931C92D92AAF049
SHA-512:	75A23C35D48BB44E59406F3E997471ECBE0CFA8549514BF63F986C3C917170CDAB009E21A632D251B394F40D7F1C1C802112D6EAC0803F579AC31B2D71C7170
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q.....h....._keyhttps://cdn.cookielaw.org/scripttemplates/otSDKStub.js .https://typeform.com/{.E[%./.....y.....u..9.....fN.....2.v|....A..Eo.....y.....A..Eo.....'..3....O.....?....r!.....t.....(S.@..`<.....L`.....L`.....Qdfx.....OneTrustStub.(S....`v.....L`|....0Rc.....Qb^..g....l...`....I`....Da2...tg...(S...`.....|L`:....8Rc.....Qb.....c...a.....S.`....Da\B...g.....Qc.k.r....iabType...Qd.....iabTypeAdded..Qd.6.Z....crossOrigin...Qc.....isAmp.....QcB.$....domainId.(S..... Qf.....addBannerSDKScript..a.!...'.....d.....J.J..@..@..I.....@.-....DP.....6...https://cdn.cookielaw.org/scripttemplates/otSDKStub.js..a.....D`....D`....D`.....`j...&...&....&.(S....`.....L`<.....Qe..}.....OptanonConsent... Qf6.....optanonCookieName.... Qf...<....optanonHtmlGroupData..Qe.....optanonHostData...Qe.")3....gen VendorsData..I..QeB..9.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\781980b07f1bb38f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.673922076826899
Encrypted:	false
SSDEEP:	6:mql9YiRDHwA7qYsDpNdNFvNgDeugBhoR0QK4RnK6t:RTDHXqn/xNgDPEhFQX
MD5:	2E5CA5005643F88030515D1D27D44619
SHA1:	A16496C565DE8718A29D1D0D9612F6AB5ACA62D9
SHA-256:	3714EC0736E593ECEAAAAFC8289BE059FA3F59AE38BEB5354AE10B7C08566A6B
SHA-512:	A46C8E07C2132E38517BBC07EAC93FB23DA3228FBD4A67396D4D5AF7E20713609F43B4B26858412D43A6F7423139E385630C612AB27BBB069A593BE39AB43626
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...0.v....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4 .https://microsoft.com/W.@\%./.....$N.....5...a.....S...s5.O..8O....F$.|3F.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\798a66ccbf5360cd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3267
Entropy (8bit):	5.8142046290279215
Encrypted:	false
SSDEEP:	48:BijJiMN9GCmXSUij4/o2ZrA/Mdb/JCJ82yf1fM0Z8rboOQhrK:Bs/4ls4/LjdzJCJ82AfM0Z8rb7
MD5:	0DB0117FAF0557145E8BB7DFAE138534
SHA1:	091AA45D01A54AB00E1C2105F241200D581527F0
SHA-256:	25C78698D2608940B6BECC618E7AFB9A7F134417E074F72394530D418A11A7A3
SHA-512:	1FE8A31A309AB5C75036264065363E9449BB8052062715009378453906489546DE333A00EC816E4DC9A1233E453DAA7BFBAF598F388B75DF59EA2EE35D0AB72
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\798a66ccbf5360cd_0	
Preview:	0\r..m.....s.....M...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3idxF4/y8/l/en_GB/YwXlwrrPSAG.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/Yv.Z%./.....\`.H.].=V%...M.s....'i...9...A..Eo.....|fl.....A..Eo.....Yv.Z%./.....'.....O....H....o.....D.....(S....`0....LL`".....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`.....M`.....Qc.6.....gBdI5.....Qb>....__d..(Qh.....XUIDialogCancelButton.react....`.....M`.....Qb.....fbt...Qc.....React....$Qg...s....XUIDialogButton.react....(S.\.`r.....L`.....@Rc.....O...Qbz..0....h...b$.....I`....Da&.....(S.....Ia..... ..f..... ....I..q..@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3idxF4/y8/l/en_GB/YwXlwrrPSAG.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`Z...D`.....I...`2...&...&....&.....D&.(S.@..`8.....L`.....0Rc.....O.`....I`....Da*.....(S.....Ia:.....,..i....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7bfe9e92ce3f3ce1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3352
Entropy (8bit):	5.568202367097812
Encrypted:	false
SSDEEP:	96:i/8ufGnwu4/NTS1DYCQiutN0/gX37/SNi8M/f10ht:iZfGwu41TUDSbtN0/gXr0i8M1+
MD5:	FED527C88EB3120F6CD120A67D062A00
SHA1:	DA1326B6F5CEB583F95C7982D2931E0CB5932D1D
SHA-256:	FA7ED5998F495F3D9FFF10F1580F65131B4882C9C3711D3FCFBCD020A48568A4
SHA-512:	78F1CEC05E1A8094B76E04FBD1D9580FFB137CC774A5844498789B5E0A75A20C883FD07ABCD3B0CADE489D31DDE02F1B8FFA0CCE9A48A81DDBBD463C9B714822
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:.G...._keyhttps://www.typeform.com/_next/static/chunks/6770615276bd5da6d0c72e0b9a6c4cc60237862a.23e7894a0300c926b249.js .https://typeform.com/..F[%./.....O....'.l!.....yO`.)..k..o.Xd.A..Eo.....c.8.....A..Eo.....F[%./.....'..A....O.....k..6.....(S....`.....L`V.....Qc.....window....Q.`.....webpackJsonp_N_E..Qb*.....push....`.....L`.....`.....Ma.....`.....aN.....Qb...b....0k5RC..Qb.>.L....7zquC..QbR.Rf....EImmC..Qb.n.`....IW5jC..Qb..7....Ir57C..Qb..B.....LGUTC..Qb..p.....LmNUC..Qb..5z....SqJuC..Qb.....Tzk4C..Qb.....U3kXC..Qbn-.....UVEWC..Qb..u.....VvHCC..Qb&1.\....WJ6wC..Qb.@a.....a+KiC..Qb.....bJbuC..Qb.u.....hj8oC..Qb.P.....i0cmC..Qb.).c....iifWC..Qb.12.....kCDfC.(S.....Pd.....push.0k5R...aP...c....$..g.....@.....@.....@.....E.@.-....|P.....m...https://www.typeform.com/_next/static/chunks/6770615276bd5da6d0c72e0b9a6c4cc60237862a.23

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d748ba4e1f95dcd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2727
Entropy (8bit):	5.860143920882394
Encrypted:	false
SSDEEP:	48:jH5AhcsWmzRvKCzDQuVjYCels0K7quoybdheYZs:72fvKCzcuKjxuoy3Ns
MD5:	841D52BB840EF67DBE77B7206F6B6D05
SHA1:	26A64484DC85D2F5B572434F9C4C4027BE064E29
SHA-256:	E0293BC1522E5B57900A2BB0492760CC31154E5D32D487D7096035F7294E35BD
SHA-512:	3D4BADF06DF7528ED35A0B4976BCA4F49FD5A6FB6454421D268544D6A81BDDAD6DBB06F87AA07DF4F7F111E8B6F2C1D4FFC0B1A81F0F8387ED550D4A3A82305
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....s{....._keyhttps://www.typeform.com/_next/static/chunks/webpack-eb080e3f091731f228fb.js .https://typeform.com/..F[%./.....6P7".~.H.....E.}.X....q.q.....A..Eo.....<.....A..Eo.....F[%./.x.....'.<....O....8.....$.....(S.4..`$.....L`.....(S....`.....lL`2....`Rc,.....Qb.A.....e.....Qb.....t.....Qb'*j.....n.....Qb...<....o.....R....Qb.O=.....l.....Qb>.{.....p...f$.....I`....Da.....(S.M..`P....(L`.....M.....Qeb_.....hasOwnProperty....QbN.%x....call..Qb*.....push..Qc..Tw....shift.....K`....D...x.....*..&...*..&...*..&..&.|.&.(...i...e%.*..&....&.(...&.(...&...&.Z.....)..&.%.*...(...&...&.%.*..&..*..&.Y.....&..0.. %.L"&..i.%..Qw.....#.&...B....#.4&....&.(...&.(..$&.(..&&.Z....(....&.%.*.*&.0..,%..&..B.....&.]...(..0..(..2&.X..4&.\.6....&.(...&.(..8&...&.%...|:&.Z....;..&.\.=....,Rc.....Qb..c\....r...`....Da....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\82f038845c12de11_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.626204544954405
Encrypted:	false
SSDEEP:	6:mZXtgEYj018IrAkj1QmM5nAltgM6ArCbMbK6t:qX/1t35Q9nAXeAEMN
MD5:	26BAED3CFBC67E0BA09462D9026EE959
SHA1:	A0E98AFC0A4CF2A54E3A5F679AA1669D7D096816
SHA-256:	53C7A8CE3C0EDF49463B526837BBBB1DE043F204368A37C3D2E7B86217A74D96
SHA-512:	E8C2874D0A40CD9D2BE59E56B1044948886FD684E5AEA19541C8B3BA2B45E9B4F8F6B7B6A2C38B6CD2AC53316D0B41786B5CC149E60D09D8DE5CF8A4AC8CA97
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...._|....._keyhttps://abs.twimg.com/responsive-web/client-web/i18n/en-GB.d38691c5.js .https://twitter.com/...Z%./.....W.(.,e...9....>(SC.(4.[...H...A..Eo.....\J.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8422562e17d84495_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12736
Entropy (8bit):	5.809098479680676
Encrypted:	false
SSDEEP:	192:HXJgz4rJRL7meNJiJDT9Hcw626EYt4vb4sb7Csp0aYzJRTB7/HpopS:HXJUuRnLLih5HcwvbTbRp09DR/oS
MD5:	184AC0F6A16A24E44986AA64A25AB774
SHA1:	73C80C11B6FF68032229A386C86234A6A6C67566
SHA-256:	5FE7FB0CC41A1341EA9B2877956ED2C51CBF0C88B6D181965713BE79F9D2B9CC
SHA-512:	2449B71FD5B79C68B65C85C847DF675B9C66AA1666383F94B7DA9D42CF493BD71F6DE33FC411FD2D2F4ECB0D50B4533E24F539E5938A9B2029AEC60078778A7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....,....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y8/r/v-R2pLq3QHO.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...Z%./.....T.....YZ0.aq.]....L..P..v?.... rr....o.A..Eo....."..A.....A..Eo.....'.k$....O....(0..V.....|.....(S....`.....L`z.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js .....`.....M`.....Qc.y.r....KurNM.....Qb>....._d..,Qir-.....CookieConsentBlacklistedHrefs....(S.,.`.....L`.....a.....Qc.....hrefs.....`.....0M`.....Qe..",..../about/basics.... Qf.{ z...../privacy/explanation..Qe.4...../ads/settings....$Qg"|...../help/111814505650678....$Qg2w...../help/1561485474074139...$QgN...../help/568137493302217....$QgV... .../help/769828729705201.....Qe...]..../help/cookies.... Qf~.N...../policies/cookies.....Qe...../policy/cookies...Qc.2.....exports...K`....De....8.....}...-.....(Rc.....I `....Da.....b.....S....@.-.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\849c3de6865d8565_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	410
Entropy (8bit):	5.440379103315483
Encrypted:	false
SSDEEP:	6:mEanYiMs8pMu1tgSj8IcNupgLr/nK6tWEanYiMs8pMjgN1j8IcNupgLryK6t:Mr+HLgIc8pOpGrzegIc8pT
MD5:	D6D33EA8790390AD0E921A50DC1956FE
SHA1:	F851625FFD4D202CE0CCDE94B772FBF14D0C0D93
SHA-256:	9D267D91099EFD80F89BB6144CAAC5A79AC70BECF036C093A5ADEDC142069CB6
SHA-512:	E0CAE28721FF40FAC00323D744A84978FD9A7EF24AF6115A7852CBA4A034CD600FB994D7EA88E0C721F66C646C2C3F932BD478C6FFB696DE22AC5D69DC59B8 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....._keyhttps://twitter.com/i/js_inst?c_name=ui_metrics .https://twitter.com/80.Z%./.....D...L...9..g.....-...m...oN.B.A..Eo.....B.T.....A..Eo..... ...0\r..m.....I....._keyhttps://twitter.com/i/js_inst?c_name=ui_metrics .https://twitter.com/(..Z%./.....I.....D...L...9..g.....-...m...oN.B.A..Eo.....+V.(.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8656f0c7fb41eeca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13763
Entropy (8bit):	5.911965336798771
Encrypted:	false
SSDEEP:	192:LAXlhAA+VvefeYAbLlwUFSfjtRPhHhsC9cb+nZnrlarzCP4D+8WXPK6L9:LAfAA+VQURwIaPB9cb01rNDx
MD5:	284BB92DEB177B23B625DAE7D185B27D
SHA1:	70BE79564CB51B04776271ECC2E11A4C5EF2F568
SHA-256:	0AFF1321D89D13DDC9D875C86BB44F21510098D3241A5E91A62161882CAA34D7
SHA-512:	4CF73165A59CEFCC1F25BA69A8C53F342CCD4710C1206AE91E2C17BB5D5B1FD5CC2AD559B922A60BAE26AEB2941A8D6C7F031FC3CED80A0DAB8AAD50B7EE B697
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....l...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ig1H4/yf/l/en_GB/bPadyj-38Rr.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.u.Z%./.....a].....j...h y].....'*..9y3o...A..Eo.....A..Eo.....'.IQ....O.... 4....2.....X.....(S.....`.....L`j.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3... ..start_js.....`.....M`.....Qc2.f.....nzusw.....Qb>....._d..$Qg...s....XUIDialogButton.react.....`.....M`.....Qb.6~.....cx....Qc.....React.....Qe...X....XUIButton.react...QdV.k... ..joinClasses..(S.X.`j.....L`.....8Rc.....O...Qbz..0....h...a.....I`....Da(.....(S....Ia..... ..f..... ....I..Q..@.-....dP.....X...https://static.xx.fbcdn.net/rs rc.php/v3ig1H4/yf/l/en_GB/bPadyj-38Rr.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`V...D`.....)....`....&...&....&..q..D&.(S....`.....8L`.....@Rc.....1....O....S.b.....I`....Dav. ..""....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8658bb449015c5cb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	242

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8658bb449015c5cb_0	
Entropy (8bit):	5.535162406889039
Encrypted:	false
SSDEEP:	6:mT/gEYj018IrAKGes5/vpMZugr4bv5F9LBllZK6t:81tp458uuIvbpT1
MD5:	8B15798EE1C0CAF0E7D125E1E155BE9C
SHA1:	9C747A0EA022B405BA1F9AFB48AD8F406C27D1DD
SHA-256:	170F596109A44D27554223CFA2986B478C632DAE02B26B13EE7085E7EEB37754
SHA-512:	36DAFEED920CCC5F1A1286944CC382876A85CA70CE4244AF64CEC3390E241DA0CA5885FDE132316A020D970CE14E84AA0637B2012D27FDF48C43D19B393BBA8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n...c..j...._keyhttps://abs.twimg.com/responsive-web/client-web/bundle.NetworkInstrument.8cd49fb5.js .https://twitter.com/G..Z%./.....P.....)..X.q..{.....f t.S1..... 4.A..Eo.....n}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8677d6036394824b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	376
Entropy (8bit):	5.964028905313561
Encrypted:	false
SSDEEP:	6:myUnYGLhG5k08FygUGGNdTug0CnqjrYHzbK6t7sR0W8ptSB9jFAYlSPbnqjrYil:iickpGSdi7CnqfShsRYtS5/wPbnqfB
MD5:	F8084F437C02F2B72D74E1018484E362
SHA1:	EA47B335A12CA9151F39C2840FE8EC5C677BC271
SHA-256:	A52BD86CF0F3D26281CC0BCE1A1C824F53BAF1E85F7DF6FB88836DD5A2048952
SHA-512:	DF70659E526FD99C5BD921CAD950B4AEB51306FEA5CD5EDB9E7B7BF1359E9CA808219FF79D4A53658D07BC3B99A741284DFBE87F81E3A464FB582A753BE6E98F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....=....._keyhttps://www.typeform.com/_next/static/chunks/pages/front-page-004159675a09fbf6e6f4.js .https://typeform.com/.CG[%./.....`..d.@({MK...../uv.O..B.....e...A..Eo.....=.....A..Eo.....CG[%./.....18FD3140031F3A456438F9B5D54F48F30AD826F3494DCF9D0E7ED91A0EA5C7B7`..d.@({MK. ..../uv.O..B.....e...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8995dfb6624f2499_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	26723
Entropy (8bit):	5.810503529016172
Encrypted:	false
SSDEEP:	384:JHyHIMSPzNtqAn1El4Y/kmXEneJxz/R1yu/FHO0/dn7A5tyfS0cJDb:JS/SRQl114Y/kxeJxHhHl7GCo
MD5:	0E2618A7469BC8F40C007F5CF2E45FCA
SHA1:	D730DC551EB0A915CA0189CCBDC8C04AEEDBB508
SHA-256:	2488025C74868F67A737D618D474F26114CF8CA51608653BA31071879661DAB9
SHA-512:	73EB111F2A256010B8FE82171016ECBA82AA7F233D239F460144AF93845E40CDB0FAB7C3F05A10D014BDBA6A2564DB3C7B68DFD8B8F3927D120863E2061D98F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...W@....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iYXl4/yz/l/en_GB/bOtHsRxDkOf.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...Z%./.....a.....E R.....9...@%..a:..b8.xGP}!gw.A..Eo.....})..... A..Eo.....'.....O.....f.....(S.u...`.....m.L`.....Qb.H}Z....self..Q.`^.{e.. ..CavalryLogger.....Qcz$3.....start_js.....`.....M`.....Qc.....vXvTg.....Qb>.....__d.. Qf..`.....ResetScrollOnUnload....`.....M`.....Qb.].....Run..(S.H.`F.....L`.....0Rc..... .....O.`....I`....Da.....(S.....Ia.....d.....M...a..@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iYXl4/yz/l/en_GB/bOtHsRxDkOf.js?_nc_x=Ij3Wp8lg5K za.....D`....D`:...D`.....`N...&...&..1.&..!.D&.(S.....Ia....u.....d..... .....Qb.9.....c.....q.d.....D&.(S.d..`.....$L`..... Qf.....jsExtraRouteBuilder..(Qh..I...../ajax/ autoset_timezon

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8dae72a65858ac42_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8888
Entropy (8bit):	5.8976181628234325
Encrypted:	false
SSDEEP:	192:p8EvgahAWx778nqkZh0cg8m7zw9C0UirODTU:p8KgWdkZOcgDwARirSU
MD5:	96B7B1CA4C4355B076435288EAC39B3A
SHA1:	20D0391E714D4A52F4A293A562A3CE55A6288DDB
SHA-256:	97AE5DEDAEA59995E2F9E783C7C13036239B5195738677368A2CD65F541C422C
SHA-512:	078059AFF19CDABD7D1A1691A577478614735D31FAF6F62CF5580445AFC0CCD35ED11397E6B61AE71F5B7FD7F3E637C64336E8E4AA9E9B212E090C348803518

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8dae72a65858ac42_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m......h...l......._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yr/r/51t-ENp6yHv.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...Z%./.............P.........u..j......F.1E......h........A.. Eo.......Z..........A..Eo................................'..m....O....(!..5~.......................................(S.1...`.....|L`:.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`......M`...... Qcn}....../ipQK.....Qb>.......__d.. Qf........FeedBlacklistButton....`......M`......Q.@........Arbiter...Qc.?.....Event....(S.P.`X.... L`.....8Rc..................O......a........I`....Da....j....$.. a..........Qd.c......BLACKLIST.....Qe........feed_blacklist....Qd.d......UNBLACKLIST...Qe..sf....feed_unblacklist..Qb._C.....initC.(S.......Pc........g.init..a.........,.i........................... ....A...1..@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yr/r/51t-ENp6yHv.js?_nc_x=Ij3Wp8lg5Kz...a........D`....D`d...D`.....Y....`(...&...&....&.....D&.(S.H..`F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8e45b4e4dc728c42_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5336
Entropy (8bit):	5.824790986988809
Encrypted:	false
SSDEEP:	96:5GsbJqEm56q6fyMLhua36LBMvlOEmXiVQ165twBivda2W/0d:5GsIzJ6ffhuaKWvI7ymSWy
MD5:	CAD39A3094B9FB75A1A5F73C7449BFD4
SHA1:	7A9C4041A3D203ABE74C6BE1AEB7D1935D32016D
SHA-256:	A99F38B23E30589E97CD5CEE9C11DC9A19ADA7CE865B1BAF35A8CDE55BE1BBD4
SHA-512:	07463F81FD4159668C7CEEFCD93070E9A411AB518612DDFF774FF46ED5FA2EA3A8F963CBE98A5FC5EF634EA28E7A7B0E971BF2DA978340458054FB5097980A1
Malicious:	false
Reputation:	low
Preview:	0\r..m......h...X......_keyhttps://www.typeform.com/_next/static/chunks/05d954cf.01e8d901e2813d632096.js .https://typeform.com/..F[%./.....................x.W..\.....YyT; #q=e.y.5...nPv..A..Eo.......=...........A..Eo................................'.......O....H...(S.l..`.....$L`......Qc.......window....Q.`........webpackJsonp_N_E..Qb*... ...push.....`......L`.......`......Ma....(...`........a..........Qb...f....ZMKuC.(S.......Pd........push.ZMKu...aO............Q.I...+......"..@.".#..@.#.#..@.$.$..@.$.$..@.$.$..@.%.0..@.0.1 ..@.2.2..@.2.2..@.2.3..@.3.4..@.7.7..@.8.8..@.8.9..@.9.:..@.:.:..@.:.;..@.;.;..@.;.;..@.<.<..@.<.<..@.<.<..@.=.=..@.=.>..@.>.>..@.>.?..@.@.A..@.A.C..@.C.C..@.C. D..@.E.E..@.E.F..@.F.H..@.H.M..@.M.R..@.R.T..@.T...4@.......@.......@.......@.......@........@.......@.......@.......@........@.......@.......@........@.......@......@......@...... .@.......@........@......@........@........@.......@.......@...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3c2e2c260a7099_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.312922009325342
Encrypted:	false
SSDEEP:	3:m+lSd7ta8RzY/VW4McTtRAJOIGQHLRSVNRFYtRn5A2+//lHC2u3MWUBl0iPy2wdI:mXYI4McTDsJegDn5igU1TrlEKhK6t
MD5:	0C36BA5971E3C0CFACA29AE049981915
SHA1:	5EC5701B19413E958D476CFD2DD8511F7F5CBF97
SHA-256:	ADA833BAD1A15005895C298237EDF3422925DF21B26CFA1D97A343D8940F6262
SHA-512:	FBA20AE9E4E25BD832D24DE3D8EA2FA8780520727996033C5A5A125AD5FEE868A6DAEC06F0397300A53E72F5EF31BDF286AE9859A5D0470E8231F31942A606B B
Malicious:	false
Reputation:	low
Preview:	0\r..m......V...|.L\...._keyhttps://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js .https://microsoft.com/..?\%./.............L..........<.S....l....*.W.U\..E?`..r.A..Eo......l......... ..A..Eo..................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\921a520646898d46_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.664688544643954
Encrypted:	false
SSDEEP:	6:mGYiRDHwA7nXDjSQ1rdrDtfMDFgnku5BYQ4bftnK6t:tDHXzuQ3WDFsku5BYZxp
MD5:	DB248AB29E309783C424BEE101805E25
SHA1:	79C2FC4F49AE11C63482E213AD872B05A30FAAFD
SHA-256:	DDFE55513C80A6F25CD424961FABB1EBD153F081945493598E33C41A38D1B266
SHA-512:	90521CE24A03E9ECAF63BC205728ACE9896E2DF546847ED8443EEEE781D9DE66B87E824CF846E1D722AA02149B2DD1F84F437594E73669530E7C8176865AE8E
Malicious:	false
Reputation:	low
Preview:	0\r..m......x.........._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=42ce545a-d075-ac8e-38d1-8d9b4eaa1c7e .https://microsoft.com/...\%./.............^...... A.o.,.M#4.Y..<.iZ..m..M.`.Q..k'.A..Eo......!.W..........A..Eo..................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\97c84f1bdff57978_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.575459971760203
Encrypted:	false
SSDEEP:	6:mUwnYxRQ3GjXsXZR9kTGGLn+HgyY7mxYgiArFK6t:pwoQ3+sNkTGM+HrYieQf
MD5:	F860CF314A97BCFBAF647C0E57722C31
SHA1:	FF5FFCBC2A2B2290D3C42676092DD758DCC9635D
SHA-256:	8A9F3685D81005C93DF87767CE563C009647DD261C83B3CE56B8F9A93F0BA8DD
SHA-512:	818B353F70B21EDB61FFA956043635D9798DAB174CBD28CB9773E5663917845BDFE8A35921E9030AA11519C6AA0E190AA60EA5EFF905916AA52FC52772E92A0D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...~$&....._keyhttps://renderer-assets.typeform.com/modern-vendors~form.c2051b100945aea81c26.js .https://typeform.com/.'.Y%./....._MM.....] ....`./s.....CIo.Pi.s.A..Eo.....*,R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\980dfcb1a595e1f2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5712
Entropy (8bit):	5.513533187249949
Encrypted:	false
SSDEEP:	96:+7SEqHrd8GjrRrF+8TTFm4xWGDcCQ+jhH4tAFiGDLJHE/fSMeO:+7fKrd8GXR48TxmNGDcChjhHMAFiGFEJ
MD5:	99DDDEB37F05F0BBDE91790D30972878
SHA1:	74849F69EAEBCF581AFFE5BBAFEF729CF7EEE549
SHA-256:	8F210A15F6570DE2B6FC52BF450F3614B806137D77C8C99E6AE2370E0F84239D
SHA-512:	194DF3F0478080D3B9CF622FBC9B6DC0DFF0A418D6D6C25279B2E01F688F0EBE9C99B4CFFC5E1D0377821B0C285CC2C3ED74E71D8FAFCAEF0B0C49428A6C87E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v.P....._keyhttps://www.typeform.com/_next/static/chunks/f67ee6552dd8c9c5d13d330d8891d24bdf455da3.84b0a5aeee6e94591976.js .https://typeform.com/ .%H[%./.....8.....h.$.T@LX.\.F..$.....A..Eo.....IT.-.....A..Eo.....'..=....O.....,.....(S.u...`.....-.L`.....Qc.....window... .Q.`.....webpackJsonp_N_E..Qb*.....push.....`.....L`.....`.....Ma.....`.....a.....Qb...../JZeC..Qbzh.....7W2iC..Qb^.g^....8OQSC..QbV.....CSPPC..QbB.....D 8trC..Qbfu.*....DF/bC..QbR.r.....DTdtC..QbJp{O....Dbz9C..Qb...I....KC0HC..Qb..4.....NsbkC..QbV..-....PJYZC..Qb6.....QILmC..Qb*.+w....QLa3C..Qb.....S1F2C..Qb .um.....SYBZC..Qb.r....SaEtC..Qb..k.....SksOC..Qb.....VkANC..Qb...r....W8MJC..Qb..'T....YEIVC..Qb..L.....Zk/3C..Qb.._ ....a1guC..Qb..C.....b7vGC..Qb.....czaSC..Qb.... ....e5x7C..Qb.{.....gEJnC..Qb*L.m....hia/C..Qb..y.....io0TC..Qb..JT....lwsEC..Qb&..e....mbcPC..Qb..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99bd1e70f89aba87_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.582717278524531
Encrypted:	false
SSDEEP:	6:mYdYj018IrAzyvLCAspM/2Kvtg/5bUdyP4/EobK6t:FV1t/LCAVFAywPiBN
MD5:	46482C7FE75F0FC3FF78C38BD6E83D46
SHA1:	8EAF09DCEF0206A46EEBDB12AAC90CDFD0ECD3F6
SHA-256:	8806984C8CB3EE95E258D3E2172FC6627D6D6052954EB5E86519C6D0CA9E26E6
SHA-512:	4DF1E547E333B9F5BA8A4CFE58852527586F1D98B9300EB04A3291D2335D613915361343C50EC75D04C9CD92665F1680D54954C0A4413521D39F555102EB3EDB
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...U.,o...._keyhttps://abs.twimg.com/responsive-web/client-web/polyfills.18a65025.js .https://twitter.com/LQ.Z%./.....n.....:.....j._Q.).L.[V..y.#..a(H.6MI.A ..Eo.....!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b74ddb25b0808a2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	158840
Entropy (8bit):	6.073060828527778
Encrypted:	false
SSDEEP:	3072:o3rhPN91psIALW6AmoAZAAi0eTmMT7MQjS5p53J:o7J1p9gZAp0eTmc7MYS5B
MD5:	86CBF99B38A38333323892977FF92474

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b74ddb25b0808a2_0	
SHA1:	51DBD608A79DF1ADF744B500350B28F92BD531BD
SHA-256:	B875BA5C2056B5DC15164AB9C06BE804B2A6C6E203F0A3577CEB580C901248C7
SHA-512:	C47EE86EFB4D9C9551D3F9A8298345DD16A09C2A23BAB3C07C583B8B06F23B7D1D67AC8866F3013402714F8B0EE1B79FA8579F180BC9D339E69632FFC79192A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...oXj`....62C2A1BEB187BD41D2AE0467EC6E2017FCABDEF1D26F3DCC3A14EA9102FCB2A8.....'.H.....O3....j...n.....|.....T.....d.....P.....(S.....`.....E.L`.....Qc.....window....Q.`.....webpackJsonp_N_E..Qb*.....push.....`.....L`.....`.....Ma.....`.....`.....L`.....`.....@Mn..... .....&....9...a.....Qb..>M....+hRcC..Qb"@.....+x4dC..Qb.\...../CXEC`....C..Qb:.....0M26C..Qbn.....0nhoC..Qb&.o.....1TCzC..Qbf.....26GRC..QbrF.x....2hb/C..Qb*-4.....2qJxC..QbF=.K....3TWMC..Qb.up.....4jwJC..Qb. 7.....6Cs/C..Qbr.....6iWjC..QbJ.....6uIrC..Qb.....8B0SC..Qb~.5.....8BbgC..Qb. .\....8tprC..Qb..4J....A55RC..Qb^.QG....Ae27C..Qb...B....B3/pC..Qb..R....B5UdC..Qb.q.....Bu3cC..Qb...A....C5RTC..Qb.....CGyVC..Qbn.....DJU3C.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e483e6ac05655c7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9088
Entropy (8bit):	5.7235198518250545
Encrypted:	false
SSDEEP:	192:m/9bQh16vGVUSCN9a2lcQO8OvBxIErduEbEmYWWX+NJz:mJg6ebR2RErduE9YWdn
MD5:	2725DD20E0312538CA1BC9662B90306C
SHA1:	4B7689BA79BC627E6C7337E2B080D865AFB38F31
SHA-256:	9E1B920FDDC4B87FC84901269AB0C3C0CAD87A864EEC2B1A9C0D8F2A271C9A52
SHA-512:	8A6F02E7903ADFD5411ED61D8D42F79719CBC1163D6BB509B96AD89E1BBD56FC75DD3F59684790AD8752B74167A2D0F8E8CD61F3E3ADAA1091FA1D2B4B40042
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....)....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yu/r/SXjJMCvIgO9.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.m.Z%./.....V..:.....>qb.fU"..O...QXz....:S.A..Eo.....\8.....A..Eo.....'..'....O.....!...C.....(S.i...`.....L`D.....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`.....M`.....Qc...{....LmicE.....Qb>.....__d..$Qg..d@....XConsentCookieController...`.....M`.....QdZ..o....XController..(S.H.`F.....L`.....a...Qc.6w"....create....Qe...../cookie/consent/..Qc.2.....exports...K`....Dl(...8.....&.]...&.(...&...&.~&.Z.....-.....(Rc.....I`....Da....~.....c.....@.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yu/r/SXjJMCvIgO9.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`L...D`.....`....&...&....&.(S...`&....pL`4....`Rc,.....O.....Qbz..0....h.....S...Qbb.....j.....Qb...-....k.....QbZ!Wy....I..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9eb8d01121d07a87_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.46159486305846
Encrypted:	false
SSDEEP:	3:m+l8dHR/la8RzYj0KKKXlMMIrATQUMLA/BNC7lMRl/A2KF/lHCYg/NqXuKjbBNg0:m1Yj018IrAkhAQMXItFgYgQpvqnqK6t
MD5:	79465DF0BCE5835419DDC3DDA4E14CA5
SHA1:	78AE9EA9AE357286AE47DDFB0059A617960B9C0D
SHA-256:	9634E554852CD33F7FE726428D2750A44CDE281BF666D4606BB2F2204857B6BD
SHA-512:	E3E1870EC20B7A0F865AA6E36ABD3B88EABFF4425EC303A178751A443B8D64F97364200A8C6EE4755D1F3D2F35A6D28544CEF2ECE6A76F8BC55E8D5CF3DB1881
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j....8"....._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.emoji.en-GB.5e35eec5.js .https://twitter.com/w.)[%./.....j.....dO...{.H.....b.....Y/.|..Wi.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a148d5fe00cdc87d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2064
Entropy (8bit):	5.924685298828664
Encrypted:	false
SSDEEP:	48:dyxCB7KDq6+18en6Qnoyxv0ywJ+defxul/sElYDZ:8wYqAgLfa+dM4l/oZ
MD5:	C4743D72E6EB1B316C6FB1FA17B87FAE
SHA1:	8E1AEA704E4CD6633577BA792A32B30A4F31225C
SHA-256:	8731ACE093D90FCBE4F50B91A0746E08E4CBCAE94C2C2E47DF17AB8F39FC446B
SHA-512:	203639BE88E5689E81F653B92023F54F48544FAAC07377B23F844F42BA0AE013EB72795A0B387BFC6B2BA81677D3CD7F08F375C18DEF37DFB87E9EAAB978EC74
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a148d5fe00cdc87d_0	
Preview:	0\r..m.....wu...._keyhttps://www.typeform.com/_next/static/chunks/da7d6f2c1cb60259cb5602697fb99e51555843ec.fb18d74f73fb1ccf5100.js .https://typeform.com/ .EI[%./.....".....JTW8..v..c..DW=\.....,..iN.5.A..Eo.....P.....A..Eo.....EI[%./.....';!....O.....caa.....(S....`.....DL`.....Qc.....window.. ..Q.`.....webpackJsonp_N_E..Qb*.....push.....`.....L`.....`.....Ma....$...`.....4..a.....Qbz`u;....2qu3C..Qb".....a6RDC..Qb^r?9....gX9aC..Qb.....jwwSC..Qb.....yCM9C. (S.....Pd.....push.2qu3...aQ.....|j.....@.....@.....@.....@.....@.....@.....@...&..@.&.&..@.&.'..@.'.(..@.).)..@.).*..@.....H.p<.....@.....@.....@ .....@.....@.....@.....@.....@.3.....d.....@.....,i.....@.....@.....@."....@.....D.n3.....@.....@..."..@.#.$..@.$.%..@.%.%..@.%.&..@. ....d.....&.&..@.(.....d. .....*.*..@. . .....E.@.-....|P.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a1509c51f351ee1d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.524365593424256
Encrypted:	false
SSDEEP:	6:mDYj018IrAMUKmUhLiMCIXgD+vlp2W09whzryhK6t:m1thUKFXX92JOzm7
MD5:	F8DC30F1E418FB1A0A3C65FB806F41CA
SHA1:	2E75EB98EC3D9704FA516D6F6BA13698654CFD7F
SHA-256:	B1B170B6C517A048C20E5D8FEF47D1722D0E6863C47EB5F5874664B392707382
SHA-512:	9FC7BF6A8E14AC0472F9BC4AAF75E37C8C525B35B28E34C88FC18FD4C655F269085CCD4C3177F49C7AC7B4FF8C19F0FB46B650DE2EE1E39625FA964BA1FEEF 41
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`....pZ~...._keyhttps://abs.twimg.com/responsive-web/client-web/sharedCore.f32fe095.js .https://twitter.com/m..Z%./.....`...(../..#-s,.a...s...r.SR....A ..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a1d302bfacba25c9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	368
Entropy (8bit):	5.936409784524593
Encrypted:	false
SSDEEP:	6:monYk+f2pomC2hmJ2Bg6jw/nVmWK6th4up+gpE5OSqg/gHY2jw/nT:9D++amfkJkljiD4ukg6hqAgHvjy
MD5:	C2140A973F55EE1BC85B69A5BC2F36B7
SHA1:	2245D9128DE87126752D316CCBD1DD8A863A8374
SHA-256:	FFB0CB919A8193C0D0668CFAFC3228E3947F0E21D53D31BE1D5ADEF1950B1D34
SHA-512:	9966497F43BE033494D8819CCB2FFB8CEDB35FD8B372BAE093413A4C6E1BEBE614E40F3730EB05CDD7B94AB0077316D7FA9A1EE863FAB37968724467FA9AEC 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...q.ek...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y7/r/A2DXEAuiCb2.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/e.s]%./.....E.....m....8....a..w|..v..... .a.;."..A..Eo.....X.].....A..Eo.....e.s]%./..0..D942805D6128FED211860B5FF15C5F69950488F120F99DEE1CC1D66BA80B00BE.m....8....a..w|..v.....a.;."..A..Eo.. .....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a37dd3f3370e7a86_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8248
Entropy (8bit):	5.6900309778618325
Encrypted:	false
SSDEEP:	96:3PH1cr0KRPJ6I6XozP0GtrSkDTLDzaqlALMLahWKftmbRCX47/W/4yr4pL+BKBsJ:3feIKRfzP08Jz0La7Kf7X4zG4CaLqu6
MD5:	E133E6DF98C4BFCC1E216363E770CF61
SHA1:	8A267C1CC7F1F294D77F0439661BEDD10B133214
SHA-256:	9AE4B0F9CE5A1B4F636CAF232A75CBB8E07E89E8C05BCE23833CB96769B996EA
SHA-512:	F4E1339A396096E8347B15E22AB7B6204ADE42FB9568383CBA49F255C4B33316311922EA4D2DB4DC9C1752E88F175090C9830DD01EFDFA769A275D9FD2BEB04
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....$...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yu/r/jnuFTNJnMhL.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.Z%./.....k.....v..o...(.y...k...<._e... .^.....A..Eo.....c..O.....A..Eo.....'.,....O.....]n.....,.....(S....`.....`L`,....Qb.H}Z....self..Q.`^.{e....CavalryLogger.....Qcz$3.....start_js.....`.... ..M`.....QcB}.....ujL8/.....Qb>.....__d...Qe..N.....ArtillerySegment...`.....M`.....Qd.^.....invariant....$QgZ-.`....performanceAbsoluteNow...(S.H.`F.....L`.....HRc ..... ....O...Qbz..0....h.....S.c$.....I`....Da....z....(S.....Ia.....D..n3.....d.....%@..I.....@.-....\P.a.....M...https://static.xx.fbcdn.net /rsrc.php/v3/yu/r/jnuFTNJnMhL.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`p...D`.....`....&...&....&..!..D&.(S.D..`>.....L`.....8Rc.....a$.....I`....Da.....(S.

Static File Info

No static file info

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:44:05.816351891 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.816492081 CET	49733	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.832715034 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.832762003 CET	443	49733	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.832828999 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.832866907 CET	49733	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.833092928 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.833223104 CET	49733	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.849308014 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.849354982 CET	443	49733	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.849901915 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.849942923 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.849982977 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.850019932 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.850020885 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.850078106 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.852652073 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.853558064 CET	443	49733	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.853600025 CET	443	49733	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.853638887 CET	443	49733	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.853677988 CET	49733	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.860388041 CET	443	49733	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.860419989 CET	443	49733	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.860491991 CET	49733	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.892887115 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.893038988 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.893110037 CET	49733	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.893429041 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.893459082 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.909239054 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.909271955 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.909297943 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.909496069 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.909523964 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.909526110 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.910397053 CET	443	49733	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.910496950 CET	49733	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.920885086 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.920939922 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.920981884 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.921008110 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.921013117 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.921063900 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.921071053 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.921076059 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.921139002 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.922297001 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.922338009 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.922373056 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.922403097 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.922446012 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.922492027 CET	49732	443	192.168.2.4	13.224.93.102

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:44:05.922506094 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.922591925 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.922652960 CET	49732	443	192.168.2.4	13.224.93.102
Nov 20, 2020 20:44:05.926207066 CET	443	49732	13.224.93.102	192.168.2.4
Nov 20, 2020 20:44:05.998687983 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.015768051 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.015880108 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.016174078 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.032181978 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.032728910 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.032757998 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.032782078 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.032809973 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.032850981 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.032903910 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.034796000 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.067487955 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.067651033 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.067799091 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.083838940 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.083878040 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.083908081 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.083933115 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.084178925 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.084398985 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.084472895 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.084494114 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.084534883 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.084567070 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.084598064 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.084625006 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.084692955 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.084837914 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.084903002 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.084949017 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.085021019 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.084996939 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.085098028 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.085112095 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.085163116 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.085779905 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.085848093 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.085861921 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.085892916 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.085933924 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.085935116 CET	443	49735	13.224.93.45	192.168.2.4
Nov 20, 2020 20:44:06.085978031 CET	49735	443	192.168.2.4	13.224.93.45
Nov 20, 2020 20:44:06.086014986 CET	49735	443	192.168.2.4	13.224.93.45

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 20:44:04.931586981 CET	192.168.2.4	8.8.8.8	0x1df9	Standard query (0)	mcmms.typeform.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:05.777281046 CET	192.168.2.4	8.8.8.8	0xd4ae	Standard query (0)	images.typeform.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:05.959346056 CET	192.168.2.4	8.8.8.8	0xc8fc	Standard query (0)	renderer-assets.typeform.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:06.770226002 CET	192.168.2.4	8.8.8.8	0x923b	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:07.080126047 CET	192.168.2.4	8.8.8.8	0xabab	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:08.477832079 CET	192.168.2.4	8.8.8.8	0x6d0b	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 20:44:14.062242985 CET	192.168.2.4	8.8.8.8	0xd660	Standard query (0)	rfp.contemporarylivingconstructions.com.au	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:14.992850065 CET	192.168.2.4	8.8.8.8	0x6c68	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:15.134042025 CET	192.168.2.4	8.8.8.8	0x622c	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:15.134643078 CET	192.168.2.4	8.8.8.8	0xabc1	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:19.209022045 CET	192.168.2.4	8.8.8.8	0x71c2	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:19.361669064 CET	192.168.2.4	8.8.8.8	0x6c1d	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:20.120563984 CET	192.168.2.4	8.8.8.8	0x644b	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:22.082437038 CET	192.168.2.4	8.8.8.8	0x89f9	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.515733957 CET	192.168.2.4	8.8.8.8	0xcc48	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.824126005 CET	192.168.2.4	8.8.8.8	0x986c	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.827630997 CET	192.168.2.4	8.8.8.8	0xcf9d	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.827889919 CET	192.168.2.4	8.8.8.8	0x26e0	Standard query (0)	api.twitter.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.868757010 CET	192.168.2.4	8.8.8.8	0xe4d4	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.871481895 CET	192.168.2.4	8.8.8.8	0x33cc	Standard query (0)	video.twimg.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:27.226026058 CET	192.168.2.4	8.8.8.8	0x8b5e	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:27.778289080 CET	192.168.2.4	8.8.8.8	0x7529	Standard query (0)	static-exp3.licdn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:28.193368912 CET	192.168.2.4	8.8.8.8	0xd9e1	Standard query (0)	platform.linkedin.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:29.955764055 CET	192.168.2.4	8.8.8.8	0x973b	Standard query (0)	static-exp3.licdn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:31.550523996 CET	192.168.2.4	8.8.8.8	0x2166	Standard query (0)	www.typeform.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.041277885 CET	192.168.2.4	8.8.8.8	0xfc20	Standard query (0)	font.typeform.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.043138981 CET	192.168.2.4	8.8.8.8	0xb938	Standard query (0)	cdn.optimizely.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.043787956 CET	192.168.2.4	8.8.8.8	0x11ab	Standard query (0)	cdn.cookielaw.org	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.100370884 CET	192.168.2.4	8.8.8.8	0x7cd8	Standard query (0)	polyfill.io	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.235654116 CET	192.168.2.4	8.8.8.8	0xfac9	Standard query (0)	public.profitwell.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.247647047 CET	192.168.2.4	8.8.8.8	0x9bdc	Standard query (0)	d3m6p8tvnbsibq.cloudfront.net	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.602149010 CET	192.168.2.4	8.8.8.8	0xfa29	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:33.676044941 CET	192.168.2.4	8.8.8.8	0x3bbb	Standard query (0)	cdn3.optimizely.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:33.687419891 CET	192.168.2.4	8.8.8.8	0x2457	Standard query (0)	a15381830540.cdn.optimizely.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:34.831968069 CET	192.168.2.4	8.8.8.8	0xbd4c	Standard query (0)	logx.optimizely.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:35.966883898 CET	192.168.2.4	8.8.8.8	0x611f	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:38.442848921 CET	192.168.2.4	8.8.8.8	0x8617	Standard query (0)	www.typeform.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.497885942 CET	192.168.2.4	8.8.8.8	0xad23	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.788768053 CET	192.168.2.4	8.8.8.8	0xdc93	Standard query (0)	lnkd.demdex.net	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:48.396456003 CET	192.168.2.4	8.8.8.8	0xa6eb	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:48.901648045 CET	192.168.2.4	8.8.8.8	0x103e	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 20:44:49.897526026 CET	192.168.2.4	8.8.8.8	0xc88b	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:49.919672966 CET	192.168.2.4	8.8.8.8	0x6102	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:52.639436007 CET	192.168.2.4	8.8.8.8	0x5a3a	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Nov 20, 2020 20:45:08.331770897 CET	192.168.2.4	8.8.8.8	0x9f5d	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:45:14.390566111 CET	192.168.2.4	8.8.8.8	0xfb64	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:45:14.503452063 CET	192.168.2.4	8.8.8.8	0xa2aa	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:45:18.312066078 CET	192.168.2.4	8.8.8.8	0x188e	Standard query (0)	pixel.facebook.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:44:04.986032963 CET	8.8.8.8	192.168.2.4	0x1df9	No error (0)	mcmms.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:05.815335035 CET	8.8.8.8	192.168.2.4	0xd4ae	No error (0)	images.typeform.com	d2nvsmtq2poimt.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:05.815335035 CET	8.8.8.8	192.168.2.4	0xd4ae	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.93.102	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:05.815335035 CET	8.8.8.8	192.168.2.4	0xd4ae	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.93.115	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:05.815335035 CET	8.8.8.8	192.168.2.4	0xd4ae	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.93.46	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:05.815335035 CET	8.8.8.8	192.168.2.4	0xd4ae	No error (0)	d2nvsmtq2poimt.cloudfront.net		13.224.93.75	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:05.997349024 CET	8.8.8.8	192.168.2.4	0xc8fc	No error (0)	renderer-assets.typeform.com	d2citsn5wf4j9j.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:05.997349024 CET	8.8.8.8	192.168.2.4	0xc8fc	No error (0)	d2citsn5wf4j9j.cloudfront.net		13.224.93.45	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:05.997349024 CET	8.8.8.8	192.168.2.4	0xc8fc	No error (0)	d2citsn5wf4j9j.cloudfront.net		13.224.93.60	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:05.997349024 CET	8.8.8.8	192.168.2.4	0xc8fc	No error (0)	d2citsn5wf4j9j.cloudfront.net		13.224.93.43	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:05.997349024 CET	8.8.8.8	192.168.2.4	0xc8fc	No error (0)	d2citsn5wf4j9j.cloudfront.net		13.224.93.116	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:06.808067083 CET	8.8.8.8	192.168.2.4	0x923b	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:06.808067083 CET	8.8.8.8	192.168.2.4	0x923b	No error (0)	d296je7bbdd650.cloudfront.net		13.224.100.80	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:07.107340097 CET	8.8.8.8	192.168.2.4	0xabab	No error (0)	api.segment.io		52.38.212.85	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:07.107340097 CET	8.8.8.8	192.168.2.4	0xabab	No error (0)	api.segment.io		35.160.159.121	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:07.107340097 CET	8.8.8.8	192.168.2.4	0xabab	No error (0)	api.segment.io		18.236.5.74	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:07.107340097 CET	8.8.8.8	192.168.2.4	0xabab	No error (0)	api.segment.io		50.112.221.239	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:07.107340097 CET	8.8.8.8	192.168.2.4	0xabab	No error (0)	api.segment.io		35.164.248.150	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:07.107340097 CET	8.8.8.8	192.168.2.4	0xabab	No error (0)	api.segment.io		52.38.215.191	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:44:07.107340097 CET	8.8.8.8	192.168.2.4	0xabab	No error (0)	api.segment.io		54.69.174.156	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:07.107340097 CET	8.8.8.8	192.168.2.4	0xabab	No error (0)	api.segment.io		54.70.109.173	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:08.521779060 CET	8.8.8.8	192.168.2.4	0x6d0b	No error (0)	clients2.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:08.521779060 CET	8.8.8.8	192.168.2.4	0x6d0b	No error (0)	googlehosted.l.googleusercontent.com		172.217.16.193	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:14.373841047 CET	8.8.8.8	192.168.2.4	0xd660	No error (0)	rfp.contemporarylivingconstructions.com.au		192.185.141.132	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:15.019954920 CET	8.8.8.8	192.168.2.4	0x6c68	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:15.019954920 CET	8.8.8.8	192.168.2.4	0x6c68	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:15.161642075 CET	8.8.8.8	192.168.2.4	0xabc1	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:15.173465014 CET	8.8.8.8	192.168.2.4	0x622c	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:15.173465014 CET	8.8.8.8	192.168.2.4	0x622c	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:19.244818926 CET	8.8.8.8	192.168.2.4	0x71c2	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:19.244818926 CET	8.8.8.8	192.168.2.4	0x71c2	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:19.397234917 CET	8.8.8.8	192.168.2.4	0x6c1d	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:19.397234917 CET	8.8.8.8	192.168.2.4	0x6c1d	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:20.147624969 CET	8.8.8.8	192.168.2.4	0x644b	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:20.147624969 CET	8.8.8.8	192.168.2.4	0x644b	No error (0)	scontent.xx.fbcdn.net		157.240.9.23	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:22.110302925 CET	8.8.8.8	192.168.2.4	0x89f9	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:22.110302925 CET	8.8.8.8	192.168.2.4	0x89f9	No error (0)	scontent.xx.fbcdn.net		157.240.9.23	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.542702913 CET	8.8.8.8	192.168.2.4	0xcc48	No error (0)	twitter.com		104.244.42.65	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.542702913 CET	8.8.8.8	192.168.2.4	0xcc48	No error (0)	twitter.com		104.244.42.193	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.854979992 CET	8.8.8.8	192.168.2.4	0x26e0	No error (0)	api.twitter.com	tpop-api.twitter.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:23.854979992 CET	8.8.8.8	192.168.2.4	0x26e0	No error (0)	tpop-api.twitter.com		104.244.42.2	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.854979992 CET	8.8.8.8	192.168.2.4	0x26e0	No error (0)	tpop-api.twitter.com		104.244.42.130	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.854979992 CET	8.8.8.8	192.168.2.4	0x26e0	No error (0)	tpop-api.twitter.com		104.244.42.194	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.854979992 CET	8.8.8.8	192.168.2.4	0x26e0	No error (0)	tpop-api.twitter.com		104.244.42.66	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:44:23.861582994 CET	8.8.8.8	192.168.2.4	0x986c	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:23.861582994 CET	8.8.8.8	192.168.2.4	0x986c	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.864619017 CET	8.8.8.8	192.168.2.4	0xcf9d	No error (0)	pbs.twimg.com	twimg.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:23.864619017 CET	8.8.8.8	192.168.2.4	0xcf9d	No error (0)	twimg.twitter.map.fastly.net		151.101.12.159	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.895807981 CET	8.8.8.8	192.168.2.4	0xe4d4	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.895807981 CET	8.8.8.8	192.168.2.4	0xe4d4	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.895807981 CET	8.8.8.8	192.168.2.4	0xe4d4	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.895807981 CET	8.8.8.8	192.168.2.4	0xe4d4	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:23.907083035 CET	8.8.8.8	192.168.2.4	0x33cc	No error (0)	video.twimg.com	cs296.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:23.907083035 CET	8.8.8.8	192.168.2.4	0x33cc	No error (0)	cs296.wpc.edgecastcdn.net	cs2-wpc.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:23.907083035 CET	8.8.8.8	192.168.2.4	0x33cc	No error (0)	cs2-wpc-eu.8315.ecdns.net	cs531.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:23.907083035 CET	8.8.8.8	192.168.2.4	0x33cc	No error (0)	cs531.wpc.edgecastcdn.net		192.229.220.133	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:27.252978086 CET	8.8.8.8	192.168.2.4	0x8b5e	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:27.816240072 CET	8.8.8.8	192.168.2.4	0x7529	No error (0)	static-exp3.licdn.com	2-01-2c3e-0069.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:28.232417107 CET	8.8.8.8	192.168.2.4	0xd9e1	No error (0)	platform.linkedin.com	2-01-2c3e-0055.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:29.995714903 CET	8.8.8.8	192.168.2.4	0x973b	No error (0)	static-exp3.licdn.com	2-01-2c3e-0069.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:31.590351105 CET	8.8.8.8	192.168.2.4	0x2166	No error (0)	www.typeform.com	d1l34lgko5ugnb.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:31.590351105 CET	8.8.8.8	192.168.2.4	0x2166	No error (0)	d1l34lgko5ugnb.cloudfront.net		13.224.93.121	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:31.590351105 CET	8.8.8.8	192.168.2.4	0x2166	No error (0)	d1l34lgko5ugnb.cloudfront.net		13.224.93.102	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:31.590351105 CET	8.8.8.8	192.168.2.4	0x2166	No error (0)	d1l34lgko5ugnb.cloudfront.net		13.224.93.119	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:31.590351105 CET	8.8.8.8	192.168.2.4	0x2166	No error (0)	d1l34lgko5ugnb.cloudfront.net		13.224.93.129	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.070775032 CET	8.8.8.8	192.168.2.4	0x11ab	No error (0)	cdn.cookielaw.org		104.16.149.64	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.070775032 CET	8.8.8.8	192.168.2.4	0x11ab	No error (0)	cdn.cookielaw.org		104.16.148.64	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.079925060 CET	8.8.8.8	192.168.2.4	0xb938	No error (0)	cdn.optimizely.com	cdn.o6.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:32.106024027 CET	8.8.8.8	192.168.2.4	0xfc20	No error (0)	font.typeform.com	d3m6p8tvnbsibq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:32.106024027 CET	8.8.8.8	192.168.2.4	0xfc20	No error (0)	d3m6p8tvnbsibq.cloudfront.net		13.224.93.101	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:44:32.106024027 CET	8.8.8.8	192.168.2.4	0xfc20	No error (0)	d3m6p8tvnbsibq.cloudfront.net		13.224.93.89	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.106024027 CET	8.8.8.8	192.168.2.4	0xfc20	No error (0)	d3m6p8tvnbsibq.cloudfront.net		13.224.93.56	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.106024027 CET	8.8.8.8	192.168.2.4	0xfc20	No error (0)	d3m6p8tvnbsibq.cloudfront.net		13.224.93.95	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.127254009 CET	8.8.8.8	192.168.2.4	0x7cd8	No error (0)	polyfill.io		151.101.130.109	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.127254009 CET	8.8.8.8	192.168.2.4	0x7cd8	No error (0)	polyfill.io		151.101.194.109	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.127254009 CET	8.8.8.8	192.168.2.4	0x7cd8	No error (0)	polyfill.io		151.101.66.109	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.127254009 CET	8.8.8.8	192.168.2.4	0x7cd8	No error (0)	polyfill.io		151.101.2.109	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.275804996 CET	8.8.8.8	192.168.2.4	0xfac9	No error (0)	public.profitwell.com	dna8twue3dlxq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:32.275804996 CET	8.8.8.8	192.168.2.4	0xfac9	No error (0)	dna8twue3dlxq.cloudfront.net		13.224.93.112	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.275804996 CET	8.8.8.8	192.168.2.4	0xfac9	No error (0)	dna8twue3dlxq.cloudfront.net		13.224.93.97	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.275804996 CET	8.8.8.8	192.168.2.4	0xfac9	No error (0)	dna8twue3dlxq.cloudfront.net		13.224.93.17	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.275804996 CET	8.8.8.8	192.168.2.4	0xfac9	No error (0)	dna8twue3dlxq.cloudfront.net		13.224.93.84	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.298147917 CET	8.8.8.8	192.168.2.4	0x9bdc	No error (0)	d3m6p8tvnbsibq.cloudfront.net		13.224.93.56	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.298147917 CET	8.8.8.8	192.168.2.4	0x9bdc	No error (0)	d3m6p8tvnbsibq.cloudfront.net		13.224.93.95	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.298147917 CET	8.8.8.8	192.168.2.4	0x9bdc	No error (0)	d3m6p8tvnbsibq.cloudfront.net		13.224.93.89	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.298147917 CET	8.8.8.8	192.168.2.4	0x9bdc	No error (0)	d3m6p8tvnbsibq.cloudfront.net		13.224.93.101	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.629133940 CET	8.8.8.8	192.168.2.4	0xfa29	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:32.629133940 CET	8.8.8.8	192.168.2.4	0xfa29	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:33.712939024 CET	8.8.8.8	192.168.2.4	0x3bbb	No error (0)	cdn3.optimizely.com	cdn.optimizely.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:33.726298094 CET	8.8.8.8	192.168.2.4	0x2457	No error (0)	a15381830540.cdn.optimizely.com	wildcard.cdn.optimizely.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:34.859216928 CET	8.8.8.8	192.168.2.4	0xbd4c	No error (0)	logx.optimizely.com	p13nlog-1106815646.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:34.859216928 CET	8.8.8.8	192.168.2.4	0xbd4c	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		34.200.62.85	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:34.859216928 CET	8.8.8.8	192.168.2.4	0xbd4c	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		50.16.119.144	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:34.859216928 CET	8.8.8.8	192.168.2.4	0xbd4c	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		3.225.88.81	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:44:34.859216928 CET	8.8.8.8	192.168.2.4	0xbd4c	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		34.234.23.30	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:34.859216928 CET	8.8.8.8	192.168.2.4	0xbd4c	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		3.228.235.75	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:34.859216928 CET	8.8.8.8	192.168.2.4	0xbd4c	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		34.202.25.133	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:34.859216928 CET	8.8.8.8	192.168.2.4	0xbd4c	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		52.73.245.54	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:34.859216928 CET	8.8.8.8	192.168.2.4	0xbd4c	No error (0)	p13nlog-11 06815646.us-east-1.elb.amazonaws.com		52.200.116.103	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:36.010404110 CET	8.8.8.8	192.168.2.4	0x611f	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:36.010404110 CET	8.8.8.8	192.168.2.4	0x611f	No error (0)	pagead46.l.doubleclick.net		172.217.22.34	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:38.484662056 CET	8.8.8.8	192.168.2.4	0x8617	No error (0)	www.typeform.com	d1l34lgko5ugnb.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:38.484662056 CET	8.8.8.8	192.168.2.4	0x8617	No error (0)	d1l34lgko5ugnb.cloudfront.net		13.224.93.102	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:38.484662056 CET	8.8.8.8	192.168.2.4	0x8617	No error (0)	d1l34lgko5ugnb.cloudfront.net		13.224.93.119	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:38.484662056 CET	8.8.8.8	192.168.2.4	0x8617	No error (0)	d1l34lgko5ugnb.cloudfront.net		13.224.93.121	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:38.484662056 CET	8.8.8.8	192.168.2.4	0x8617	No error (0)	d1l34lgko5ugnb.cloudfront.net		13.224.93.129	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.170.224.115	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.78.155	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.194.171.8	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.18.91.199	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.48.66.74	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.208.235.219	A (IP address)	IN (0x0001)

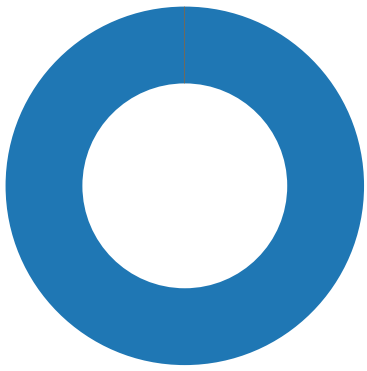
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.212.209.68	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.564482927 CET	8.8.8.8	192.168.2.4	0xad23	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.229.194.56	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	lnkd.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.48.66.74	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.208.235.219	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.251.184.34	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.19.92.244	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.248.49.247	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.248.78.233	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.212.209.68	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:46.824312925 CET	8.8.8.8	192.168.2.4	0xdc93	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.194.171.8	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:48.423309088 CET	8.8.8.8	192.168.2.4	0xa6eb	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:48.433228016 CET	8.8.8.8	192.168.2.4	0x99c7	No error (0)	consentdeliveryfd.azurefd.net	t-0001.t-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:48.939358950 CET	8.8.8.8	192.168.2.4	0x103e	No error (0)	cm.g.doubleclick.net	pagead.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:48.939358950 CET	8.8.8.8	192.168.2.4	0x103e	No error (0)	pagead.l.doubleclick.net		216.58.207.34	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:49.722281933 CET	8.8.8.8	192.168.2.4	0xac90	No error (0)	pagead.l.doubleclick.net		216.58.206.2	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:49.924432039 CET	8.8.8.8	192.168.2.4	0xc88b	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:49.924432039 CET	8.8.8.8	192.168.2.4	0xc88b	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:44:49.924432039 CET	8.8.8.8	192.168.2.4	0xc88b	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:49.924432039 CET	8.8.8.8	192.168.2.4	0xc88b	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:49.924432039 CET	8.8.8.8	192.168.2.4	0xc88b	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:44:49.924432039 CET	8.8.8.8	192.168.2.4	0xc88b	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:49.955195904 CET	8.8.8.8	192.168.2.4	0x6102	No error (0)	www.google.co.uk		172.217.21.195	A (IP address)	IN (0x0001)
Nov 20, 2020 20:44:52.678718090 CET	8.8.8.8	192.168.2.4	0x5a3a	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:45:08.370810986 CET	8.8.8.8	192.168.2.4	0x9f5d	No error (0)	facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 20, 2020 20:45:14.426263094 CET	8.8.8.8	192.168.2.4	0xfb64	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:45:14.426263094 CET	8.8.8.8	192.168.2.4	0xfb64	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 20, 2020 20:45:14.540884972 CET	8.8.8.8	192.168.2.4	0xa2aa	No error (0)	facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 20, 2020 20:45:18.351304054 CET	8.8.8.8	192.168.2.4	0x188e	No error (0)	pixel.facebook.com	z-m.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:45:18.351304054 CET	8.8.8.8	192.168.2.4	0x188e	No error (0)	z-m.c10r.facebook.com		185.60.216.36	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5896 Parent PID: 1476

General

Start time:	20:44:00
Start date:	20/11/2020

Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://mcmms.typeform.com/to/Vtnb9OBC'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF609CBFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: 5564 Parent PID: 5896

General

Start time:	20:44:02
Start date:	20/11/2020
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1620,15715787858784209187,14403432740096362 10,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1808 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: chrome.exe PID: 6068 Parent PID: 5896

General

Start time:	20:44:27
Start date:	20/11/2020
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1620,15715787858784209187,14403432 74009636210,131072 --lang=en-GB --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5040 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: 1284 Parent PID: 5896

General

Start time:	20:44:28
Start date:	20/11/2020
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1620,15715787858784 209187,1440343274009636210,131072 --lang=en-GB --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=6168 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly