



ID: 350128
Cookbook: browseurl.jbs
Time: 20:25:01
Date: 08/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report http://www.abmcovidvaccine.com 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Compliance: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 11
Public 12
Private 12
General Information 12
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 46
No static file info 46
Network Behavior 46
Network Port Distribution 46
TCP Packets 46
UDP Packets 48
DNS Queries 51
DNS Answers 52
HTTP Request Dependency Graph 55
HTTP Packets 55
HTTPS Packets 56
Code Manipulations 56
Statistics 56
Behavior 56
System Behavior 57

Analysis Process: chrome.exe PID: 4696 Parent PID: 1560 57
General 57
File Activities 57
Registry Activities 57
Analysis Process: chrome.exe PID: 6224 Parent PID: 4696 57
General 57
File Activities 58
Registry Activities 58
Analysis Process: chrome.exe PID: 7200 Parent PID: 4696 58
General 58
Disassembly 58

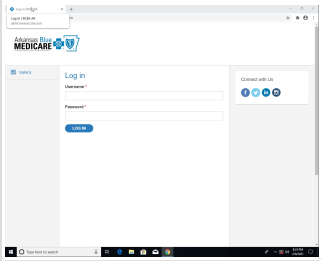
Analysis Report http://www.abmcovidvaccine.com

Overview

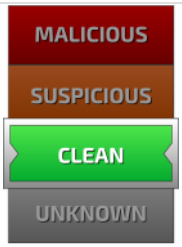
General Information

Sample URL:	http://www.abmcovidvaccine.com
Analysis ID:	350128

Most interesting Screenshot:



Detection

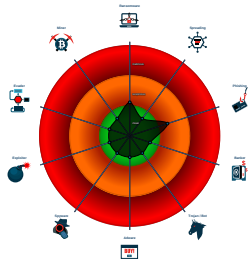


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- HTML title does not match URL
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 4696 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://www.abmcovidvaccine.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6224 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1312,15472918294386558836,11097865136599668024,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1740 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7200 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1312,15472918294386558836,11097865136599668024,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5688 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

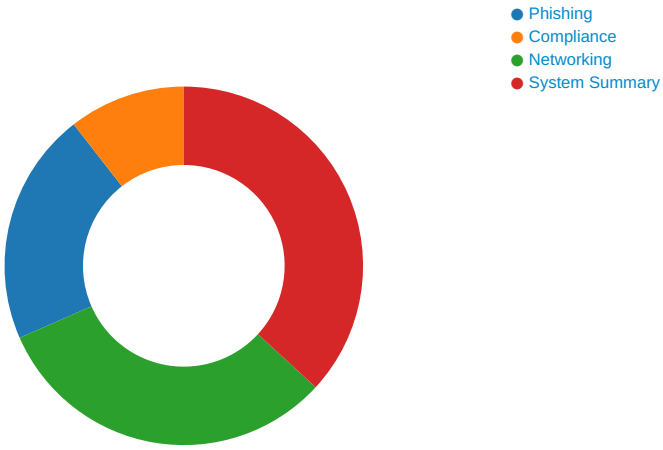
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright null 2021



Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Compliance:

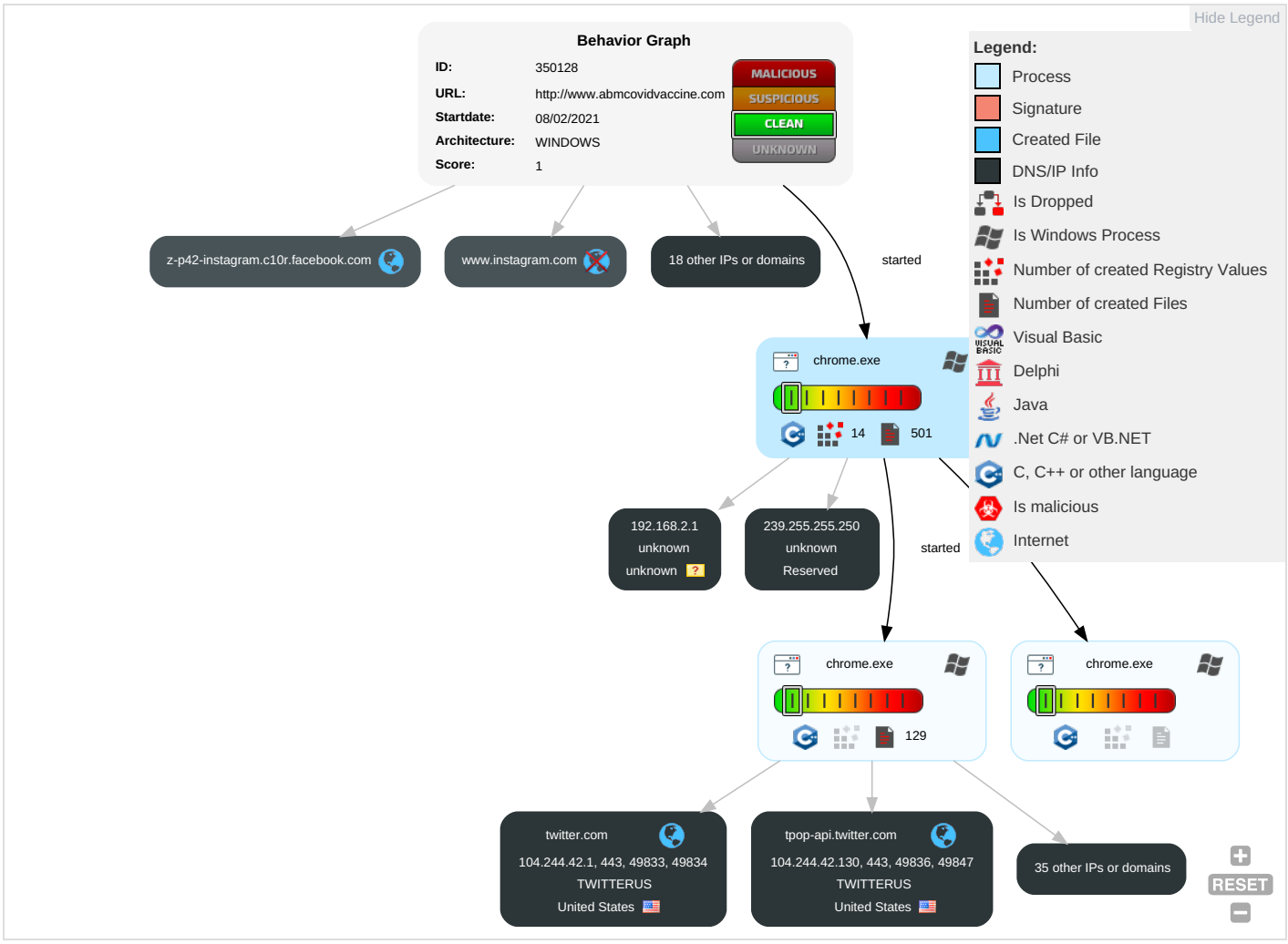
Creates a directory in C:\Program Files

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

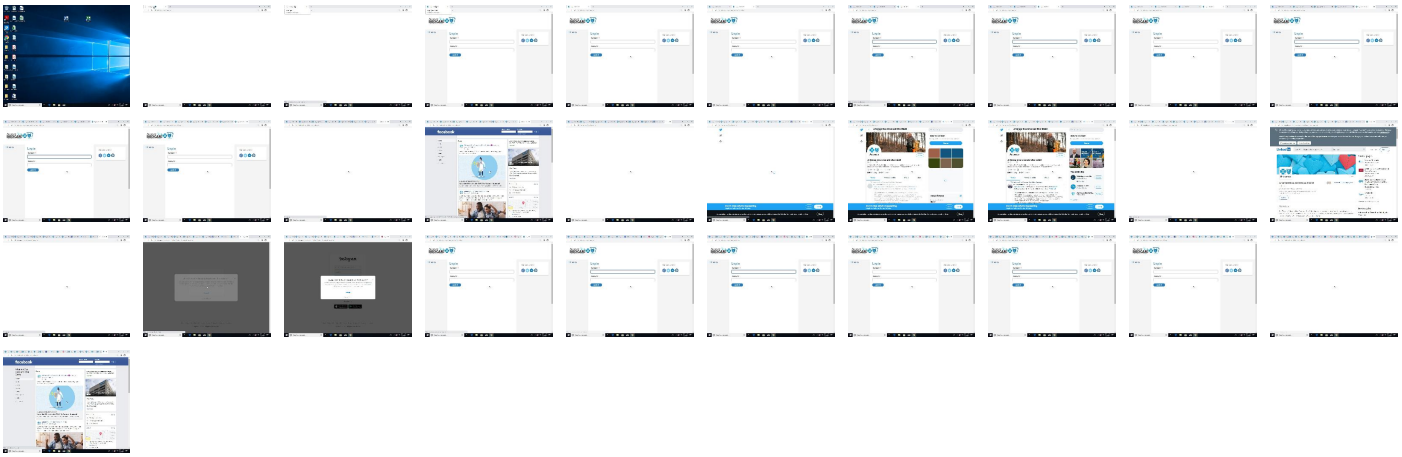
Behavior Graph

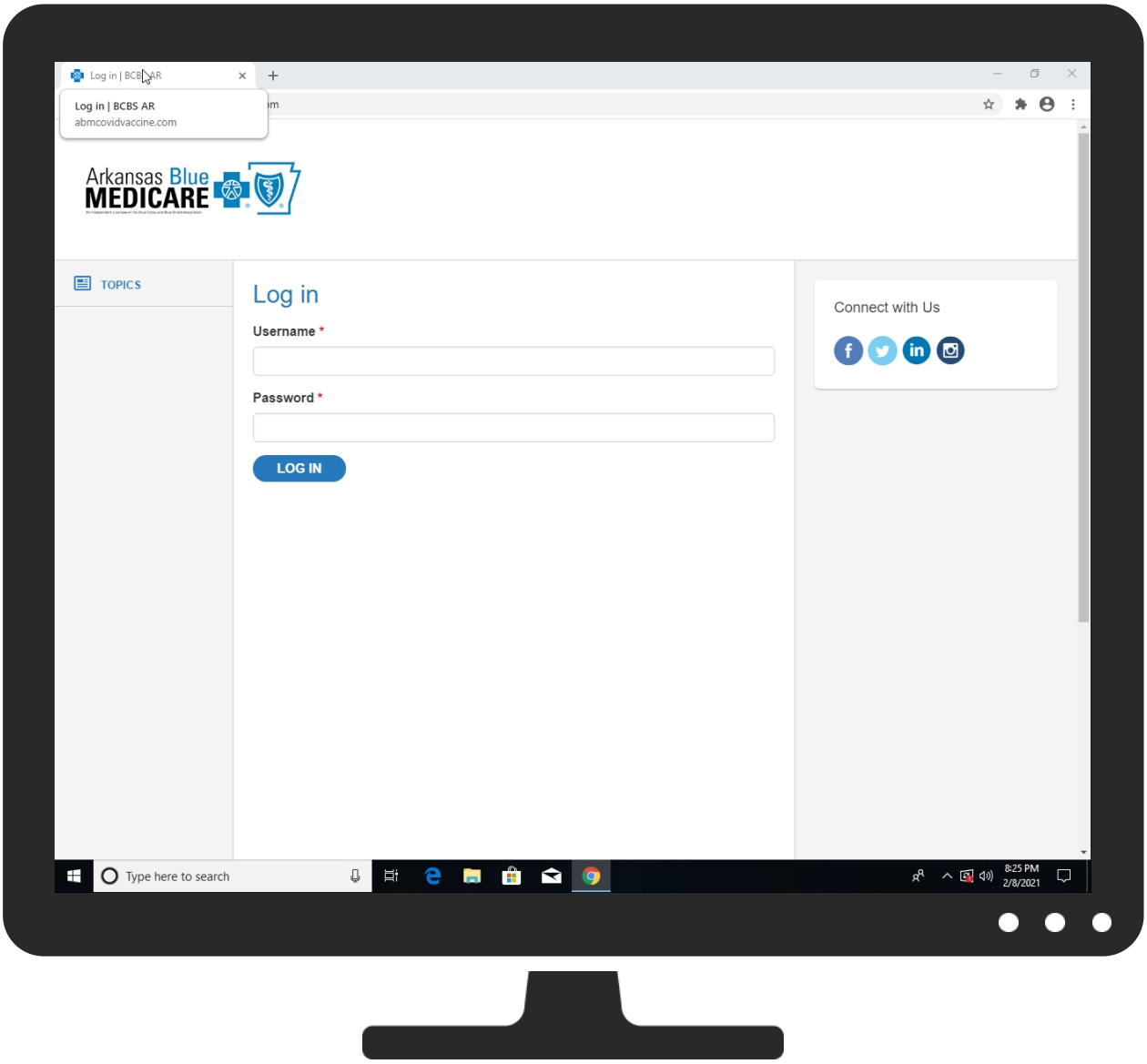


Screenshots

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://www.abmcovidvaccine.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1404.wpc.epsiloncdn.net	0%	Virustotal		Browse
cdn.onenote.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.abmcovidvaccine.com/article/healthLog	0%	Avira URL Cloud	safe	

Copyright null 2021

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
scontent-frx5-1.xx.fbcdn.net	185.60.216.19	true	false		high
twitter.com	104.244.42.1	true	false		high
stats.l.doubleclick.net	108.177.15.156	true	false		high
www.abmcovidvaccine.com	23.185.0.4	true	false		unknown
instagram.com	52.22.200.157	true	false		high
scontent-frt3-1.xx.fbcdn.net	31.13.92.14	true	false		high
tpop-api.twitter.com	104.244.42.130	true	false		high
scontent.xx.fbcdn.net	157.240.9.23	true	false		high
t.co	104.244.42.69	true	false		high
scontent-frt3-2.xx.fbcdn.net	157.240.20.19	true	false		high
facebook.com	185.60.216.35	true	false		high
cs672.wac.edgecastcdn.net	192.229.233.50	true	false		high
cs1404.wpc.epsiloncdn.net	152.199.21.118	true	false	• 0%, Virustotal, Browse	unknown
z-p42-instagram.c10r.facebook.com	185.60.216.174	true	false		high
googlehosted.l.googleusercontent.com	172.217.23.33	true	false		high
cs510.wpc.edgecastcdn.net	152.199.21.141	true	false		high
cs189.wpc.edgecastcdn.net	68.232.34.217	true	false		high
www.facebook.com	unknown	unknown	false		high
external-frt3-2.xx.fbcdn.net	unknown	unknown	false		high
abs.twimg.com	unknown	unknown	false		high
pbs.twimg.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
static-exp1.licdn.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
api.twitter.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
static.xx.fbcdn.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
www.instagram.com	unknown	unknown	false		high
video.twimg.com	unknown	unknown	false		high
media-exp1.licdn.com	unknown	unknown	false		high
cdn.onenote.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.abmcovidvaccine.com/#main-content	false		unknown
http://https://www.abmcovidvaccine.com/	false		unknown

URLs from Memory and Binaries

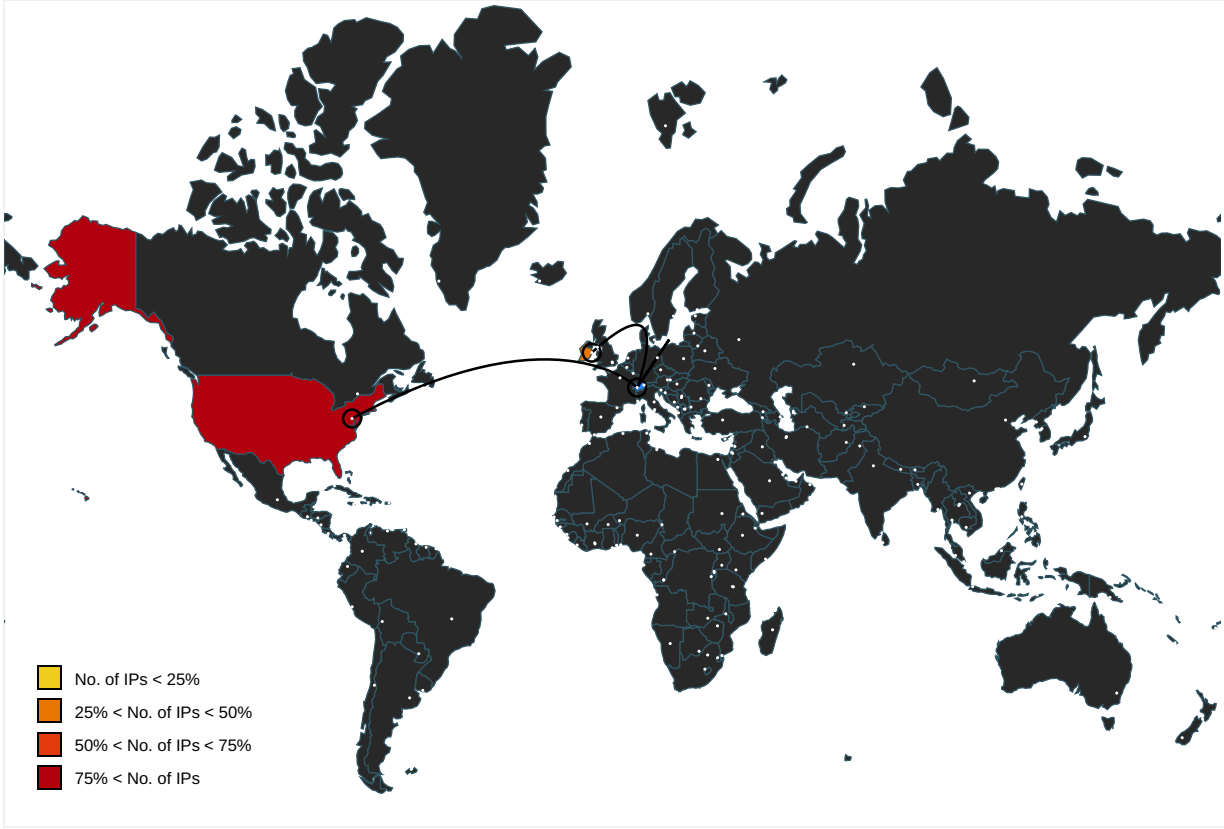
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.fr.f9ea93e5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iJRM4/yc/l/en_US/dgX93DXzt42.js?_nc_x=Ij3Wp8lg5Kza	84a6934849a0ce26_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yC/r/BwjU4B_qfpp.js?_nc_x=Ij3Wp8lg5KzaD	5854018eddf7ea85_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iw_34/y6/l/en_US/eyQpJxMA-MQ.js?_nc_x=Ij3Wp8lg5Kza	172a860821ea046b_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.DMRichTextCompose.9cd058d5.jsa	6065fc8ff2ba9114_1.0.dr	false		high
http://https://support.twitter.com/articles/14606#receipts	1f657cd9d2e651bf_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.ga.5b670865.js	2cc80dabc69f58b6_1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3iIma4/yM/l/en_US/otABH8Hq8lW.js?_nc_x=Ij3Wp8lg5Kz	7e28d95156f38456_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.pt.4c8c9925.js	2cc80dabc69f58b6_1.0.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://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.FleetsNotification.c7ca	305fc401532e681c_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.SettingsRevamp.9e9401c5.jsH	dd7c08f8afa3e0ed_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3icrf4/yc/l/en_US/3K56jq1-BJo.js?_nc_x=Ij3Wp8lg5Kza	321c89a0cf980c7a_0.0.dr	false		high
http://https://www.abmcovidvaccine.com/article/healthLog	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://abs.twimg.com/responsive-web/client-web/ondemand.SettingsRevamp.ad87b945.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iFo84/yJ/l/en_US/dE34yGDewPm.js?_nc_x=Ij3Wp8lg5KzaD	520c8eb9b503bbdd_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.QuoteTweetActivity.80f12765.js	2cc80dabc69f58b6_1.0.dr, 2ea2178a0c609e73_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-he.7cbd4675.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.	6ffa308dc8e676c0_0.0.dr, 2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.bg.00e7b245.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3ilNU4/y9/l/en_US/AgUTJo_P37N.js?_nc_x=Ij3Wp8lg5KzaD	5496109d4f7b96d3_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.sv.28392d45.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/loaders.video.PlayerHls13.af32	5f83f7680931967d_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.FleetMediaDetail.b3698f65.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://twitter.com/sw.js	000003.log8.0.dr	false		high
http://https://cards-frame.twitter.com/i/cards/tfw/v1/uc/	14e649e30da9e482_1.0.dr	false		high
http://https://www.instagram.com/arkansasbluecross/Login	History-journal.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.tr.39d2e245.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.ru.fb6ee8f5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://www.abmcovidvaccine.com/articles	Current Session.0.dr	false		unknown
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.it.5e2db425.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3izlq4/yE/l/en_US/XcRl1L0H-6g.js?_nc_x=Ij3Wp8lg5Kz	c7096addd330082a_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-en-GB.2cbbd055.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iJRM4/yc/l/en_US/dgX93DXzt42.js?_nc_x=Ij3Wp8lg5Kz	84a6934849a0ce26_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-ar.8be46b85.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loaders.video.PlayerHls14.e03a2c55.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/i18n/en.6035ab55.jswindow.__SCRIPTS_LOADED__	584b02e94f90d6f0_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-kn.4d7c8785.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.SettingsRevamp.9e9401c5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.ComposeMedia.23580fc5.js	911303b706017723_1.0.dr, 2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iiFl4/yV/l/en_US/AUE5LGU8LPg.js?_nc_x=Ij3Wp8lg5KzaD	af41504502ee4663_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yJ/r/Lc8ECXL-UZC.js?_nc_x=Ij3Wp8lg5KzaD	28ecb4a79ba7dfeb_0.0.dr	false		high
http://https://www.abmcovidvaccine.com/article/healthy-living	Current Session.0.dr	false		unknown
http://https://abs.twimg.com/responsive-web/client-web/bundle.Search.e9bdd2a5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loaders.video.PlayerHls13.af3257a5.jsH	5f83f7680931967d_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.ko.bc9d7c95.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://cm.g.doubleclick.net/pixel?google_nid=twitter_dbm&google_redir=https://analytics.twitter.com	14e649e30da9e482_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Notifications.46033325.jsH	dadb79121f80db3b_0.0.dr	false		high
http://https://pbs.twimg.com/lex/placeholder_live_nomargin.png	14e649e30da9e482_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.ro.6b76b7a5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.BadgeViolationsNotification.57f85145.jsaD	277dc301fdbe4abf_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.ProfileRedirect.8718dfd	1fb1a4c4227ee3d7_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3ivL14/yE/l/en_US/OF0KXH7dXN7.js?_nc_x=Ij3Wp8lg5Kza	f970d696945d87bb_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.de.33cf6c55.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://help.twitter.com/using-twitter/twitter-videos	1f657cd9d2e651bf_1.0.dr	false		high
http://https://twitter.app.link/interstitial_switch_to_app	6489a8171d2f5aec_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loaders.video.PlayerHls13.af3257a5.jsHP	5f83f7680931967d_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yv/r/UxUwcdLgDuO.js?_nc_x=Ij3Wp8lg5Kz	50ac3b97b0ab1700_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yz/r/jcBZHUAk_Pz.js?_nc_x=Ij3Wp8lg5KzaD	1b1a5636e4986bb9_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Notifications.46033325.jsa	dadb79121f80db3b_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.AboutThisAd.11e4f855.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.TweetActivity.6447dad5.	6ef694d5ce1f425f_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loaders.video.VideoPlayerDefaultUI.42e72665.jsH	36d638cda08e0c85_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.FeedbackTombstone.8304e745.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iGD54/yL/l/en_US/gsrgPauTlZK.js?_nc_x=Ij3Wp8lg5Kza	dbf423f5fee4c1f0_0.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/loaders.video.VideoPlayerDefau	36d638cda08e0c85_0.0.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	1f657cd9d2e651bf_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yg/r/8iyi8cdwOLY.js?_nc_x=Ij3Wp8lg5Kz	2d9c625b3c10b617_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iLl54/y4/l/en_US/u5b7Jnjloqb.js?_nc_x=Ij3Wp8lg5Kza	7511033aad8ca3b4_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Bookmarks.70354f35.jsHP	5cdb003fa2438ec0_0.0.dr	false		high
http://https://abs-0.twimg.com/emoji/v2	14e649e30da9e482_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-nb.17d2ecf5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.es.feda7605.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.UserAvatar.948d1485.jsH	c8d1ca64e7b747d2_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://abs.twimg.com/sticky/default_profile_images/default_profile_normal.png	14e649e30da9e482_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.TweetCurationActionMenu.521fd635.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://www.abmcovidvaccine.com/	Current Session.0.dr	false		unknown
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-zh-Hant.8fc0bd25.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iFJA4/y_/l/en_US/aOGyzlMDcOb.js?_nc_x=Ij3Wp8lg5Kz	74921b3da4070251_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iw_34/y6/l/en_US/eyQpJxMA-MQ.js?_nc_x=Ij3Wp8lg5Kz	172a860821ea046b_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.LottieWeb.f4c2aa65.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loaders.video.VideoPlayerDefaultUI.42e72665.jsHP	36d638cda08e0c85_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/y_/r/JopZtdti8dq.js?_nc_x=Ij3Wp8lg5KzaD	6386862eb4b2bb21_0.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.UserMoments.80ac0335.js	b75d4bf482224df9_0.0.dr	false		high
http://https://scontent.xx.fbcdn.net	2cc80dabc69f58b6_0.0.dr, af47be93e4c33dc6_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iSUg4/yW/l/en_US/QUdFdbF8LuY.js?_nc_x=Ij3Wp8lg5KzaD	7506bc5effcaeb50_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3itji4/yN/l/en_US/POy4OSHUNA_.js?_nc_x=Ij3Wp8lg5KzaD	6f86a0170f447fa9_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Compose.90f29255.jsH	3d15c038e89633f9_0.0.dr	false		high
http://https://proxsee.pscp.tv	74ac1f2cd2c7e3ab_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Compose.90f29255.jsaD	3d15c038e89633f9_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iw_34/y6/l/en_US/eyQpJxMA-MQ.js?_nc_x=Ij3Wp8lg5KzaD	172a860821ea046b_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.AudioOnlyVideoPlayer.e86ca895.js(window.webpa	57c5a41b8cb0a730_0.0.dr	false		high
http://https://help.twitter.com/rules-and-policies/twitter-cookies	17049efb338b0154_1.0.dr	false		high
http://https://clients2.googleusercontent.com	bd8fcc6a-1249-4a82-8db3-ba32c00605e1.tmp.2.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yg/r/V8C3I2Budu6.js?_nc_x=Ij3Wp8lg5KzaD	669d5033304a9f70_0.0.dr	false		high
http://https://www.abmcovidvaccine.com/#main-content	Current Session.0.dr	false		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.156	unknown	United States		15169	GOOGLEUS	false
152.199.21.118	unknown	United States		15133	EDGECASTUS	false
31.13.92.14	unknown	Ireland		32934	FACEBOOKUS	false
68.232.34.217	unknown	United States		15133	EDGECASTUS	false
172.217.23.33	unknown	United States		15169	GOOGLEUS	false
23.185.0.4	unknown	United States		54113	FASTLYUS	false
152.199.21.141	unknown	United States		15133	EDGECASTUS	false
104.244.42.1	unknown	United States		13414	TWITTERUS	false
104.244.42.69	unknown	United States		13414	TWITTERUS	false
157.240.9.23	unknown	United States		32934	FACEBOOKUS	false
192.229.233.50	unknown	United States		15133	EDGECASTUS	false
52.22.200.157	unknown	United States		14618	AMAZON-AESUS	false
185.60.216.174	unknown	Ireland		32934	FACEBOOKUS	false
104.244.42.130	unknown	United States		13414	TWITTERUS	false
185.60.216.35	unknown	Ireland		32934	FACEBOOKUS	false
157.240.20.19	unknown	United States		32934	FACEBOOKUS	false
185.60.216.19	unknown	Ireland		32934	FACEBOOKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	350128
Start date:	08.02.2021
Start time:	20:25:01

Copyright null 2021

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.abmcovidvaccine.com
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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@50/610@37/20
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.abmcovidvaccine.com/#main-content • Browse: https://www.abmcovidvaccine.com/ • Browse: https://www.abmcovidvaccine.com/articles • Browse: https://www.abmcovidvaccine.com/article/health • Browse: https://www.abmcovidvaccine.com/article/healthy-living • Browse: https://www.abmcovidvaccine.com/article/nutrition • Browse: https://www.facebook.com/ArkansasBlueCross • Browse: https://twitter.com/arkbluecross • Browse: https://www.linkedin.com/company/arkansas-blue-cross-blue-shield • Browse: https://instagram.com/arkansasbluecross/ • Browse: https://www.abmcovidvaccine.com/#main-content • Browse: https://www.abmcovidvaccine.com/ • Browse: https://www.abmcovidvaccine.com/articles • Browse: https://www.abmcovidvaccine.com/article/health • Browse: https://www.abmcovidvaccine.com/article/healthy-living • Browse: https://www.abmcovidvaccine.com/article/nutrition • Browse: https://www.facebook.com/ArkansasBlueCross

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 172.217.22.205, 216.58.207.174, 172.217.23.78, 173.194.164.140, 74.125.173.25, 172.217.23.46, 172.217.23.42, 216.58.207.131, 172.217.20.234, 172.217.23.74, 172.217.22.202, 172.217.22.234, 216.58.207.138, 13.88.21.125, 52.147.198.201, 51.11.168.160, 13.107.42.14, 51.103.5.159, 13.107.246.13, 92.122.213.247, 92.122.213.194, 216.58.207.163, 172.217.20.227, 52.155.217.156, 20.54.26.129, 23.210.248.85, 173.194.151.75, 2.17.179.193 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, 2-01-2c3e-005c.cdx.cedexis.net, clientservices.googleapis.com, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, cdn.onenote.net.edgekey.net, r6.sn-4g5e6nle.gvt1.com, l-0005.l-msedge.net, r5---sn-4g5e6nes.gvt1.com, clients2.google.com, emea1.wns.notify.trafficmanager.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, li-prod-static.azureedge.net, www.google-analytics.com, r5.sn-4g5e6nes.gvt1.com, fs.microsoft.com, content-autofill.googleapis.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, r3---sn-4g5e6nld.gvt1.com, www.googleapis.com, ris.api.iris.microsoft.com, t-0003.t-msedge.net, blobcollector.events.data.trafficmanager.net, li-prod-static.afd.azureedge.net, e1553.dspg.akamaiedge.net, clients.l.google.com, cs2-wac.apr-8315.edgecastdns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, 2-01-2c3e-003d.cdx.cedexis.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, redirector.gvt1.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, r6---sn-4g5e6nle.gvt1.com, www-linkedin-com.l-0005.l-msedge.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, accounts.google.com, www-google-analytics.l.google.com, e1723.g.akamaiedge.net, Edge-Prod-FRAr3.ctrl.t-0003.t-msedge.net, star-azureedge-prod.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, cs2-wpc.apr-8315.edgecastdns.net, skypedataprdcoleus17.cloudapp.net, r3.sn-4g5e6nld.gvt1.com, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\0bc3c62c-42e2-4f9e-82d1-af0dd8a48b01.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7436155576362147
Encrypted:	false
SSDEEP:	384:H3NCicf5IcLGlN6rvvuW3d2E5HUNGhIrjgyExNoYALrzSmfEDQaWGlOwk2N716bU:v2xhC0FtwePc+ksfzWWK8mmRv
MD5:	1F0717BC64193895E7E4C611EE5B9A6B
SHA1:	0F288DA26B1979240204996F421DC23A4B35A30D
SHA-256:	FCC119694DC552F950FB7BE61D5A0918B31D86A107E5B3A0F53C119102156611

C:\Users\user\AppData\Local\Google\Chrome\User Data\0bc3c62c-42e2-4f9e-82d1-af0dd8a48b01.tmp	
SHA-512:	7C32D622C99B495FC7243F1386555FECE739761360A12B2D07FDFDEDC16905A81E5EE5328B5D53FB9A729848BB0E32F619A48B91A7A353F89A00739D7453430E
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....18.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\75c95981-70af-425d-bbf1-52af832c2c2a.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):	367004
Entropy (8bit):	6.050419626688261
Encrypted:	false
SSDEEP:	6144:8qF6yYdqUZOmRHuuMG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinh:8i1YwUo5uMGNPUZ+w7wJHyEtAWM
MD5:	141A37961C5019FC6C085AAA5316A870
SHA1:	5E2A935FFEBC349EE6A92A8F8039B604801CFFBF
SHA-256:	37A24B072BC4E8C3BDFF94C215AEA5FCBCB46A8186309A7F29953EE5AD6E0921
SHA-512:	D9163EEEDE0C5472CB300844AE68A99E34D21C767BDE4BE1CCE933103820D3337BE21FD0DF1C54443D1B24EF6E6D251C6CA69C45C3711A22F61F2D630112B97
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.612844752906844e+12,"network":1.612812354e+12,"ticks":153849614.0,"uncertainty":4466155.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\06ea4b78-3069-41f8-8e9c-224afe541745.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):	3216
Entropy (8bit):	5.619941287073546
Encrypted:	false
SSDEEP:	96:+U0rLU7eUUlUUaNpUDUUyUXBfUkKUdUuURLU6FU4jaUJUu7UwSUVUuyUf:+U0rLU7eU8UUaNpUDUZUxfUkKUdUuUR1
MD5:	29045276FF039854F6A99D4389F0D7FC
SHA1:	CC14BCAFE571F209A4018C3135AA87C43A7199C3
SHA-256:	9E37075D55890EB3EC54DC93EA6D05220BCE62EB831D1B4863315694CD878A9F
SHA-512:	458B9E081B1FBE9C0CEDDF541243CD1F21DDDDE91E452244097D5E87D8C139D850D39020246F98822A6284FFE5EFD391EE5E6C1B78E3699D3AD1ECCAD372AB3E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\06ea4b78-3069-41f8-8e9c-224afe541745.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1644380798.022475,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612844798.022478},{"expiry":1644380790.017715,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612844790.017718},{"expiry":1623731153.814578,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612844753.814585},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1628396793.149191,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612844793.149194},{"expiry":1612845076.116455,"host":"ZgakHcFnxwDGF9PERSixkUh/HMzJniLCV//wXgjiVEY=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\15f9de0d-8fc1-4257-821d-d0386657b950.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):	5684
Entropy (8bit):	5.181046278156595
Encrypted:	false
SSDEEP:	96:neLVBF/44YEyuGnafjaAVGxk0JCKL86kZ1f9bOTQVuwn:noVBi4VKa79I4KbkZBl
MD5:	891B09A4E92355E4E458137B81B0573B
SHA1:	B0D18EAEDC994C7C62A8192816954AE177C59FA6
SHA-256:	5FC25D09CD23894726E141ACE53692CE26905E11B578BD88B6C05A4DE447FD38
SHA-512:	8E16B1769D9E25074C78CEA7D6CB78D29F7399F98696AE1E33CF7353BA4D74DF8A6D4267949AFC759FC7DEE9C571144465ECB7249554F1077FAE84C95C46C5F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13257318350165601","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2330daf1-8efc-440b-affd-49454cceef4b.tmp	
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.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://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13259910352667424","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertis

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\235b3c69-80bb-4e2b-83fc-c2d0921b0afd.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):	5686
Entropy (8bit):	5.181585668082028
Encrypted:	false
SSDEEP:	96:neLV6nF/44YEyuGnafjaAVNxk0JCKL86kZ1f9bOTQVuwn:noVai4VKa79p4KbkZBl
MD5:	E761E47F0CBB7016312B9B4457DA617C
SHA1:	BDB9F3FB40F25B6275E7F3A4F6E5A2F235E0EA8E
SHA-256:	437F1B2C52DB17610D1132A9805467757FE56A311862554D6F6C0C252F675190
SHA-512:	56F2CC51A14061F5E3D3FF80B9D59E4B04FD7E1CA8827E4B6398036B69DBCC066ED1ED8A646036CA4D08762EEC39AD6EDD4508EAA8847BB3E6D971985410A2DE
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13257318350165601","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2fbe8363-cfe2-4b91-94c6-3181cc08f548.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1623731153.814578,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612844753.814585},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1612845062.08589,"host":"ZgakHcFnxwDGF9PERSixkUh/HMzJniLCV//wXgjiVEY=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612844762.085895},{"expiry":1623731153.192604,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612844753.192609},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.52056},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\322ba49d-aa75-4491-8677-5384329545e3.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):	2548
Entropy (8bit):	5.607218619497944
Encrypted:	false
SSDEEP:	48:YJFU8rLU1eUUc6UUhcMbEEUtUQryUBfUkKUeMjTUyb5lUuaUe8bPUu+wUwwDhUew:KU8rLU1eUUlUUaaUtUgyURUkKUdU2Uub
MD5:	5498E73F2EF4E329637FD6B2F7ECCE6E
SHA1:	321E048C16A2389A9E8374E55E02845DEC409424
SHA-256:	9667286F68A22A4F0FFBBD4C0D459ACF5C01CE83F43803581BED2D4232D994CF
SHA-512:	229D188C13728AACB8E82B5D2ADF51D3E6A381B204849746E08349DBED1BB6A12790DB83BD00F18FCFAA04F2AD5368233666EA5AC1945058C0ADC13F8EAA398
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1644380789.122041,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612844789.122043},{"expiry":1644380789.231088,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612844789.231091},{"expiry":1623731153.814578,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612844753.814585},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1628396783.713372,"host":"TZmujbl93Yt3Jl8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612844783.713376},{"expiry":1612845076.116455,"host":"ZgakHcFnxwDGF9PERSixkUh/HMzJniLCV//wXgjiVEY=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7106ec49-53fe-445b-8b86-84c34b3fee5d.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):	5684
Entropy (8bit):	5.1809067610296715
Encrypted:	false
SSDEEP:	96:neLVBF/44YEyuGnafjaAVfxk0JCKL86kZ1f9bOTQVuwn:noVBi4VKa79T4KbkZBl
MD5:	21C016190B6ABCE2C663CD72FD6AEE02
SHA1:	F3E202DEFF45DCC040146D83105DE68D96854BDE
SHA-256:	50ABBE7BB8DBD99343E794A0675DD339387765B6E64EAEDF9F232930EA85EF3E
SHA-512:	94B5D063967CEE06BEF22D4C327853BB799B33BE82507BF064E1714A14DFC564A26884CF41321033591E4E2ABC2F372E99BD2DDC494A5806A925795A25199DB1
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13257318350165601","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\72701be1-6b5b-4d49-8f5c-4c51a61938d9.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13257318350165601","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\98b8365c-da47-497a-a98a-cf2b7cb39ef7.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1644380801.005827,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612844801.00583},{"expiry":1644380790.017715,"host":"l/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysl=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612844790.017718},{"expiry":1623731153.814578,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612844753.814585},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1628396799.721206,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612844799.721209},{"expiry":1612845108.69241,"host":"ZgakHcFnxwDGF9PERSixkUh/HMzJniLCV//wXgjiVEY=","mode":"force-https","sts_include_subdomains":false,"sts_ob

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):	337
Entropy (8bit):	5.190825954202145
Encrypted:	false
SSDEEP:	6:mj6UN+q2PN723iKKdK9RXXTZIFUtp4MZmwP4+FG3VkwON723iKKdK9RXX5LJ:I6UN+vVa5Kk7XT2FUtp4M/P4+83V5Oav
MD5:	FB6C5E8B9A1E8AD8E978C72DAA317DC3
SHA1:	B08FB814092882B20CBFA1783870F2C31BE135A1
SHA-256:	053F2C976DD29F77A37ED425AE839A2550479F1E1FCE5492517CE19F5EFB178E
SHA-512:	CBC526B2945014BD6D901A4596FEEE9BCD057F87170D0491CFE319E690AFE782C30B4068C2C898C1DFE9929CF3084A62B3179B450E01C7FBB786A03E79D0F2DA
Malicious:	false
Reputation:	low
Preview:	2021/02/08-20:25:55.962 ddc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/02/08-20:25:55.963 ddc Recovering log #3.2021/02/08-20:25:55.966 ddc 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):	321
Entropy (8bit):	5.168224888096085
Encrypted:	false
SSDEEP:	6:mj++q2PN723iKKdKyDZIFUtp4bCcZmwP4bLVkwON723iKKdKyJLJ:I++vVa5Kk02FUtp4Gc/P4/V5Oa5KkWJ
MD5:	1FAC58D816EA26DF28EA9B6A4753E04D
SHA1:	4EA51868105126EDBF6CED7B12E14AA1EF6E4A5D
SHA-256:	7253C984A113B7AA91962C6E2211CCCE3DF9F3F2203570F088CB26AD478A98DA
SHA-512:	487CCA64E5BD47569D777A243DFB8DE4A5003D35C06834C24F362C79767E175A428B924A576BC81529189F8EB6A15369EA7DB0E0FF502DD9AD39488E504DC45
Malicious:	false
Reputation:	low
Preview:	2021/02/08-20:25:55.947 ddc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/02/08-20:25:55.953 ddc Recovering log #3.2021/02/08-20:25:55.955 ddc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\00824f37ca87544e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	274
Entropy (8bit):	5.63932598158908
Encrypted:	false
SSDEEP:	6:mkO9Yj018IrAMUBTJcpuHIK1A0CuFvpMZv2kx3G/iEK6t:e1thUBS8HIU9XFWxWX
MD5:	B16FDDCA0EBFA3C028AFE7B8C44CFEAB
SHA1:	49560AB762E7A64A76A45C1CF035555A68B4D341
SHA-256:	08CE6A967282A84659791F8827DC6408F6C5815727AF921AF8B3635B7DE4C223
SHA-512:	60425A12AA83989ABE35DD553E7508E1142E2C63D742BDD88F3A68F3566549A46209993447085CC3ABD9DFB330FFBB73D7A1E880E5537B6FD87CA017F98403B1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~loader.AudioOnlyVideoPlayer~ondemand.InlinePlayer.5e2ac1b5.js .https://twitter.com/....u./.....w.....i..wz.I.Y.\..vJ.V.....A..Eo.....&.8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\01ba7c5ad05b8b27_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\01ba7c5ad05b8b27_0	
Category:	dropped
Size (bytes):	1240
Entropy (8bit):	5.759519032598835
Encrypted:	false
SSDEEP:	24:PnVT/lil7gytWDFjMad1cnVT/wXcjmLiJTjHjE:PlNi7WhlWeTjjE
MD5:	1CE89EE3853C0805D809242D3CB6AD36
SHA1:	C9D96C1E16563D73A4AC88B7DC759FE515C2F768
SHA-256:	917B76A4AE4C18C7FB39FEB24E1402AB918D2E6DA0B3B4E8A88CC2F300C8B902
SHA-512:	D3D02028B617F2F36C2C6FF39146745CE39F2D493BFB8466661E9217E7D84F7B266B5594E97A13E6C49FB52904F66262174233119392808 7AA5F5E13097A9D41
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...7s.d...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y6/r/OzwlrmZ6Ecz.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....N;L..h.=...W...Em.+... .....A..Eo..... .v.....A..Eo.....u./.....'.....O....h.....(S.d..`.....(L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`. .....M`.....Qc>)?5....mzorV.....Qb.1tb...__d.. Qfj..W....CometImageIcon.react...`.....M`.....(QhJt.....BaseImage_DEPRECATED.react....QcB.....React.....QcN.....stylex... (S.H.`J.....L`.....@Rc.....O.....Qb.....h...b.....I`....Da(.....(S.....Ia.....M...!..@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/y6/r/OzwlrmZ6Ecz.js? _nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....`....&...&....&..a.`....DI]d.....@.....Qc^.....exports...a...K`....DI....8.....%.....&.%.-.....&...&.]....b.....A.d.... ....@.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\02820c69bd9c0256_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13416
Entropy (8bit):	5.925618361819305
Encrypted:	false
SSDEEP:	384:kuocLyDMooAuzURRZAQ9vgYYSEjLhvPS9rvBfm:kuo9xOSEjLhQ0
MD5:	2CED848FD56529B051EB41A995CD5AC4
SHA1:	9B66E0E5B87D21B6C93B8FB85EE8A610C786280F
SHA-256:	4FF6AC90659C476AAA9982544A99B2987A42747E476C1F4867AEE6A227871092
SHA-512:	C331550E2D14740C1D9F7470E8565E4A58476218C75AA30885C9514F50742FB6A91B39BAFB8B223CA0B4D4B97F21FC0A1C730D92104C2C91927224AC2F9124F8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...R....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yC/r/1lTbj7nYIoz.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./...../..ZN.....G^A..!.....=k$. .)j..A..Eo.....yKOe.....A..Eo.....'..0....O.....2..u.&.....(S.....`.....L`^.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js... ..`.....M`.....QcZw.B....i1bCZ.....Qb.1tb...__d..,Qi..aa ...DesktopHscrollUnitEventConstants.(S.l.`.....@L`.....,Qi..|q....DesktopHScrollUnit/itemInserted..(QhZ.(..... HSCROLL_ITEM_INSERTED_EVENT..(Qh.7.....DesktopHScrollUnit/itemShown.$Qg..''p....HSCROLL_ITEM_SHOWN_EVENT.4Qk...3%...DesktopHScrollUnit/HideI ndividualItem....$Qg...u....HSCROLL_ITEM_HIDE_EVENT..4Qkr.Pv'...DesktopHScrollUnit/scrollItemBeforeXout..4Qk.~ G%...HSCROLL_ITEM_SCROLL_BEFO RE_XOUT_EVENT....4Qk.L{.'...DesktopHScrollUnit/unhideIndividualItem..(Qh...W....HSCROLL_ITEM_UNHIDE_EVENT.....Qe.....logLastAdXout....0Qj.. ."

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\036e14d0acca75e5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6864
Entropy (8bit):	5.783431202828164
Encrypted:	false
SSDEEP:	96:00+0UHkdGtNeDjnk/I2sI+rzkFkHmLTm0uJkR7mb+0d0rB63pAYaRfhxkp:00+0UEgEjeIyokkHQPufbCV65AYckp
MD5:	C9AC8ED28FE6A283EFC9E498B8123005
SHA1:	02C70AD926FAB950F50D8003B54D901D94C98592
SHA-256:	C9C6984DAAB07CEA8A2DB9024CF5D2CFA96FA722319E30EA8E1A211EE8ACA469
SHA-512:	BB4F2EE48145A15B6BC07A606D942E2A13BD61007E5D62742239D949AADE637C725213C37E6E598F70A036B7387D10917CC65CFA7446C99575278982CB61093D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...~.#....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yf/r/kNNh_jXgUbS.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....<.....nEX..]9._.]Bj.7.F. B..A..Eo.....*.....A..Eo.....'.....O....@....j.....(S.I...`F....|L`:.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.... ..M`.....Qc...{....iJb/D.....Qb.1tb...__d..4Qk...'&...VideoPlayerContextSensitiveConfigUtils...(S.<.`2.....L`.....0Rc.....`....I`....Da.....(S.....a.....d.....@. .....a..@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yf/r/kNNh_jXgUbS.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`....-....`....&...&..q.&..!.D&.(S.....M.a....%.....d.. .....@. .....q.d.....@.....D&.(S.@..`8.....L`.....0Rc.....O.`....I`....Da.....(S.....Ia....8....<..I,.....@.....@.....@.....@.....@.....@.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\050ec6bcdc2c22e3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.585783893166888
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\050ec6bcdc2c22e3_0	
SSDEEP:	3:m+lPtATXlA8RzYkwlAd0CW/KNGKYHUuArW7EafVNRzLxKacQ8KNlHCenltlHl2XH:mkWXYkvwyHUu71nNN6eXBjKYHdK6t
MD5:	4A937DC0DF6D99A265499F35732ED969
SHA1:	6BC31DAF49B85BA614B6334028A8FC2CCEC3327D
SHA-256:	E10315286097052BD7E9A42AFCB63DB20D21D7F713F1CE5523E90C8F44051685
SHA-512:	41E1199413BC3B5B8E334A6011F5906219E41D9AEDD7C25FC506B2B4D13BBC3D6B82AD7DF1D887D80272C9EFB64CD19CBFA37EB005AB77A8BC43197DFFD63 9B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...A..6..._keyhttps://static-exp1.licdn.com/sc/h/b045gzzgfxgfysptabriery88 .https://linkedin.com/E...u./.....B.....kz...>.m.|*V|+G..?.j ...Y...+!.A..Eo....._.9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f5ca93f02a10079_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	5.73606693284383
Encrypted:	false
SSDEEP:	24:KnVR3l41yETF7gHUyUbbM/keYDqc1cnVR3l41vz7fgttcl35J32v0iJTRiz6Z:Ko4cEgQM/Eqpo45fWmlJJGPTIz6Z
MD5:	AC4E32DF4BBB50AC9099D573A7E202BD
SHA1:	F9482687D25F17C82336CCF947BD5220C7B5BBA1
SHA-256:	F565AF82E9BDD3D5B47A7A367252E7C8CEAE15B78111912BA440B548F6217568
SHA-512:	BCDF75F9E1E5203CE16CE8BC9F396ABCA80C8993C1A40E3F96AF28BA2D1D05FD1C1B3447BE5F3F98AE6D6DFF0818AACDA54CCC2A01094217FADD49F03A744 752
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....YQG...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yz/r/f-n_noRIlUB.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....d..[6.....,(..y<.....`..K.4..A.. Eo.....A..Eo.....u./.....'.....O.....'.....P.....(S.d..`.....(L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`... ...Qc.v.....L8vbC.....Qb.1tb...__d.. Qfn.X.....ProgressBar.react.....`.....M`.....Qb...E....cx....QcB.....React.....QdRLx~....joinClasses..(S.`.`z....$L`.....8Rc.....O.. .Qb.....h...a.....I`....Da....,.....(S.....Ia.....P..rB..... ...I..a..@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yz/r/f-n_no RIlUB.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....8...`....&...&....&.....D`....DI]d.....Qd.....Component.....Qc^.....exports..4..a.....Qb..y.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f88fbc7ffd0909d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.584101421557387
Encrypted:	false
SSDEEP:	6:mCYGLDlynflGB7WLaI1nwlyPnWKyYSwu+4YK6t:0flGtWLainwgPCwuy
MD5:	F27CFD374CCA000F10BAB182BDD3B166
SHA1:	42F32B93AEF7E4AB6A3AF9E364DA669D7741353F
SHA-256:	902A293A26D65197B392DDDF8838BBD17DF63A796B4EAB7DF7A4536A34228BFD
SHA-512:	211D5C64CF78ADAAEEA6C235F044EDCEEA9458F9E6889A373EFF3FEF718D9E1F5F656129C743AD5BCCD162E22B9A06498D29B4C428235AF314047A04C463C7 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...7|....._keyhttps://www.instagram.com/static/bundles/es6/Vendor.js/c911f5848b78.js .https://instagram.com/....u./.....L-[.8..U.;.[...9$.5.y....'....A..Eo.... ..Vp.4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\116b3d0378c2811d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	20619
Entropy (8bit):	5.941274517543002
Encrypted:	false
SSDEEP:	384:t09LOPF0aJgHohwyqo4EhxZToBr42pJB7Mu5lMW/XYgY:t0OPAzB0oBr4O3XY1
MD5:	8471150BDD691DD3B79AF4806E12D15A
SHA1:	5C8045AD393DED2F1E76500CB969B1A5C844F233
SHA-256:	87111DA9ADF378783B0FE3C822CE38B4793EB8FA6A01C93E5C6E54B7225C7AC4
SHA-512:	4FD1FDE90593357D734760CC71B69941E0661B427F9EA583A3B87D02EEABCF2B53512FEF756FB325651FBDEE02550B8EEEAC2CE2200C33B5CE575464E681362
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\116b3d0378c2811d_0	
Preview:	0\r..m.....s....zr....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iQbs4/yD/l/en_US/rdHsYaZrptY.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/f...u./.....W.\.O./.....H.:.."4C.}(j.A..Eo.....w.....A..Eo.....'.....O.....N...@.....(S.m...`.....L`z.....Qbj$.....self..Q.`>n.....CavalryLogger....Qc.h,.....start_js.....`.....M`.....Qc.....owBnN.....Qb.1tb...__d..(Qh.:.....CometDensityAwarenessContext...`.....M`.....QcB.....React....(S.D.`D.....L`.....1...Qen!.....createContext.....Qc^.....exports...K`....Dk....8.....&.]...&..&.(...&.Y....&.%.-.....(Rc.....I`....Da.....c.....@.....@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iQbs4/yD/l/en_US/rdHsYaZrptY.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`f...D`.....`h...&...&....&.(S.D.`D.....L`.....K`....Dk....8.....&.]...&.(...&..&.Y....&.%.-.....(Rc.....I

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\16bc35347ddd7631_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	258
Entropy (8bit):	5.601446965805244
Encrypted:	false
SSDEEP:	6:mTXXYj018IrAMUF/1S0MMYtLKWLJerP4HxnK6t:SP1thUpcztLNgzcp
MD5:	9580E7A0E9560F922E4DDEB8F8CD1EB0
SHA1:	3B716DA56E359BA3547C921F3F15831EC38FE6C3
SHA-256:	1F2F8AE9292810653171073 48E9ACB2718A19E611F9D65C12FE5ACCB24FB68F1
SHA-512:	C81888891377B5F0E3095DF6140CF2A2F6270E0312B7CBD3F05663301D8BB583B0F02F631CA1CDC21100C5307399AA15537192490C0FB1BD98B968793DFC3065
Malicious:	false
Reputation:	low
Preview:	0\r..m.....~....c/....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~loader.Typeahead~bundle.UserLists.a10f5765.js .https://twitter.com/....u./.....x}.0.....wY....D..."..e..5_..A..Eo.....R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\172a860821ea046b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29155
Entropy (8bit):	6.065774548380319
Encrypted:	false
SSDEEP:	384:da6IVoXmUFsrjjB3nzO8GEICK9XvrrZvCgYxJr+7dCe5t:da6T0jB3zO8hIx9D1y0cgt
MD5:	E71BE0B2834225659C83F654B046317A
SHA1:	6F0E74C041AD1B4CB497D9A9970DBD4FCEEC137D
SHA-256:	6919578E3031FE31DAB6B8B280AA9FF3368FB6233736C8DB50D67AEAAF41574E
SHA-512:	405933EAC471D77297877ADC8778AB2801E25A5CD58CDC8E0D76D3407675B48804D0C44E61016B4548EE6FFEB5766F097DFE84D319AEA9BE63B5443845C84D8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...l..)...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iw_34/y6/l/en_US/eyQpJxMA-MQ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....y.....p.E...p.P^.C6..a..>^M.F.....A..Eo.....-..q.....A..Eo.....'.....O....0p..}..7.....(.....(S.....`.....L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc...n....HzC6y.....Qb.1tb...__d..<Qm2;.$....VideoComponentWithLoopingPlaybackQuery.graphql...(S.8.`&.....L`.....(S.....Ia.....IE.@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iw_34/y6/l/en_US/eyQpJxMA-MQ.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`*...D`.....)....`....&...&..a.&..!.&.(S.|.`.....$L`.....8Rc.....O...Qb.....h...a.....I`....DaB..... Qf..,...UserAgent_DEPRECATED..Qb.....ie...(S.....Ia.....X..tI..... ....I..Q/....d.....

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):	5.468746015738161
Encrypted:	false
SSDEEP:	6:mwh0lXYGL+MIwJJwMJp12tZSJilxhm4jK6t:dGIwvLAZUDy
MD5:	2E0CDAA545A6626D5D8AD8F2CEE5BEAA
SHA1:	E1197D7C3B4C4E1D197ADC8406433D64A66EB584
SHA-256:	8D36448318025753A4AE94D46989BCF0D4D49734CA0411B6282884EB7FE6E2B5
SHA-512:	4A8C6227A5670487F3DF7690A08E76C43404C0E72DB78ED6F91A6607E4D07B77CE62354794307D34A9964CF0DA6575E797CC7C8AD22AA54B06F64CC7F298382
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.....I....._keyhttps://www.google-analytics.com/analytics.js .https://twitter.com/..".u./.....:.&..L...jC...1UR@u<$mz.B...u..A..Eo.....H.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1aa071b50f41ec1b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1aa071b50f41ec1b_0	
Category:	dropped
Size (bytes):	5088
Entropy (8bit):	5.710584047059507
Encrypted:	false
SSDEEP:	96:AGVI4G35uPZOSJITInUvZk/DnFYWjKDCoDDd/FN6EPpG/41q:AG24G3EVJZnUe/DFYWj0Nx/1R241q
MD5:	8C99FD574DDEBB2456BD6858491B2BA4
SHA1:	03807690D815BB71D13362E537F64968D29611AA
SHA-256:	7E2B681FA33EE3668C388EFEDFD4C2F6046B77BCDC6F39E79E1D9EA6EB4CF9A8
SHA-512:	2338EE4CE1E3714968CE2AD84F972F834F2D1F6B04EC02CD1E21531C405BF7BC6B3E5B53E62268BB1CD3E030953FDF0040AD692B013C6B8441D4478FD32AF4C F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...L....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y8/r/m1LX7nnWMlK.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....".I.@Q.<..1BN.+.ju...<...A..Eo.....K.....A..Eo.....'..#....O....P.....j.....(S.....`.....lL`2.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`... ...M`.....Qc..k.....VltY8.....Qb.1tb...__d.. Qf...o....fbjs/lib/emptyObject...`.....M`.....Qd.%.....emptyObject..(S.0.`.....L`.....a...Qc^.....exports...K`....Df....8.....&.]...-.....(Rc.....I`....Da....T.....b.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/y8/r/m1LX7nnWMlK.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`N...D`.....`r...& ...&....&.(S.H.`H.....L`.....@Rc.....O.....Qb.....h...b.....I`....Da\.....(S.....Iab...o.....d.....@.....(S.....Ia~.....@.....@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1b1a5636e4986bb9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211504
Entropy (8bit):	5.880040341653236
Encrypted:	false
SSDEEP:	3072:8tfFsEMDWs0gI9GRN5rSBL177IAWffg1W8fcMLbnDM:qVLGFYJHbWacMLbDM
MD5:	6E8147C53E6D8B20F0299EE66B931CA9
SHA1:	305CCDD4CB896F1DCFFE6AFA2C5FB73501A80FCD
SHA-256:	763F06B3145D142395E340D6A6FF33E90D9CEC54DADE2ED3C9FACD501AF42F6E
SHA-512:	1EC5D7912E671233401848D4E1036E3164A69C1A93117E75B20CEFD4860C5FC67B9BE5D6BD4AB328221340131764E0810951AFD7D7BC046ECDEB94741E76F79(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....42BEA4579AF167E1EF1E1A011696919BD106D1746329B237EAB5D6ABC3955328.....'.-=....OB...X8.....(...X(.....@!..... .....|.....h.....(.....(S...Y(..`fP.....L`.....Qbj$.....se lf..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc..9.....PJVgx....(S...`.....,L`.....8Rc.....M....O.a.....I`....Da.....Qb.C.....flat.(S.....Ia....,.....d... .....Q3.@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yz/r/jcBZHUAk_Pz.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....A!...`....&...&...0&..q4D&...(S..... .Pd.....Array.flat..aJ.....I....5d.....&.(S.....O.a.....Q3.d.....&.(S.....5.a.....Pc.....flatMapa.....I..d...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1b64920e176572d0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.450557528325968
Encrypted:	false
SSDEEP:	6:m7mEYj018IrAkhVDRSVpM5Zp1RSE6sTSQZ+4XMK6t:Ymw1tvpbZkmTSQA
MD5:	C9D82274D2BD2583D3DA473A27350775
SHA1:	62B27031F30D407F0B2563121EECFAC512E7CF8C
SHA-256:	2AC7DEBFF9E3A04B320750EF5BBA1E26B5BD33DAB18EC69E346BEC84D13319B9
SHA-512:	FD10214C8D6B0F67EE910409B8321ED29345E79F6FCF4CCCF5B4CECA15A6B9CB3EAFFCD42B3D76B9DB34CCD3F72BF0A8D79309AD97B7078CF7E5DC31988A 4F4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....K....._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.emoji.en.4d4ef105.js .https://twitter.com/..`.u./.....d.....*..bw.tHt..n....v.fq,T..j .6$1..A..Eo.....t.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1cacf995d3453aa2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	30336
Entropy (8bit):	5.919357424106182
Encrypted:	false
SSDEEP:	384:TGpCGjAu8FLFAi9i4+lLkRNvn4z4fqJZbI3lAby0u7mW7aNEkeLFBZFID:TGkK8Di4+lUBlfqTE3eTLELTZyD
MD5:	01460463987FAF45D8E125B1B9E4173E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1cacf995d3453aa2_0	
SHA1:	9893EA8E738DE8BBAC286CD4E6718565D08F3E94
SHA-256:	05709C96667793CF9E0CCBB5300DF71BCDE42CFCAC17FB5C9AF28B4F1E2F990A
SHA-512:	0773A8765D5F0D98DB6AEE5958F1EEE3B7FD7BB082E58980403A55E104DA5DCBBA35D3E1728CAD2C0B60EE42F9EC2020A09CD1DF7C741DFA0D56A7496CC8D78A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....1....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yY/r/mCqfpPPW9ho.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....R.....".....3.....y.kW. .S..>.H..A..Eo.....MN.=.....A..Eo.....'.....O.....t..5.....(S.....`<.....L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Q c.h,.....start_js.....`.....M`.....Qc.....aNSDH.....Qb.1tb...__d..(Qh".....ChatReliabilityTypedLogger.....`.....M`.....Qc^..[....Banzai... Qf..=.....GeneratedLoggerUtils.(S.D.`D... ..L`.....0Rc.....O.`....I`....Da....J....(S.....Ia....{....P..rA.....@.....@.....@.....@.....@.....@.....@....I...!.@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yY/r/mCqfpPPW9ho.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....`z...&...&....&...!.D&.(S.D..`D.....L`.....8Rc.....O.....a.....I`....Da.....*...(S.....Ia'.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1e1f711d389d6632_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	17640
Entropy (8bit):	5.84373733795933
Encrypted:	false
SSDEEP:	192:1RMd5wIPoztGbZZlLqTYy/DzT0twna9dkdTK2vt3lhUW+1gKgHU+kNxa8p:1Rk5M4bvkXDVK053uQMtkm8p
MD5:	023EB94937A560DDE029FE6676A4BA90
SHA1:	C30E9EE8707E8E221BC26B913E8FC4216485B6CA
SHA-256:	CDD0B59AAA60D54D0BECC4E39E6124BC6BD9EFF43BB7536D3E0E4155CB5518BB
SHA-512:	07BDA61D6FE6C205294B62CB9143ED437481B2863E5D5C304EC48B728B2B2D64C06A816B0B4E3222AF53A490DA556F88979073BDCA5B7BC6CE34D0FCC60C916
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....]....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yJ/r/gJ2DXYeISll.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/~...u./.....t.....%...E>R.a.e..[..P.....qz .....A..Eo.....{.....A..Eo.....'..{....O....HC.../.....(S.U...`b....].L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....st art_js.....`.....M`.....Qc..7.....0gk7U.....Qb.1tb...__d..8Qlb..r)...QualityOfConnectionsExperimentTypedLogger.....`.....M`.....Qc^..[....Banzai... Qf..=....GeneratedLoggerU tils.(S.D.`D.....L`.....0Rc.....O.`....I`....Da6.....(S.....Ia.....I..y].....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@....I.....@.-....\ P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yJ/r/gJ2DXYeISll.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`^...D`.....`I...&...&..q.&..A..D&.(S.H..`F.....L`.....Qd.R .....X Controller...QcZ|bF....cr

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f5d1d09f52c2a0c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	379
Entropy (8bit):	6.037656557067488
Encrypted:	false
SSDEEP:	6:mr9Yk+f2pomWdCUxPhmJ2EJK6TjQKEzlKwDK6tGs/VVjxU88V+AMALQKEzlK:Ql++amIHkJiCQK4b1lFU8809ALQK4
MD5:	6B3C2F9C42CAA76B652D2FF3A6DA4490
SHA1:	0147D7449FDC9F23AF2E61E2D07CA30DE9EBD34E
SHA-256:	67C59167A5E06CC124B4713927B2FC7085EF976F9C1E326606B53C5E05D1AB80
SHA-512:	2721269240D9AEDB60211CB0942A4F52941D600567B4CEE5F85E8D13921909E339E9DA17DE334E060888A5807B6E12E2367F4D60B10C944DEBD5DCC70829D1BI
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....C.D...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iGD54/yL/l/en_US/gsrgPauTlZK.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....6.....m.]*.E..G.N.. ..=s..?F].SI.....A..Eo.....EwS.....A..Eo.....u./.....BD9FBC20F2DD6B376D2FC2676553F018212860E2EE3E90681A648073111D9A60m.]*.E..G.N....=s..? F].SI.....A..Eo..... L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22d5bf2d2e4b1b94_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	261
Entropy (8bit):	5.577478316155585
Encrypted:	false
SSDEEP:	6:mAVYj018IrAMUscnQ42X/ViRWnvpMqQGZ4OdD2iaDK6t:51thUsYQV/VGWnaOnd+1
MD5:	5CA040A0FCF4CB41C0075A42A1FE1C66
SHA1:	0D8C7A1BBBA947E01CD7B68463EB71738AD36819
SHA-256:	59F21B3AF1C8E7DAA00037BD951B4C275F0A90098BC52C12FA665CF4AE51D2CF
SHA-512:	C25A52AFB34CCA13D6FE44A290AEEE1CCBB10A5425B566BA614B8340220ADB9613781B58D688BCDA67923B80AC3EC03A6D3E371EF527E6E0E5881603F901904 1
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22d5bf2d2e4b1b94_0	
Reputation:	low
Preview:	0\r..m....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~bundle.Explore~loader.ExploreSidebar.d931fc25.js .https://twitter.com/....u./..... j.tQ. ..r]co'...q/J[...N...Q..A..Eo.....İ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\24dc2b696914d6eb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.5288025491025845
Encrypted:	false
SSDEEP:	6:mxnYj018IrAWQQckQMjyPFfFp0y+4athK6t:w1tBQQnL77t7
MD5:	0791586CC6AA288B034D69E477CBD6D4
SHA1:	AF516D2D7B05444C7621902D044E660B4D747945
SHA-256:	487594F4DE5614DAA8FB91822E55FDD6746EE5E5973C78AC1A0F18C4D8AE8D5C
SHA-512:	52E5DEA34B11BDD99BA4E57D7E924505E449C5C828EE714ED8D9061F47A93B02FFF4D01EFF144540FE213E4C2A696912BA61BB0E436F29757F628FF88D989D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...._.....,_keyhttps://abs.twimg.com/responsive-web/client-web/loader.SideNav.cae9d795.js .https://twitter.com/....u./.....*.....,..`....?2.).d..N...7GK..U.s A...A..Eo.....Vs.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2634b6e1ae1cb852_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.443571862642274
Encrypted:	false
SSDEEP:	6:mG7qlVYj018IrAE7uPTgePspMSGMbAMFEeRzCFprNK6t:xCN1tnuPcemAMK6Cjr
MD5:	1B8FBEB36B8512F0101C7DFF3C62EF50
SHA1:	3AD68591AEE1C03C034A5D0F206AADAB3E4ACDBB
SHA-256:	7C98279EC783E51757EA1FC38953A777890679D87A008DC9322A7A150908922A
SHA-512:	2F28519A5EF4AED731CA5D74BE909DB568BAEEEEE6B0916352D26E3208260CF70BEA52BAF1BAC692FD483167C6593C3778EF0733FA5461B42E0E35B6F41B9AA A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j.....ro...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.AbsolutePower.2f2dcbb5.js .https://twitter.com/.*.u./.....em.%|...=S.j`. =....P. .`/.....A..Eo.....$..t.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\26cdb4c6b74f6afe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2743
Entropy (8bit):	5.664855780536826
Encrypted:	false
SSDEEP:	48:wL/nSL70SLNTSL6ySLG2SLjvDSL1t1SL9gSLNASLXNSLUI6SLDc7SLBRn:wL/SL7DLNmL6xLG9Ljv2L1tgL9HLNnLK
MD5:	3BC7EC549AA83887E867979170222E10
SHA1:	06BFDE9C97F88678232C53E65616A0E7D5E022E6
SHA-256:	3954554DF020F8FF33439587BF4F332E060F35F1C6595A4B62945C799BB9F9F0
SHA-512:	B6A61990A25C692B2790C1C95FE503F5904C46CC4F35B3E0D859A6163207ED535E2AF73CE00EFD861686DC8A0BA4C36FB42162F201A0E6BBD88C045B9D4AEE9 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....&....._keyhttps://www.google-analytics.com/analytics.js .https://abmcovidvaccine.com/....u./.....Z.....H.....V..d..U.....K...}..A..Eo.....F.5B.....A..Eo .....0\r..m.....O....&....._keyhttps://www.google-analytics.com/analytics.js .https://abmcovidvaccine.com/.R..u./.....x~.....H.....V..d..U.....K...}..A..Eo..... ..%.....A..Eo.....0\r..m.....O....&....._keyhttps://www.google-analytics.com/analytics.js .https://abmcovidvaccine.com/a...u./.....H.....V..d..U.....K. ..}..A..Eo.....A..Eo.....0\r..m.....O....&....._keyhttps://www.google-analytics.com/analytics.js .https://abmcovidvaccine.com/....u./.....&.....H.....V..d..U. .....K...}..A..Eo.....k.....A..Eo.....0\r..m.....O....&....._keyhttps://www.google-analytics.com/analytics.js .https://abmcovidvaccine.com/..C.u./.....H..... V..d..U.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\276f68a52e4d6ee4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\276f68a52e4d6ee4_0	
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.602310486750327
Encrypted:	false
SSDEEP:	6:mMEYGLDlynflGSF5XilyRR144FFgdhgDK6t:1flGSLXigRTFM61
MD5:	6CB1057108C58C914106D09509F42CB6
SHA1:	66CA56F87BA7977B3ED0FB928579DF91997E1994
SHA-256:	5F3D8D8B25BDFCFA94208E16A95990FAF8AA42AE30E2F007D6C4461E027B483A
SHA-512:	94110F7E96CA38C911CCED15D896B4045BA89843B65C9379BC0D04F92EF41A83C470396B7A09EBE94C0E04DCAC9C6E199FB523766BB7F6D386B6E62A55FD875 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...P....._keyhttps://www.instagram.com/static/bundles/es6/FBSignupPage.js/4bd13ed69872.js .https://instagram.com/....u./.....u.....#.+ .AK...=`6\...Xj=.... .....V.A..Eo.....uD.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2855e9c53078550e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.511675795748065
Encrypted:	false
SSDEEP:	6:mmX6EYkvwyy1MeNmfN3j0vlpsNY4k4lK6t:zXzvwyBeNmfNTlUIw
MD5:	FC0F1B02340D0375C2FA99740BD86693
SHA1:	71CA8E34CEAB86A57ADCBE59F683216235BF61AE
SHA-256:	939A5307336F18F30710B37761E0246240D984198C7BF4FFE0F0B390A0C662A4
SHA-512:	F7970159732E0D4C01102BBC5ACFF568157C5147992E41DC696C35CDE695DF4B3D9F58EB71014F1E865ED5BE8241B42302A32626CDABC3CDC147F91CD1ABD5 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...$7g....._keyhttps://static-exp1.licdn.com/sc/h/cjdtbm4q6e6q3rw3okr55eu4l .https://linkedin.com/.]..u./.....!.....%.....j.@7el.{.....9..jc...A..Eo.....E.M.... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\28ecb4a79ba7dfeb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	11544
Entropy (8bit):	5.715590729371457
Encrypted:	false
SSDEEP:	192:wUU20dP3dPSOTdB40EhFgof4FxhSpZFuwcgy5Z0Ob93rNPu6d+F4:wUUBzPVEpUfslgLb93xf7
MD5:	592343F6EDF6F950951B9760E24E2B6D
SHA1:	66516676C6DF334DAC697C9F0EAAD380407BF5F2
SHA-256:	3F597729A9098B6D891FE18E68FB5A056E091EBE4A23A9F5C7831A8977ACBB46
SHA-512:	1DF56CA4511E75097F81844B62BC33072395BC0AAF9725CC444DCB1FFEA58B1980B31D649450F8DF022F0DF03F32C9409EADECF4158266E965604D97CBF9DAB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....f...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yJ/r/Lc8ECXL-UZC.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....h...~doe.u.L..4....|.6.... <0..A..Eo..... .....A..Eo.....'.&?....O.....+..]L.....(S.....`l.....L`Z.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js... ..`.....M`.....Qc.....2EENj.....Qb.1tb...__d..$Qgf.....EventPermalinkURISetter....`.....M`.....Qe.....PageTransitions...Qb6.!3....URI..(S.T.`^....$L`.....8Rc.....O .....a.....I`....Da....T....(S.....Ia....c.....M.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yJ/r/Lc8ECXL-UZC.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`D...D`.....5.. ..`....&...&....&....&.(S...Iam.....Qb...C....c.....d.....&.(S.....Ia....).....d.....Qb.L.....d.....d.....D&.(S.<..`.....L`.....0Rc.....O.`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\29153dfa3ae67bd6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	5.794469925381997
Encrypted:	false
SSDEEP:	24:nnVb9mZPu7H7gMYOe/d5X0tsddR1cnVb9mMbbvBeuifbd0iJTJ9hZ:n4G7a/ALFlxjdTJ9/
MD5:	682A499CA315EE2C01F3EA85B5F04C9B
SHA1:	6DE54948C6CB3DADE9376B016F2544CD3D0ED465
SHA-256:	15E3D540C0C922640CFC600E98D2FC8F0A477200CA81281C4618599D54C691F6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\29153dfa3ae67bd6_0	
SHA-512:	0AC061FBF68CF7BB7AA7904D68FCE14ACC2456D25F728BDC7AE37A32223802B69C49F86FFCDE3BE4F5E70E21B74F8313D48123B7772DD669D3A57CB77EF1E54
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....t.#...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y7/r/FZd9_oPUnsJ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....$.),.N.W...].J>o.o.Q..T.{0..`.A..Eo.....A..Eo.....u./.....'.....O.....y.F.....0.....(S.d..`.....(L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.M.....qcZAr.....Qb.1tb...__d.. Qf...w....intlSummarizeNumber....`.....M`.....QeV.)i....FbtNumberType....0Qjj".Y$...IntlCompactDecimalNumberFormatConfig..Qe.....IntlVariations....Qd...`....intlNumUtils.(S.T.`b.... L`.....XRc(.....O.....Qb.....h.....S...Qb:..4....j.....Qb.p.....k...e.....I`....Dax.....(S.....Ia%...M.....M...A..@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/y7/r/FZd9_oPUnsJ.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....`....&...&....&..a.&.(S...IaW.....!....A.d.....`...

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):	5.6147531897859215
Encrypted:	false
SSDEEP:	6:mu/XYj018lrAMUowfs21fKYvpMF0gtwuoRo4aRK6t:T1thUU29Kt88r
MD5:	A5C3A812ACA1F2984254095C85E613F3
SHA1:	CE3298D046715DBD572EEDCC2FFC055325A14FCC
SHA-256:	25DA2D845295EC3BDB089932D65AC451BE7F664E131B79503EB15D5AA7087772
SHA-512:	4C6C664590D19861B23603482A7D3B778F027025D699A5C2F7471DAEC9A62A638335DA79FA6B9C3588F9EE463EC794B5A3D71512ABC3597AD28FFBF203CBD3E
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/..a.u./.....0...j.x.*s.B..."._.f...f.K.:<.R.A..Eo.....H3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2ccaa17c5b2630b2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	116704
Entropy (8bit):	6.098854244787223
Encrypted:	false
SSDEEP:	1536:fZJVsrByZno8ywBK3A627tn0r+qjX0n28YnkN1rkHkEIz:jV2aL68tn0xFn6AkLz
MD5:	9ADF9C3D374FA1808E12581CFE2E471C
SHA1:	81C528E82FD192CC7F2CEEFFFB4E73687B2C0956
SHA-256:	2419FAA3BC203275C81E3C15CD283FCA430954C37ED822DEC8D7861B6493296D
SHA-512:	B9F5046B8BFD85A72E4649462EB2130B262ACCAEC800FBDF5A1ACA1978D9A253503522EFEBD742525354BFBD28F0595F23DB63776713EFDD4D42C81F784B4E69
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....527A9D383D4FC3666787C206857EF3E75755AD800721F3F7D00B8DD1F31AE385.....'.nK....O(...p.....m.....(.....X.....(S.....`.1....U.L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.`.....16LYZ.....Qb.1tb...__d..<Qm.%Tq....FeedStoryUFICommentActionLinks_comment.graphql...(S.8.`&.....L`.....(S.....Ia.....IE.@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3irjT4/y3/l/en_US/I-oh63DaTQ_.js?_nc_x=Ij3Wp8lg5Kza.....D`....D``...D`.....e...`....&...&..1 &...!&.(S.0.`.....L`.....D..a..... Qf...K....argumentDefinitions....`.....L`.....a.....Qb.5?.....kind..QdB.\.....RootArgument.....QejP.o....useDefaultActor....9..Qc.....Fragment..Qc.....metadataF..4Qk:O<.'...FeedStoryUFICommentActionLinks_feedback...QdR..:....selections.....`.....L`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d9c625b3c10b617_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1680
Entropy (8bit):	5.74566025532648
Encrypted:	false
SSDEEP:	24:HnVKzczd7gjFonGlxcyUGa11cnVKzfpBMdtgEJptpwqKkpBeJv0J:H4giHccr4kIEJDPfoJvs
MD5:	F1EF24CCBA53098656AC1E69B119F67B
SHA1:	08E03F159DB7DAD7F6CDCBB389C88D21CBE2AFAB
SHA-256:	8B22EB58684FCBA84D42AD27735124976A6E9985ADA1A5E15855D16A1F341B73
SHA-512:	A232AACA8A01A8882FD00D71E9EC117D2EB084784E88DBF0343067CF9F1B0BAE16E635B21A0533B3C4446573EE1E8C3E1891A021016C6C597893B9DA8904906(
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d9c625b3c10b617_0	
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yg/r/8iyi8cdwOLY.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/Oo..u./.....D...../..'...F.&.P...+..... <O..A..Eo.....Dq.....A..Eo.....Oo..u./.`.....'.....O.... .....k~.....(S....`.....0L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.. ....M`.....Qc...C....vb6jB.....Qb.1tb...__d...Qe.....OnVisible.react...`.....M`.....Qc"i,c....FBLogger..QcB.....React.....Qc".$`....ReactDOM.4Qk...'...intersectionObserver EntryIsIntersecting.. Qf6.?.....observeIntersection..(S.X.`j.....L`.....8Rc.....O.....a.....I`....Da~..&.....(S.....Ia.....T..rB.....@.....@.....@.....@.....@.... ..@.....@.....@.....@. .....d.....@.....I.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yg/r/8iyi8cdwOLY.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....D.. .`....&...&....&.....D&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3163c1abddb5daf8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2864
Entropy (8bit):	5.790699191411214
Encrypted:	false
SSDEEP:	48:I236ihm60QtAGT86t2ecipDRwxSq26qzQhGnXl:I2ebQCGT860evFqhvWl
MD5:	1E9AAA5FB3D4D0082A730F5454C2368C
SHA1:	DE3F413ADA14F4697EDA6E44A2DDFC9BF7F8126F
SHA-256:	AD7F520D3BA37334A83D90B476C4A74B26ED67643009A2F3D3180FD917F55D98
SHA-512:	3F65D36A9A3A08F817F7478A107F1F9050CED84E09D1FA5EF52379C470DD69CE28E1DFE014D6F88842776E930397BB7AFBAE44F733635F222F9A63EA266EB573
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...pC.|...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y6/r/fn-nWQ9Q6Ak.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....8....s/...O.q..F.B..%.. .....A..Eo.....1=.....A..Eo.....u./.....'.....O.....9.....h.....(S....`.....@L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....` .....M`.....Qc.....dyAtU.....Qb.1tb...__d..8Ql...+...RequestStreamCommonRequestStreamCommonTypes....`.....M`.....Qe.Y.c....$InternalEnum....(S...`.....4L`.....Q..$..a..... ....Qc*.\....Accepted`.....Qc..k.....Started.`.....Qc..H.....Stopped.`.....,a.....Qc>Xr.....Rejected`P.....`d.....Qc*.....TryAgain`.....Qc.Y.....Closed..`.....$.a.....Qd... ....BestEffort..`.....Qc.....Socket..`.....QcZ^.D....Device..`(....<.a.....Qd.(.....Flow_status...Qdr.....flow_status...Qb..S.....Log...QbZ.;u....log...QcFn.I....Rewrite...Qc..... .rewrite...Qb:..L....Data..Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\321c89a0cf980c7a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	39515
Entropy (8bit):	5.912996918312795
Encrypted:	false
SSDEEP:	768:ofVGYHaepJ3iUp2tOPzj3COJZFLF3EYP3ixnnZCIl0:ofv6ezi82yF0GgnnAs0
MD5:	E1EF3096925EF6BB5CC1681A7B2AD036
SHA1:	57051D71FB1E9BE9ADA0D2A0458DF19CB74C9B70
SHA-256:	5EDC6852E66B552DA61F1537F7A30883B5986DA1CBB52FCF59B0147C28E7F762
SHA-512:	FF1931B78222E69073B070777F4790A1DA7804829F9184B80767D248BA7AF6A7F0FFC6FA3EE234F9B9A8619845C878268070C637DCAB76F85A2A89AA7E877721
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...\.#...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3icrf4/yc/l/en_US/3K56jq1-BJo.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...u./.....Q...t... S;.5..15.v...wwL.A..Eo.....d.....A..Eo.....'..(....O.....U!.....(S.....`.....L`.....Qbj$.....self..Q.`>n.....Caval ryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.....qcyed.....Qb.1tb...__d..0Qj2..[$...CometDisableDarkModeMutation.graphql.(S.8.`&.....L`.....(S.....Ia...;...IE.@.-....dP.....X ...https://static.xx.fbcdn.net/rsrc.php/v3icrf4/yc/l/en_US/3K56jq1-BJo.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`h...D`.....U....`&...&...&...-&.../&.(S.8.`&.....L`.....(S...Ia....H.. .IE...0d.....@.....Qc^.....exports...K`....Dh....8.....&.\..&.%.-.....(Rc.....I`....Da.....b.....,...d.....@..@.....&....&.(S....`.....LL`"....XRc(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\35272284e7d1ddc6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8288
Entropy (8bit):	6.034400817619577
Encrypted:	false
SSDEEP:	96:RzQFH5hXDWqMgcwSP6WL3/3qpS0ihtVJTf//uCzrg5Qhw6+f9CF+4vLhiFDuipTg:RzQF3TFMgvSPL3/3qo0sdXhgCDtiDhg
MD5:	46A152480990DD0AAD6CB9EF897F2847
SHA1:	8673D54539860B5C2A249CAB2970641C4AB4B5E8
SHA-256:	E3062B9217D72269D9B4C1EC58B710F8F078C4CCE7968D3CB5FB5C14A83702DE
SHA-512:	52EC0A01A3CC6D486C7D2B8EEF1480CBC3D69BECB21195A2994A48DF0E6278F649042FD80C99DF59EA3FC919B1FA09EEBBDC65BFD55275F10E14B04377C854 12
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\35272284e7d1ddc6_0	
Preview:	0\r..m.....h....(....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yR/r/X7uk38mSJJh.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....N..U.A....|iB.b.$..I..KY. j..O...A..Eo...../VP.....A..Eo.....'.?....O...../7Qs.....(S....`.....IL`2.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`... ...M`.....QcfC6.....SLAWL.....Qb.1tb...__d...Qe.....ChannelConstants.(S...`.....L`D....0Rc.....`....I`....Da.....Qc.6.....channel/.....a.....0Qj....#...CHANNE L_MANUAL_RECONNECT_DEFER_MSEC.`.....$Qg.....MUTE_WARNING_TIME_MSEC..`P....,Qi.(qg ...WARNING_COUNTDOWN_THRESHOLD_MSEC`0u....Qd. .lc....ON_SHUTDOWN.C. Qf..-....ON_INVALID_HISTORY..C..QdFhF.....ON_CONFIG...C..Qe.Gl%....ON_ENTER_STATE..C..Qe.#.....ON_EXIT_STATE...C. Qf...;....ATT EMPT_RECONNECT...C..QdJ..#....RTI_SESSION.C..Qd.....CONSOLE_LOG.C.$QgB..f....GET_RTI_SESSION_REQUEST.C..Qd.:.d....SKYWALKER

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\358a20822d05d974_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14808
Entropy (8bit):	5.792214001656879
Encrypted:	false
SSDEEP:	384:ohTqiRlbV3z4lbfxYCh6lf0KbRytQgnUd3:ohTqsWlb+ChhKVKQgnu3
MD5:	843A50062F3F365BE2118973F45AFB63
SHA1:	6868576636AFC46222D12B3D3975B96273C07646
SHA-256:	1B85CA17D0E05357CD0D8E49BE1958C88BCDD9B6ABF640668045CFDD13835B11
SHA-512:	FEDA0CBEF67906DB4BDFA83A83A93D4DD0AE930F5AD6F10C4A7A31BC6719FA80906CD2164C62F568388CBF15A38AF5ACD894F630EC5434B043F2BCB34A256 03
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....p....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yx/r/-z0NZqsVLWj.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....'.....BR.J.T~..[Af.P.TQ.O7.|. ....p.A..Eo.....+.....A..Eo.....'..5....O....@8..".8.....(S.....`.....L`J.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js... ..`.....M`.....Qcj~.....GdzBB.....Qb.1tb....__d..$Qg..c>....EventListenerImplForBlue...`.....M`.....Qc.....Event.....Q.P&.....TimeSlice.....Q.`.....emptyFunction....,Qi.z;.....s etImmediateAcrossTransitions....(S.x.`.....HL` ....8Rc.....O.....a.....I`....Da\.....(S.....Ia.....d.....(.....@.-....\P.a.....M...https://static.xx.fbcdn.ne t/rsrc.php/v3/yx/r/-z0NZqsVLWj.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....`....&...&....&....D&.(S.....Pc.....a.listena.....Qc..D....listen.....d.....&.(S.....P d...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\35db5d4b8d812ed5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.5524714449628165
Encrypted:	false
SSDEEP:	3:m+lFBIa8RzYj0KKKXlMMIrAkRNEHFL0DlMRPYD1lHCZynlX4wj9lsNkGq7FkoyR6:mKkYj018IrAkRfpM9YGZyEpRvAtbK6t
MD5:	4EC1AC5BC626E3BCEB7D59FF06AEC667
SHA1:	8D42B5346430DC12B62C3D32C8E41AFFEB0A1463
SHA-256:	7F480751DCE85776C8517A49F61AF08F394E56AF5DF1C62708D2DBBE975EB280
SHA-512:	4939100A45F30BAC4C74491A3D4FC1F14D765467812D09F35FDCAA07336D2CB715B707A5082FED5D49FEF41517A67A39E7E7ABE901E6AB210B6CB6CCC1CEE0 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....+....._keyhttps://abs.twimg.com/responsive-web/client-web/i18n/en.6035ab55.js .https://twitter.com/.(..u./.....E..U..dj.r....8.C+@)n...c..I,Q..A.. Eo.....W3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\38e541f701915d70_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	56171
Entropy (8bit):	5.931863574299166
Encrypted:	false
SSDEEP:	768:rSOSqMmJcup2EBkWRQnY0EuDmiIWcl1HrqH0kg3smm6P+WeMIdLEhmP+H351/Zs:rSRqx+EuadWGlqM3AO6EhmP+H//Zs
MD5:	C2C2DFFD05972C39A439A72D137DAB8C
SHA1:	1DBA9A0F2DA41055C3305B81D94446A1BD598ED2
SHA-256:	5AAC4765AE93CFC31F132B83B90F691498653F25FA7B00258801B2BD3F12CF6C
SHA-512:	0CB0EFA45F1B0C337D0E46EF7280D922648D7C4920405C532336EB6456672B68B37133622C446D3EF12F0DD4BDD836D57774E1E8DE6E91F8057DB296BD488776
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...2.i...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iJBN4/ye/l/en_US/NdCj_jA-cDu.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/I...u./.....(I.n.ov..!. ..4]5...#..)-7."...A..Eo.....I.....A..Eo.....'..$....O.....8.....(S.....`X....!.L`.....Qbj$.....self..Q.`>n.. ....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.....yN3Xi.....Qb.1tb...__d..0Qj....!...CometDismissFBNuxMutation.graphql....(S...8.`&.....L`.....(S.....Ia...._...IE.@.-.... dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iJBN4/ye/l/en_US/NdCj_jA-cDu.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`....D`.....`....&...&...?&..!.&.(S.8.`&.....L`.....(S...I a.....IE....d.....@.....Qc^.....exports...K`....Dh....8.....&.\..&.%.-.....(Rc.....I`....Daf.....b.....,..d.....@..@.....&....&.(S.8..`&.....L`.....(S.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3967c78861991466_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22552
Entropy (8bit):	5.737430006362414
Encrypted:	false
SSDEEP:	384:AlnqKyAwyWKxkso0lzIwEKU8Lnf16rSCeS7EUjG3jalc:Al19fxkso0ienoWCv71jG3jalc
MD5:	72C826B21B7F2ED389D82843EB5C48BA
SHA1:	3A27B4145EBF37DD21FFDBFD4A37A742458B4CE3
SHA-256:	B506AF8945B7B1AF08E2F38E1737FF228FAD7FAC900E732958DD81642C225A42
SHA-512:	120B367C78884120D988048F0BA92CAECCAC3864E96DA14DCEFBA10DBA6A3D851912BBCB34FB676F0D5B6F8CA065E132E9DC924353DD74E24FA931BCA53C185
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...E..~...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yu/r/Xx81bxKYnCX.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....y..W..C..5..k.%9S&...2C.....A..Eo.....9.....A..Eo.....'.....O....xV.....d.....(S....`t.....L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc...@....QEGHK.....Qb.1tb...__d...QeFk.....BlockMapBuilder....`.....M`.....Qd6.N.....immutable....(S.P.`\....$L`.....0Rc.....`....I`....Da.....Qd..!.....OrderedMap.....a.....Qe&8.D....createFromArray.C.(S.....5.a.....M....a.....1.a.....d.....@.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yu/r/Xx81bxKYnCX.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`j...D`.....a....`....&...&..Q.&....D&.(S....`X....8L`.....PRc$.....Qb.....h.....S...Qb:..4....j.....Qb.p....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ae39c3c9b31d772_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2272
Entropy (8bit):	5.709112334784234
Encrypted:	false
SSDEEP:	48:wshwMNVhPeqPtSWiSN0wPV4ff7zsOQTzhB:wyxNTdtSWiSN3Wff7p6B
MD5:	B168D6F5CA33901E796F25E53074A5B5
SHA1:	D2B68E608DDD89E3F734F757C57B285764007E0B
SHA-256:	9370ED66B7347678ADD295128307F7981658B8F6EFB96E004A967FED902BF386
SHA-512:	43FD1690D1D1BDAD9DF3466571530C6D3372870B42CA166D23CE2937AEDAD05C8D1214FDE4663C0DBFD028A58EB4222CCFE5EA84AE5DCDE61787B76C02ED02D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...(/,....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yp/r/JVKVtmNda5g.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....-8])...Q..P`l...gE.$e.....8....A..Eo.....K.....A..Eo.....u./.....'.....O....p....|v].....(S....`....<L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.....1MFXF.....Qb.1tb...__d..$QgR).(....QPLAddBlueRequestHeaders...`.....M`.....Q.@..$.....Arbiter..$QgB.:.....QuickPerformanceLogger...(S.<.`.....L`.....0Rc.....O.`....l`....Da....(....(S.....Ia.....d.....@.....M.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yp/r/JVKVtmNda5g.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....d...`....&...&....&...q.D&.(S.H..`L.... L`.....(S.....Ia.....M.E....d.....@.....(S...Ia....u.....O.E.d.....@.....(S...Ia....'.....Qb...C....c...E.d.....@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ca44ab12f4efada_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	379
Entropy (8bit):	6.024354731477308
Encrypted:	false
SSDEEP:	6:mXnYk+f2pomWIUbKv2Ch6zhmJ2cGdTtQHSC4V2K6teyA+1vRgkpqiKnztQHSC4Q:uD++amoY2CszkJDKBSSGVhRgiqHhSS
MD5:	FDA4F176AD372371A9DCE6A540FEF31D
SHA1:	A9B4B20F60FBAF4AF72C4ED14AC0FD5288B7E096
SHA-256:	75494083E8D7EA15F74878580F54274D7F974CC99BE82DB73EFBF975F0478AF0
SHA-512:	23B034D760E43A35C611968E53F0AB7AEAF0BD64480203A9EC5A1916349B35042FFDD2FCDC6F291CD62F27371857BBD5D524D72FAF3A7CCE2476BDCE57CC718
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....P....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3itji4/yN/l/en_US/POy4OSHUNA_.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....}!...sO.}.....eV~.".. ..n+...A..Eo.....Db.....A..Eo.....u./..7..90C4CC710E85B38B272A3434BA3FFFAEFAF272FEBA2D3966972386571FEE8EFA...}!...sO.}....eV~.".. ..n+...A..Eo.....?.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\407efd6a85d9704e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8664
Entropy (8bit):	5.838857972998041

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\407efd6a85d9704e_0	
Encrypted:	false
SSDEEP:	96:F4lB3MJEgSsblYm4GaH9Ma3NjUd+LNd9pyYnf6bbZ0ifAzrqcs9LGQjr2359OOH:F4lB3MJExGJ4JndId+L9py6fOBvLGlzb
MD5:	09D1613EA25A19E1ADBCD8727A652EAD
SHA1:	97947E96354D080D5763F6C208D9AD27384509AC
SHA-256:	BDD03D943466F0B6C4D36C60B04BDC2851C4E4C32A93EA64C7AFDFD78647C9FA
SHA-512:	208ABCE78E63B8F133BC78F26B27534887C63D38090744AB836B9D145EF2986FF9DF24000CD107294E0A09FA2E4DB3AD93D3F07E0EF36B86B12D00EC31272241
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....A=...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yd/r/RTVjqXpUeRp.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/o...u./.....P.....4[...$8%._...P.qof.8s. ...*)...A..Eo.....9.....A..Eo.....'.. ....O....H ...(.....I.....(S....`.....`L`,.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.... ..M`.....Qc.@m0....wwhGv.....Qb.1tb...__d...Qe.x+.....stableStringify..(S.<.`2.....L`.....8Rc.....Qb.....h...a.....I`....Da.....(S.....Ia.....A..@.-....\P.a.....M.. .https://static.xx.fbcdn.net/rsrc.php/v3/yd/r/RTVjqXpUeRp.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`R...D`.....`j...&...&..Q.&..a.&.(S.....Ia.....d.....@.!....!...A...A.d. .....@.....D&.(S.]...`t....LL`'....8Rc.....O.....a.....I`....Daz.....(S.....Ia.....d.....(S...Ia.....M...d.....(S...Ia.....Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\429bc8764e94c711_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10232
Entropy (8bit):	5.936231126556763
Encrypted:	false
SSDEEP:	192:Tw87dQwia0Bd9dNInMgqqRRgB+OXHpUYt9+S3b:T9CnrXNmMgqcRmuH8
MD5:	63D1935DA209A62E2396ECCC4CF973B8
SHA1:	6D405BE588DD4C9EDA39C1E4BA9BFC112333DBDD
SHA-256:	8D35E34D6A69F5D56D388579B6A77BF172FD9AB714673903156E7B0B67446714
SHA-512:	91D120C4ED3992A26FB7C6A8A7CD417E92EA6962A96C4B3095BC6892CC6941819BFF60E4B4A37ECD6579802F8E721DE8588D690E3D038242DC3E098E500B01C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....7X...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yJ/r/-L9c_oAt3hw.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....W.....B.<.zr...i..0..... ...A..Eo.....F|.....A..Eo.....'..~....O....h&.....p.....(S.M...`N.....L`>.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`..... .M`.....Qc.h.....GXq1C.....Qb.1tb...__d...Qi..M2....CometTranslationDetectorContext....`.....M`.....QcB.....React....(S.D.`D.....L`.....Qen!.....createContext.....Qc^. .....exports...K`....Dk....8.....&.]...&.(...&..&.Y....&.%.-.....(Rc.....I`....Da.....c.....@.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yJ/r/-L9c_ oAt3hw.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....`v...&...&..1.&.(S.T.`b.... L`.....8Rc.....O.....a.....I`....Daj.....(S.....Ia.....d.....@.....e..... ...@.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42c00e799e52f1d7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12344
Entropy (8bit):	5.819326214050629
Encrypted:	false
SSDEEP:	192:JNS1thzLtE2MiM99gaFKMC7ycKTUvpBpymnC8PDoIPZ/wdq1MUkhep:JWhzLt1M/bk7IIL7Vl1bkhG
MD5:	C5612A9F29721F71C5CB3CA2DB6391C4
SHA1:	AE637F99420F7A55AEEA3566C80BD6C6F1A09600
SHA-256:	C92D31344BCEF905EF130B28A6E9F04319188A6EEC9EDEB5831A07051EC0F1F6
SHA-512:	BA3C8EACE1F4148F62F153BCAFA54DDCD2962155D79DDBBC7EE7D2EE273CEE2D4F8A79244BAC1F7A9D66A8B786EBB09763BB77F0A6E480C28E2DCC32D9D5 1A62
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....;...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yL/r/aN4b4_zC5e6.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/C...u./.....5..DB...0..=.W.=.M..aW f.....A..Eo.....&v.....A..Eo.....'..(....O.....1.....(S.-...`.....tL`6.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.. ...`.....M`.....Qc.sMd....KA9YB.....Qb.1tb...__d...QdN..h....ChatOpenTab....`.....,M`.....Qb.f".....csx...Q.Pn.v:....Bootloader....Qe.&<.....ContextualThing...QdB+.....Current User...Qc.....Event.....Qdb>.Q....MercuryIDs....Q.@VV.....Parent... Qf*.hB....WorkGalahadSettings...Qd.W.....requireWeak..(S..`d....|L`:....XRc(.....O...Qb..... h.....S...Qb:..4....j.....Qb.p.....k.....QbN.....l...e.....I`....Da.....(S.....Ia....B.....d.....@.*.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yL/ r/aN4b4_zC5e6.js?_nc_x=I

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42c72aaec1d4bf15_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7547
Entropy (8bit):	5.564956440482727
Encrypted:	false
SSDEEP:	192:JE1GdUj5J9PqsosWAkalSDYWRpOxz0YhpPWE9ajHB:JEAUJ97Aaq+6Cf92
MD5:	A245D4FC1A850032CE8C69C38D99FDF5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42c72aaec1d4bf15_0	
SHA1:	B5C782C723CE7B2790E8E6E5F4BDE66F501AE0CE
SHA-256:	41C5AACE776BF668CAFFCCAE5778BC38F62327F61728FC0B95DD41CA286CFC7E
SHA-512:	1DB818116DF04B57A8146FD24937F9DD75985008FCCCE4DFE4BE10C20EBB47F0C8B6EBA6F0078A9A09CE1B1B6716091660DC02B0E7B0AD98F779BDD9D63B52 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....B....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3id1D4/y3/l/en_US/CZjfyYLnoHa.js?_nc_x=lj3Wp8lg5Kz .https://facebook.com/....u./.....(...../'.....Q. p.....\.-+.];....A..Eo.....A..Eo.....'.....O.....t0.....(S....`.....L`T.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_j s.....`.....M`.....Qc.\.i....DrIrb.....Qb.1tb...__d...Qe..0.....WebPixelRatio.....`.....M`.....Qc.^.x....SiteData.(S.<.`.....L`.....0Rc.....O.`....I`....Da.....(S.....Ia.....M.... ..@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3id1D4/y3/l/en_US/CZjfyYLnoHa.js?_nc_x=lj3Wp8lg5Kza.....D`....D`....D`.....`p...&...&..!.&....&.(S.H..`H.... L`.. ...0Rc.....`....I`....Da(.....(S.....Iak.....M.....d.....@.....Qc^.....exports.....Qe.R.....hasOwnProperty....K`....Dl....8.....&.%.-.....&.(...&.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4427a0214be5601f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.581827352169251
Encrypted:	false
SSDEEP:	6:mQgEYGLDlynflGgKPwlydcky56hr9K6t:oflGPIgea
MD5:	FA0906E3F46E439C92D3ABA1C080E5C9
SHA1:	2B19609DD368FC97B1391A7645C71B468CA646DE
SHA-256:	CD92777C135A77317EC31DCAD4B83BFAB65674E117D0035EF6D74B0551ABBF51
SHA-512:	55BC4E60243649EDA3940F1DE8D639FA56FC4CA398BABB43D4F3F485431137916501E4221E4779A2CAE72B65DC54E7FDDB79B7CC80A4174FDBC8C4B8E47587 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....T....._keyhttps://www.instagram.com/static/bundles/es6/en_US.js/1d557e6824b4.js .https://instagram.com/4...u./.....mP.|.....]U.>-.....5..>`.2. A..Eo.....1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\45ee6bf642a34fd7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	20056
Entropy (8bit):	5.82221358551419
Encrypted:	false
SSDEEP:	384:U+4aFbKn8k9e9L3JPpmYL19wrCsYdcWj1Pln1u:UZr45R1irNdWjPnU
MD5:	6F2200CD307ADA38DA7F3AA5D156F0E9
SHA1:	CAE5B78341D90468ECBF618D1938E6BF739B3BEB
SHA-256:	FF68EC74C99ED9E0205CAB3FAF69D6DE6AB0BE95164DF609E1B1AAD02B9D5AA8
SHA-512:	FCFE5D6F3A66F36E8E21695C714D8A6E9FC142EEE031B4AF4ACA80BEFD0936FEF7A6B9851E18637DF374B98EE9292C1D5FFDF64B31FA413CED6CF28F7F4FF5 BD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...).....,_keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yA/r/RSPXeIDS-55.js?_nc_x=lj3Wp8lg5Kz .https://facebook.com/....u./.....a.....Z.....|.....,v..g.`...Z.A.. Eo.....Q.....A..Eo.....'.....O.....L....e~.....X...t.....(S.....`.....L`d.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.... .`.....M`.....Qc.....HdAhw.....Qb.1tb...__d.. Qf.D.u....ResourceTimingStore....`.....M`.....Qd.....performance..(S..`Z....<L`.....@Rc.....Qb.....h.....S...Qb:..4. ...j...b.....I`....Da.....(S.....Ia.....!..@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yA/r/RSPXeIDS-55.js?_nc_x=lj3Wp8lg5Kz...a.....D`....D`(...D`.....`....&. ..&..Q.&....&.(S...Ia.....M.....d.....@.....&.(S.....Ia&...t.....Qb...C....c.....!..d.....@.....&.(S....` ....XL`(.....RcH.....O.....!....S...a...Qb.p....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\461f136cb8b4cf6d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.579398464580181
Encrypted:	false
SSDEEP:	6:mpPYj018IrA/PspM3q+AjOTrxvOGh1K6t:M1t40ajR5vOg
MD5:	8C4862BFC4B1913CB72F33FF7C215F84
SHA1:	8D5412B5C5E7008F2D8DB8BD9C0B022D53E15B52
SHA-256:	7B263F9A7E9F49D128581C45BC900D437DCC709BD05E43711A7465249890BB5A
SHA-512:	4DAA17BE2E98D4E486FD155EE5158F4CF41A1FA90A5D7CE11FDBF5150C34585BF2E24F1EBDC7F343817A74718F8EBF17C069690DDC0478369467AAC6B7D9A3 C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\461f136cb8b4cf6d_0	
Preview:	0\r..m.....b.....\...._keyhttps://abs.twimg.com/responsive-web/client-web/vendors~main.2166b255.js .https://twitter.com/t...u./.....J..P...6..!=#.B..@..C...l*. .. .A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\46b15ab9a6d89021_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	17984
Entropy (8bit):	5.917211459643863
Encrypted:	false
SSDEEP:	384:+7MiLsOqBmIWXXuMRQS1QlxNMFEZazzMMtEW/1NU/3Phx2WxGem:+7MeqBtWn71Q/HStBNU7Qem
MD5:	4012CB5CE1BB83E337CFE9E64407A9B3
SHA1:	B0F47B611259D3F7A48343D44C05D31441657F82
SHA-256:	A8079720754E7FED96E708B6D3D3535C4DAD1F8670538AE6B5703CEFC111B941
SHA-512:	3405AA6A9D8D726FDB77B180BD6C8C6BD124629098B11B9119A0F23114B36BB4F60B922F329C71FD3F997BB04B021216303AB590CB0818851B251A8A9D481FEB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...$ ....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y0/r/fxZXKbUQCIc.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.B..u./.....y.....e`9o...UYV....<G`.....~F ..7.C.E..A..Eo.....c.O.....A..Eo.....'..?....O.....D..x.,.....(.....(S.1...`.....|L`:.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,..... start_js.....`.....M`.....Qc..k.....EAoOu.....Qb.1tb...__d...Qdv..Q....BanzaiUtils....`.....M`.....Qd.N50....BanzaiConsts..QdB+.....CurrentUser...Qc"i,c....FBLogger..Qd..... ..WebSession...$Qg~d{X....performanceAbsoluteNow...(S.h.`.....<L`.....HRc .....O.....Qb.....h.....S.c.....I`....DaV.....4..a.....Qc...L....canSend.C..Q d~.....filterPost..C..Qe6.....resetPostStatus.C..Qdj].`....retryPost...C..QcJ?.j....wrapDataC.(S.....Pd.....i.canSend...a...;.....q..@.-....\P.a.....M...https://static.xx.fbcdn.n et/rsrc.php/v3/y0/r/fxZXKbUQCIc.js?_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\48cd11cd96c09582_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.548715162190085
Encrypted:	false
SSDEEP:	6:mqIEYj018lrA6/sUQ7aMXYaXhZkAz0RK6t:+w1tDGMaXhZ14
MD5:	D4A4E0601027132ED2B234959B635587
SHA1:	7FF42E661E1EE9F4E190FC04066157D3CE5356F2
SHA-256:	3CBD8D51D333471E4FB0974A2B3DA707B4457A585C4F5F84CB3962F5CD57C083
SHA-512:	774CB27D7B20DD5E60022491362E48AAB32CCE6378DA0D77F2E9C4C97A3E550829BA5DD102655A09F25B30CFFE61C205A8550DF4D43FEE6F6796B1E1AAB756A 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...s....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.Typeahead.3295cbd5.js .https://twitter.com/@...u./.....f.g.....J..Kvf..... =.c>.A..Eo.....r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4b1ad506779b8238_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.556905119253614
Encrypted:	false
SSDEEP:	6:mmzVYj018lrAMUKyRpMOqXV2rq/sqQtGHThprbK6t:XzN1thUKyW20oGHXrN
MD5:	09E6F7884850C8BE19609EF97B8CC43A
SHA1:	402C530C5B32CCBEE10836F79AF5554A569DF45E
SHA-256:	DD737C40606DC51D642494580C9627FAD16190DC6548F9E030A0756CB3AAE8B0
SHA-512:	29F55E4DB746B2C6D56A6908B77DF2FF4E1E08C772A28DA0B68A9D09AC775EDDE4436B14F06114F3A5A2FC2C1275E2F70BC08785406F8E6D6FCB2DFFE04E77(A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...^....._keyhttps://abs.twimg.com/responsive-web/client-web/sharedCore.59f27d25.js .https://twitter.com/....u./.....1J'm.N.fS.WZ.x..>.r.....D.KxL. A..Eo.....Q.s.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4b8986dd2cdf416a_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\4b8986dd2cdf416a_0	
Size (bytes):	9027
Entropy (8bit):	5.982947084137822
Encrypted:	false
SSDEEP:	192:d4qy/NIB8dcxZ014HFBDGA48qjM3d/HLHdnnmsVGsiEy4z:d44BTxZ44DDBqwBjOi
MD5:	55431A59699040590AE8EEB84500C145
SHA1:	B04DF97425FE85A7E2EC4405173494539164CA5F
SHA-256:	CE71E8BEC8E47C7934CA1297A87B191CEEECA6B244D71ED1087396008A1716DA
SHA-512:	8BA80AAE5B51D9CE22DC44118F4B6AA5CCBC6A3558BF0ACC2A8166D3267A9F3ABAF5DA30C4C862DC2594BDF3CD3F90C7CA248D4387A765FB9A4C6B2225CAF69
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....k.K...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ifOm4/yc/l/en_US/6-dc-4zUXUJ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....!...#8).F.>..SJ...m..sK&..#.&.A..Eo.....2,.M.....A..Eo.....'../....O....!..;.3.....(S.....`.....L`L.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc...+....Iynq2.....Qb.1tb...__d.. Qf..+.....CometMenuFocusGroup....`..... M`.....Qbj3.....fbt..0QjB.f.#...CometComponentWithKeyCommands.react...Qd...g....CometKeys.....Qe..0.....FocusGroup.react..QcB.....React.... Qf.Z.....focusScopeQueries....(S...`....4L`.....HRc .....O...Qb.....h.....S.c$.....I`....Da.....(S.....Iaj.....e.....@.....@.....M.....@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3ifOm4/yc/l/en_US/6-dc-4zUXUJ.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`....D`.....`H...&...&....&..A..D&.(S

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\509a23027ed240fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	293
Entropy (8bit):	5.653539608735358
Encrypted:	false
SSDEEP:	6:mSUIEYj018IrAMUJABIHy6JABIHLj/pMiGZCvSSt2IjK4JKK6t:g1thULDL2CvSs2P
MD5:	3ABF1A36164A86365A5E4E764674306E
SHA1:	73EB5A71CE61488570BDC15BF0712F335B112C3D
SHA-256:	F8FE381C19BB2C02FF60CB43B57E6C06483E58DA061EC0E8E4E206D0D1B3B36C
SHA-512:	AECFB38A8E727AB3C05CBAA73D730358674B958250CD6F8EDCBB23F72C18C4EF36135A134853BF9E6F0A48AE7516D1DE91538F46591C8866CC8FDEACAE2AD187
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.Z...._keyhttps://abs.twimg.com/responsive-web/client-web/shared~loaders.video.VideoPlayerDefaultUI~loaders.video.VideoPlayerEventsUI.92a51805.js.https://twitter.com/p.0.u./.....<.....s..5.....~.2.....]...C...A..Eo.....,A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\50ac3b97b0ab1700_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	26928
Entropy (8bit):	6.1379097209020275
Encrypted:	false
SSDEEP:	384:7zEoDyT/olgtMYoXMpxSiAgdww9MeD7MbUjV:7woDyTolgMhMpx9AgioMbwV
MD5:	BB64CF1DDC1B89A6C1304F430B743FB1
SHA1:	B29C50B2C204DB61127BCD48C715381619EEC9F3
SHA-256:	B5C966B2B0E0A7809DACB1F4A9402DCD813897736B906092CACECC99E1FE3401
SHA-512:	E0C30EF3C0BBAE135262FB1871F59D84A0C96C093E6DF151FE19946880853B7572D5080D2C4C7998B81F33F5AC6B243C1428385F20EE0C89020602836C335CE4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....-...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yv/r/UxUwcdLgDuO.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/j...u./.....a.....+....e..8.s7....5...A..Eo.....v.m.....A..Eo.....'.:y....O.....g.....(S.....``.....L`T.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.eb.....hvToX.....Qb.1tb...__d...Qe..dh....FacebookAppIDs...(S..,`.....L`.....a..... QfR..!....FACEBOOK_FOR_ANDROID..Xa.....h1B.$Qgf.....FACEBOOK_FOR_ANDROID2.....Xa...#.iTB.0Qj...$...FACEBOOK_FOR_EMERGING_MARKET_ANDROID..Xa.@.E.J.B..Qd.....TURDUCKEN.....Xa`f.3...B.$Qg.V7.....FACEBOOK_MEDIA_EFFECTS....Xa.c>..I.C..Qe.+=.....MOST_RECENT_FEED..XaP..zzN.C..Qe:.+(....SAVED_FOR_LATER...Xa.7l....C..Qd.....TRANSLATIONS..Xa.. .N!.A..Qe...t....MESSENGERDOTCOM...Xa8.a1..C. Qf..h.....MESSENGER_DESKTOP.....Xa.9$.26.B..QbZ.g5....WWW...Xa..W+..MB..Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5100160870c44dae_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	37259
Entropy (8bit):	5.983961562043036
Encrypted:	false
SSDEEP:	768:Qf/2ZowgJj53+Tlbhe0YEnPlwdjkwFSS+vIquQZd7OQJ:QfeAJ9Ot9YEJM+QqrF
MD5:	800769F224D567D37186E48204ECC1BB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5100160870c44dae_0	
SHA1:	11610C8EEB5318A614A2397D5C94EF46529AA3D4
SHA-256:	181C17E9DAE72C5D9C4D266877DE662B82F38062F6C34D0F490C73BF0E1DFF1F
SHA-512:	72EB258F5E4DDF9C31F71BE1FDBFC40161C384BFDCB41D69252BD9D881D3F34D7C273D68A9168E316A1A79A143FFDF29C42820257F66AEEDDC23C897E79329F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....j9...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i1MJ4/yu/l/en_US/hT0YD4TA64G.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/c...u./.....[s..~..w|.y....n.h&...[...A..Eo.....1.....A..Eo.....'.....O.....z.....(S.....`.....m.L`2.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.....AezDT.....Qb.1tb...__d.. QfFd.....VideoBroadcastStatus.(S.,.`.....L`.....d..a.....Qc.....PREVIEW....'..Qb.....LIVE..A(..Qd.p.....LIVE_STOPPED...(..Qd^/.q....VOD_READY.....(..Qd. .....SEAL_STARTED..A). Qf.....SCHEDULED_PREVIEW.....)..Qe..X.....SCHEDULED_LIVE....!*. Qff.....SCHEDULED_EXPIRED.....*. Qff@.$....SCHEDULED_CANCELED.....+..Qc..y.....PRE_LIVE...+..Qd...j....SEAL_FAILED....+..Qc^.....exports...K`....De....8.....}..)-.....(Rc.....I`....Da....^.....b.....S....@.-....dP.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\51133f147a31b8da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	35275
Entropy (8bit):	6.09545212218256
Encrypted:	false
SSDEEP:	768:HaHr9V1JdDobBWWN8g6Q1Lw55i5L5cnRompC3C4j7n:HaHrN76BWWN56KLq5i5L5cnymp5sn
MD5:	CAD0A81C053B96B589791359128ECC02
SHA1:	0527B0BC2B70C82648A4DFAACCD4E97DF34DD2F3
SHA-256:	96067DE1B464C121519CB5F66522AC4CB7426470B65460FCF40E981B468A276D
SHA-512:	3084D285A5ECEB68AA68B8123695DB9A6D26345F5DA5BDC69D9F83BD96E43108BAB159AFF6783A8427CD1614E91875CC30CC89A9549096469325F2FDF27548D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...?..k...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ix2y4/yS/l/en_US/yDDKGRLJnTr.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.c..u./.....?.....A...E..X.../^/..>."....@.E.D.v.A..Eo.....u.....A..Eo.....'..p....O.....s.....(S.i...`.....L`t.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.i.....va0+x.....Qb.1tb...__d..(Qh...]....PagesNuxFrameworkTypedLogger...`.....M`.....Qc^..[....Banzai... Qf..=.....GeneratedLoggerUtils.(S.D.`D.....L`.....0Rc.....O.`....I`....Da....b....(S.....Ia.....\..uO.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@...I.....@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3ix2y4/yS/l/en_US/yDDKGRLJnTr.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`,...D`.....-....`....&...&....&.....D&.(S....`.....LL`"....@Rc.....Qb.....h...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\516ba86b5dcc10c1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5288
Entropy (8bit):	5.670333786727399
Encrypted:	false
SSDEEP:	96:M9/sBGPJcH8nfhCHY2zGoXJv0zU3fmwvkcPB7Jq/9fwZd:MFsc2H8Zwdb9vjp8I
MD5:	ECE66E3404FC199BEA92296D35D87702
SHA1:	765934443AFAB90F73BF4D031D0A838DAC30BFE0
SHA-256:	F3C6E5E127C4B0D992A1CEC7462C10BFB03E4D5BFBE031A1209296CB1F16AB29
SHA-512:	4065F7715A63759A7810FE2A33C5110537789DA80658F8F1C17CDCFBA6FD8705332F6326EFD723BC811B429F9A79C02FB705E29BE797920DFAC530D8BB6966DA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yr/r/kRCeNK5DCxB.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....IJ....O....`.z.#l)B.V#.|..A..Eo.....N.....A..Eo.....'.....O.....&.h.....h.....(S.1...`.....|L`:.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.....RKHw3.....Qb.1tb...__d..(Qh..s?....CometRouterRenderTypeContext...`.....M`.....QcB.....React....(S.@.`<.....L`.....A...Qen!.....createContext.....Qc^.....exports...K`....Dj....8.....&.]...&.(...&.X...&.%.-.....(Rc.....I`....Da....|.....c.....@.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yr/r/kRCeNK5DCxB.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....`R...&...&....&.(S...`.....@L`.....PRc$.....O.....Qb.....h.....S...Qb:..4....j...d.....I`....Da(...N....(S.....Ia.....a..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\520c8eb9b503bbdd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	148120
Entropy (8bit):	5.4266597405590495
Encrypted:	false
SSDEEP:	3072:deiBWUMR3wUiQ2zdzzm4Wa4q5Ikwfw0w2wkwCx8XLsaCRsXHWRUmhNPaQ8TGsH4Z:dizUpO+dt2
MD5:	2FD25639B0832C9AD672EFF41F5C8A63
SHA1:	37F57292D4CE05D1120278ABE3F11522D354CB6B
SHA-256:	7D43508DE5546D24CA99D1082F1A88AB305628D0A095F656F1995214B9A59D53
SHA-512:	97A09B7982906AF53DC2B53C1D08F41C4902543481F59B1D65A13583E067605D017CCA9A77F66334F167C4AB72F2B13594394D078FACFF3C393984027D09505C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\520c8eb9b503bbdd_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....HN.....F74A9B42E45AC461D29955FC067252CAC00DF870BE7358EDE466A47D38F5FB4D.....'.....O)... A....f.....x...hQ.....D.....(S.....`.....L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc2.....0YQmw.....Qb.1tb...__d..,Qi._.. ...FanFundingStarsEventsTypedLogger...`.....M`.....Qc^..[....Banzai... Qf..=.....GeneratedLoggerUtils.(S.D.`D.....L`.....0Rc.....O.`....I`....Da$...v....(S.....Ia....p.....A.....@....I...".@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iFo84/yJ/l/en_US/dE34yGDewPm.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`\...D`.....`....&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\52ee3a69311f528b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	141272
Entropy (8bit):	5.908944149776895
Encrypted:	false
SSDEEP:	1536:bo19u4n+eHA6rn0HgDAIfEIZ5+M5+OygjhnpHUkDVvv2znUOFjS3LCiCZZ6J3du9:bGjpyu/f7Z7y+D5vo6G3fnDbd
MD5:	BD693A8626195835909314E6C20D3ECA
SHA1:	104D12D79FD3CA375A65B76832AF54B3F383227C
SHA-256:	EED35816A4E20674CE1AE9264E3543AA55F724531C949C87CC67B57013558E52
SHA-512:	94C84D8A832C667963BC7CB1CDF4F5EFDD323308D62624CB00D19E08625D0EF6EDA02E72ECE8498B9A0A9513FE57FCA98392D71C8A4C3450EA6824338B407A2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...8.(.....3CFC743D6A160D4DF987656B9DD63AD37F9EE324A456EA70DBC0399F47494A33.....'.I.....O/...H&.....%.....,..<.....(.....(S.....`.....L`<....(S.p.`.....L`.....0Rc.....Qb...\....t...`....I`....Da....j.....Q.@.....module....Q.@.....exports...QcRY42....document.(S.....5.a.....q....a.....a.....a.....a.....Pc.....exportsa..../...I..q..@.-....tP.....h...https://www.abmcovidvaccine.com/sites/default/files/js/js_ZcvXZXOCXR6YLZCenbBQSIZQup_B6yR9tcZCBJfY33s.jsa.....D`....D`....D`.....Y....`....&...&....&..a.&.(S....%..``K.....L`.....Rcd.....*.....Qb.~&.....C.....QbZ.....E.....Qb.S.....r.....Qbz.I<....s.....R.....S...Qb^U.....n.....Qb..1@....o.....Qb..u.....v.....M...Qb.>.{....l.....Qb~DI.....y.....QbN.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5496109d4f7b96d3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	32459
Entropy (8bit):	6.123702110989076
Encrypted:	false
SSDEEP:	768:53lB6F2XIWVDvGu+DcWqJyKN9dKPPrCKd3N:53yq6VCuA9qwKns7CKd3N
MD5:	806726B3725445506BE16412653BB099
SHA1:	B71E7010BBFD18FE9E3F1A0483C444E3F8B19FAA
SHA-256:	D57A9F8463C1921EF894C969650E165F4B97F1F8F2D3B89130487F4FCED590B2
SHA-512:	A2E18BCD1041832A72B306086AADA0F5F0C194D22C32386FDEBBD7ABCCB9CB935386D09E401FA2381032DACEC08846525B34A30C3E60FCE0A2F36A8B1ABD759
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....g....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ilNU4/y9/l/en_US/AgUTJo_P37N.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/:...u./.....%.....s.%Y.P!H\...0Z.g]..{.h1Bh.:M.A..Eo.....2z.....A..Eo.....'.....O....}....S.....(S.....`.....5.L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.....SqTtm.....Qb.1tb....__d..(Qh...I....ConnectionsPYMLTypedLogger.....`.....M`.....Qc^..[....Banzai... Qf..=.....GeneratedLoggerUtils..Qd.x.....nullthrows...(S.D.`D.....L`.....8Rc.....O.....a.....I`....Da2...0....(S.....Ia.....d..wV.....@.....@.....@.....@.....@.....@.....@....@.....@.....@.....@.....@....I.....@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3ilNU4/y9/l/en_US/AgUTJo_P37N.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`.....`@...&...&....&.....D&.(S.D..`@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5782a317c325dde6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3288
Entropy (8bit):	5.559903231402788
Encrypted:	false
SSDEEP:	48:Xu+ciLkQ2GKd4N2Gp/DcO0fTyI3lQY023ISJdIyzIYAReOJ5hwAREZTlOWCq2hxA:Xu62bKNPH0fGk3IShN6hwAq5lHCc
MD5:	3288EF9C8FC35F46D132BFB4CDCDABCD
SHA1:	4E185C99011D35C37E6694BAEDD1F00A89FCC6D4
SHA-256:	F925FCBDEC707010EC69578206B182E16291EAA20B1B6F95308869931E3338EC
SHA-512:	B7C5FE71D172C63913E8481201B2878D30E9474ADBF1C177CD21A1E56545EAB4E1EE69DD415024BF938CD8693606D8148391F653807DBFD8291EE703ACDD697
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5782a317c325dde6_0	
Preview:	0\r..m.....h...m....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yL/r/wfPkGs1U5g3.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/p...u./.....Z.....U.I|..W.K~.....e.. .....A..Eo.....M..<.....A..Eo.....p...u./.....'.....O....h....).....p.....(S....`.....`L`,.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.. ....M`.....QcV..>....341IW.....Qb.1tb...__d...Qc&.....lastx.....`.....M`.....Qd^.f....invariant....(S.<.`.....L`.....0Rc.....`$...I`....Da.....(S.....Ia.....M.....@.-....\P.a. ....M...https://static.xx.fbcdn.net/rsrc.php/v3/yL/r/wfPkGs1U5g3.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....t...`6...&...&....&....&.(S.P..`Z.....L`.....HRc .....O. ..Qb.....h.....S.c$.....I`....Da.....(S.....Ia.....q.d.....@.....(S.....IaW.....H..p:.....@.....@.....@.....@.....@.....@.....@..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5802bbea60850d80_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	5.479739252624962
Encrypted:	false
SSDEEP:	6:mkPYGLDlynflG9LY7Ww6wlyD0cd7Pe5nJMtbK6t:1UflGpYSHwgfd72EN
MD5:	4767E400624292A130E818E73AE3F820
SHA1:	41A51C903BCC25704772E581A41DCC16590E2BE7
SHA-256:	0B898428F3EE70BF2B8B5BA814F886D2A21BB62FBCC3FEB88C093CCA4EFCF163
SHA-512:	C6E4F9C180F19E2528F1410E910A3F37BFDF6BC32A2D379F9DF06783B369090271B7D911AD95B4D546F4CAA786D9211BF1F80E6FDD6DBBBFE3CD383B0F7390E C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n.....v....._keyhttps://www.instagram.com/static/bundles/es6/ConsumerLibCommons.js/0a0e207e5968.js .https://instagram.com/....u./.....R.....g.....|ed.. .g.Vh.Z../..A..Eo.....;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5854018eddf7ea85_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13624
Entropy (8bit):	5.2892809155952385
Encrypted:	false
SSDEEP:	192:dz7Go3YnSLHn50W11FL6Rve/rkPUVFjvy3b1QPTVingz4K+Vlv3SNbn:dz7Goog68DG1QPTVK7VPi5
MD5:	9B8FE6C00066FE8B155894EF99AA9133
SHA1:	0A1C9C4FBF57E1A913FDB14C8208543B04DA0486
SHA-256:	024B549E93B1F05DCA375FAE6D7B45C5AC8E740D675359B279A22A1D62BBCE9E
SHA-512:	EFC72E936A81B8DEB95AD2158A81993BB8A1AE400EB18030C28AB04B345DC822E39A8F4327B52DF818E806DBF3E89A68F5D8ADA91B6106992C419670AE87CF3 F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....P.P...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yC/r/BwjU4B_qfpp.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/#...u./.....%%.k.....68q..v+..U^`..A.. <..4m..A..Eo.....2ph.....A..Eo.....'..)....O.....3.....(S.d..`~....$L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js .....`.....M`.....Qc..O.....KQ+lo.....Qb.1tb...__d...Qd&..g....flatbuffers..(S.!..`.....L`V....0Rc.....`....I`....DaL....S....Qc.....Offset....Qc6.....Table.....Qd..6.....SIZE OF_SHORT..Qd.w.[....SIZEOF_INT...$Qg.5i1....FILE_IDENTIFIER_LENGTH.....a.....Qd.|;.....UTF8_BYTES..`.....Qd.[.....UTF16_STRING`.....Qc.....Encoding.1 ...Qc.DL}....int32.....Qc..X.....float32.....Qc... ....float64.....`.....Mb.....Qe2.W~....isLittleEndian...(S.....Pc.....g.Long..a.....I...5.@.-....\P.a.....M...https:/ /static.xx.fbcdn.net/rsrc.php/v3/yC/r

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\58c0c6580a3826ef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.6330369132624245
Encrypted:	false
SSDEEP:	6:mp/PYj018IrAAABXs55FnM0nn1VJX41rgDK6t:wn1tRrx1VJX4K
MD5:	D81681A025E34E45D9E7CD602CD945E9
SHA1:	B4731E18D0C602E13319D14E981215B951E16868
SHA-256:	7F6687C79198465C49A10FC4CCEB7D84EE88F05419653F257C3CAFF5E7261B33
SHA-512:	5F8F017AE0F54B4D3AA943E45C159CED0087B10D0D0E3F14B454FDDB85B1E625AA8C80794B6FBE6071CBD8764EEC846BAFC9F0D084DEB43AB4FA0767E4C63I 3C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://abs.twimg.com/responsive-web/client-web/loaders.video.PlayerHls13.af3257a5.js .https://twitter.com/u.0.u./.....$...k..a{... ..YV...._..r.A..Eo.....K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5b9fc540bdfdf435_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5b9fc540bdfdf435_0	
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.576428071492774
Encrypted:	false
SSDEEP:	6:mXYj018IrAukGg8MusAZ+2599uDgZp5RK6t:C1tRng/8+2ZMgbp
MD5:	F6163719C3FEEE990000E031D993687B
SHA1:	6CB4F21E8A3C7CA1FD9F121202D24500B34134AF
SHA-256:	5F8AE76285CF86EA98367851EA8EE7746D5B7D88044DB545FCEA7570883CDF9F
SHA-512:	DCE7E869FEAC470FC994287698DEA38E33ACFF286F98F0670CCC990C55381DC36F2012EC9CF0EF5075DB885D544A80A06D3BBCCEBFA4E20F1689079F76E57D7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....:D...._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.BranchSdk.24398485.js .https://twitter.com/."..u./.....7PI..G;.`...t...X.Gw.O.uf]HN.?8.A..Eo.....cjn.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5cd27619c8451633_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213920
Entropy (8bit):	6.217253263790104
Encrypted:	false
SSDEEP:	3072:ztky3hmxkn+yF09IKy7+613MKOFpfISb09t+Z/l6p:Jky3hmkc613rOZJt1p
MD5:	E609F665F6DA822EB70AD0A634BAA916
SHA1:	6797C8890BAA63A1144E6EABD944D8A32504397C
SHA-256:	9469350DA40182B9A1B19D8016CFBFCD06BC11DC15FCB23C8C8480D1C1CBFCFD
SHA-512:	B8AF6CE232BA7D159355C39E179DED22A78B198ABBA6D161E19C6077D52E134357345E1FA634ED5E8FAA0FEE30A9354828367CF52DB296ABE92144D2B0E49961
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...L.0.....716B5CD918F3DF6FCA260ECA68366D709BC4C79497463BF7E36C39A1903D7383.....'..Y....OA....A...#%.....(....!.....L*.....0.....|.....(S....!..`.A.....!.L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc..d.....LskDM.....Qb.1tb...__d..$Qg2.T.....AvailableListConstants...(S.D.`@.....L`.....Qc..7....freeze.....a>.....$Qg.n.....ON_AVAILABILITY_CHANGED..,Qi."......buddylist/availability-changed....Qez.AD....ON_UPDATE_ERROR..$QgB.....buddylist/update-error....Qd.....ON_UPDATED... Qfr.....buddylist/updated....(Qhb.A.....ON_CHAT_NOTIFICATION_CHANGED.(Qh.Z.....chat-notification-changed.....Qc...n....OFFLINE.`.....Qb...K....IDLE`.....Qcbq.....ACTIVE..`.....Qc.t.....MOBILE..`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5ce7850566914a05_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10187
Entropy (8bit):	5.746247759433992
Encrypted:	false
SSDEEP:	192:k1oKlj8FTZugCbzB4Wz6/PHXLmxj9mnTzZxZcn2JyyYoe:kvp8FTXMo/PHyxIzZ7JOX
MD5:	6974E85746837482DC5E84DFADAE4903
SHA1:	44FA68040704366A8754E650DF51B9A2868CEFBC
SHA-256:	5F580A9D1F1C6A2C85146BB621FC02A4555620DAB9CB0424C25CF19C6565D4CA
SHA-512:	56BAC0D9971A4B6D5FA74BC2AD97DB4101EACB188388C458340878A7A4130E77CD1871947CC4E38E5BDA0FE4E0612CFCBEA2743C7F5FE3F62A03BF64FABE820C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...$.w....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iLI54/y0/l/en_US/0fkDDfbX-A8.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...u./.....x.....%ps...R_.....F7.Y.ta=.$}}so.A..Eo.....4-.....A..Eo.....'..-....O....0&..c..A.....,.....(S.....`.....hL`0.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc..._....uKet/.....Qb.1tb...__d...Qe.e.U....ariaGlimmerProps...`.....M`.....Qbj3.....fbt...QcB.....React....(S.P.`X.... L`.....<..a.....Qd..HT....aria-busy...G..QeJU.....aria-valuemax...`.....Qe.O#....aria-valuemin...`.....Qe.....aria-valuetext..C..Qb.N.F....role..Qd...S....progressbar...Qc.x.8....tabIndex`.....Qb.'@...._.....Qd.-./....Loading.....q...Qc^.....exports...K`....Dn ...@.....&.]...}..)&.(...&...&.Y..../...'..%.-.....(Rc.....I`....Da...>.....c.....@.-....dP.....X...https://static.xx.fbcdn.net/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5cfd57ec8c48c5f3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.576561427920644

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5cfd57ec8c48c5f3_0	
Encrypted:	false
SSDEEP:	3:m+lYW/C8RzYj0KKKXlMMIrATT7mcolMRtJcQ8elHCx/Lu40vE9/Op4mOg5X/pK5M:mYPYj018IrAniNM/SQ81Z86OhbXhK6t
MD5:	C8E1EA1F19A21D4B26147B5AC552604C
SHA1:	61D07C588193BBAA27F6CA98F7E327F2E41103D5
SHA-256:	8AD2053DA8F2754A82F6F37CC5B851EEF241A77EF2E832B3E60D6A52F35E4CA9
SHA-512:	D8B089B03F05C2881D78EE749486F754C143593F9A99C05353E423FD8DBB7D6E2BE9FB5A04655C1026644B2F867C9CB8B68EB2FCB1557B3CB4E20945CB34BF5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....;...._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.LottieWeb.f4c2aa65.js .https://twitter.com/-v,.u./.....$...Qd.?7|../6K...?G.." ...B.l9.A..Eo.....!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\63520e3b367ec63f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5984
Entropy (8bit):	5.9708596951693504
Encrypted:	false
SSDEEP:	96:7/QfY4UTyR17G0npAbsXoSbgl2J0yP0SLr+TIBlJwaFu/F/0M:7/QOWhLpAIYegRys5I1eNj
MD5:	D251BA9317F68300369D34567FF5AF92
SHA1:	6E596EDD8AC5CDC3031E54E995F4CA2B17D94A1D
SHA-256:	DB68F3440AAD9C0BE70079D1159238A64846289451F0D72ACA8398EC12D234DB
SHA-512:	46D1D7B00801E613D9BF2968D73A298CD0CFD26B8ABA940C81BBFC24660306B32FE8B988A1F3A608A483803DFB18CAAC2FE6C831C9CA1DDBD884281AF5F4E8 D4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...*AN....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y2/r/6WwHHsCOxdd.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./...../.<b...QS.*t..;6W{.....R **!)$.A..Eo.....&%.....A..Eo.....'.. ....O.....`.....(S....`0....LL`".....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`..... .M`.....Qc:2.....3zFt6.....Qb.1tb...__d..(Qh&..B....ReactCSSTransitionGroupChild...`..... M`.....QcB.....React.....Qc".$`....ReactDOM.$Qg.....ReactTransitionEvents.... (Qh.+.N....createReactClass_DEPRECATED...Qe...4....fbjs/lib/CSSCore..Qd.....prop-types...(S....`.....L`\....@Rc.....O.....Qb.....h...b.....I`....Da.....1..d. .a.....q.....Qd.i.....propTypes...C..QdV.<.....transition..C. Qf>..g....queueClassAndNode...C.(Qh.x.....flushClassNameAndNodeQueue..C.(Qh.f.V....UNSAFE_ componentWillMount...C. Qf.J.?....componentWillUnmountC. Qf.}.N

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6386862eb4b2bb21_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5272
Entropy (8bit):	5.5581932662863105
Encrypted:	false
SSDEEP:	96:7mG0dFyOvFtuRE2Xc6m0EweLCha2Lu7Yic+B4DGICbJuJvJ:7gORbM6eweOs2LYDp4DGC
MD5:	7D384ABEE0CC85B43B17E375BF7F311C
SHA1:	1A9E40B4EF510AAD60EA27AA02A612AF684B0389
SHA-256:	510E1558BEDFC9013F65A97F9D7068A21D7EB4E88B5E4A3E9BDD8E14CB32CF60
SHA-512:	6015213FBBCA522D94A7FDD423CE63017253411BCCE73DE972614AC44C1FB70158AAF3265DCA0FC395CF290DDEE58CD74392969C9727240DDBC4971C37BECA 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y_/r/JopZtdti8dq.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....;...L.tUq9..,F....x..H.....).A.. Eo.....-../.....A..Eo.....'.f.....O.....R..P.....(.....(S.d..`.....(L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`..... QcrF.....FEt5G.....Qb.1tb...__d.. Qfz.....CavalryLoggerImpl.....`.....@M`.....Q.@..$.....Arbiter...Q.Pn.v:....Bootloader....Qb..?.....ISB.. QfBj.D....ImageTimingHelper....$Qg b.~4....KillabyteProfilerConfig..$Qg.M|l....NavigationTimingHelper....Q.P...L....PageEvents... Qf.OC.....PageletEventConstsJS. Qf../3....PageletEventsHelper...Qd..\.....P erfXLogger..,Qir.O....ResourceTimingBootloaderHelper....Qdj.5....ScriptPath....Qd.....performance..$Qg~d{X....performanceAbsoluteNow...(S.l..`L.....L`j....`Rc,..... O.....Qb.....h.....S...Qb:..4....j.....Qb.p.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\64bcef824806d19f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.638097713881889
Encrypted:	false
SSDEEP:	6:mh8HXYj018IrAiXFGvQmM4GRah6Y5/bK6t:W01t1XFGQF0z
MD5:	D5740C352A0743C6CEB058A7F13938CF
SHA1:	453AC39396F46F77D2E4B1B3643B885E8ADED40E
SHA-256:	6FBA6C66DA2C3313A9A8202783C706DC94D4F994883CACA0091ACD32C22D194D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\64bcef824806d19f_0	
SHA-512:	0134E516DEF4DD7527BB2820BA521524AC2BAFF4AC3334ACA73A9456CB390B07323F0D1F027F012549932238416A2B60EC1E52241AAC1A24C649FE6A5F8A038A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m.....1+...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.graphQLDarkReads.78553645.js .https://twitter.com/..*.u./.....A.I.IU.O.....}w>. .O...k.Q.7.}.A..Eo.....g.[.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6544bf18487749db_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	85856
Entropy (8bit):	6.030492677067693
Encrypted:	false
SSDEEP:	1536:HZXNvzP0nTuZHbOg92UM90qVgiJ+j9S0/VZZgyKgqAy51Wn:Hz+KVbNqVgJ1VYAn
MD5:	D1141B18549D8BD510023523DB88F8E8
SHA1:	121AD1E00DDFFE32D0986B081C94127DD7A2F388
SHA-256:	1E1CADD9586EB0829754F656FA63E862D48715C50C1272497B1437BA053BE20E
SHA-512:	32F84418FE9C1F795364F18281CE33EBBA67A35BFBF38A776D2FE5099F962755C7C06876E12FB5DAB671DEDDCDA2B6FFA25E56D8A03EA3163790E8870E8B55E5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...n.O.....0D1A6EEFAA88649533A3F82AE5BD3CC647889A4571D3B0BD9B86F0F525BF4A25.....'.....O.....N.....{..... .....|...x.....(S.y...`.....L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....QcV&8.....UVJyi.....Qb.1tb...__d..( Qh.+.....CometScrollableArea.react.....`.....M`.....$Qg"2y.....BaseScrollableArea.react..QcB.....React....(S.X.`l.....L`.....8Rc.....O.....a.....l`....Da.....(S.....Ia..... .....M.....@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iMiq4/yP/l/en_US/XcnrNbuCsN1.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`z...D`.....`....&...&..!.&..q.&.(S.< ..`2.....L`.....0Rc.....`....I`....Dal.....(S.....Ia?.....M...q)..Q.d.....@.....Qc^.....exports..M...a.....Qb.~x....AMA....0..Qef.7v....ANIMATED_IMAGE....Qb&b ;.....GIF..$Qg...w

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6667df0f87d0f543_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	44195
Entropy (8bit):	5.912541154275085
Encrypted:	false
SSDEEP:	384:DRAT8HianFzGbphVa2L75vkk0P5udRGzX2b2LbO/0ZVegMb0PCMB4VQMOIxgQlLJ:DRNHTFzu39758eWd+02MMtxYf6q
MD5:	CA7464536784857F77572F95E9FF1111
SHA1:	5BE5DDBB7C31D5A13F705CCE2A92D97C367D6CD8
SHA-256:	E0FBCBBBABDF4D3AC0FE352465BF84372B078495DD56442B9DEA68404830E209
SHA-512:	E58D32FEE8A123B49BAE912DDA293EA2B24F47763F6FDCDAD548F0C27AD930B9EF05948B2A427FE3A679C2FA9D65C84FDD700A7C4B3406D9624938F1A4C5B8F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...E.h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iYXl4/y2/l/en_US/syDBqhuYqtT.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.A..u./.....@.....`-.F...C(-. ..q...Ew?.....N.A..Eo.....ox.....A..Eo.....'.c.....O.....v.....P.....<.....<.....(S.....`F.....L`.....Qbj$.....self..Q.`>n.. ....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.0?.....YB9E3.....Qb.1tb...__d.. Qf.....ResetScrollOnUnload....`.....M`.....Qb>.....Run..(S.H.`F.....L`.....0Rc..... .....O.`....I`....Da.....(S.....Ia.....d.....M.... .@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iYXl4/y2/l/en_US/syDBqhuYqtT.js?_nc_x=Ij3Wp8l g5Kza.....D`....D`d...D`.....`....&...&..q.&..a!D&.(S.P..`X.....L`.....4Rc.....`$.....Qb...C....c...`....Da.....1...QcZ.I.....onUnload.(S.....Ia....s...I...!..."d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\669d5033304a9f70_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6376
Entropy (8bit):	6.1730535950963095
Encrypted:	false
SSDEEP:	96:SjwOC7g9/0YcZVLxawy8O1OHSQmiSAiJrDJ8dTRnrSQEcIAPZ:SjwOC7a/0YcrIwy8O1R5DJaVrSQEzy
MD5:	70FD477375C3D110C01C04E442E9E892
SHA1:	978F9AEB624935696DC792EF935C9CA679C39AA1
SHA-256:	840C704B79DAEF5675071C52B919332D8D30A9A3477AC5DB691B8EC8C01E1F99
SHA-512:	9112783761EF7E1FAAB4005316918E47931B0B5B63616BA8C5EC43271E2D6DFA9AA89A41DA2ECDDAD04C8D1946ECA534A0C228552593A862BD624D72A6CA132
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\669d5033304a9f70_0	
Preview:	0\r..m.....h.....I...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yg/r/V8C3I2Budu6.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/C...u./.....Z.....7.%....Y...1$..... _n..].A..Eo.....?1.....A..Eo.....'.'....O....X.....`.....(S....`0....LL`"....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M `.....Qc.....y0Wlx.....Qb.1tb...__d..(Qh...I....SUIInternalMouseUpListener.....`.....M`.....Qe..RJ....DOMEventListener.(S.T.`^.... L`.....HRc .....O.....Qb.....h... ...S.c.....I`....Da.....(S.....Ia.....M.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yg/r/V8C3I2Budu6.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`. .....`N...&...&..!.&....&.(S...Ia....#.....Qb...C....c.....d.....@.....&.(S.....Ia-...B.....S.....d.....@.....&.(S....`.....@L`.....Rc<.....Qb:..4....j.....Qb.p.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68ac1a271be10ee2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8784
Entropy (8bit):	6.0809968836925625
Encrypted:	false
SSDEEP:	192:drAxOkCyarPMpLnABRdG2J15Am38F4ciM8Lob7E+IbgF+axDvK3t:drsOJTrPYk3zJ1aiM4ciM8L8cbgYOS3t
MD5:	AC50921157D1C5862CA502DC1392AFB3
SHA1:	7D7B34C6A1837BC000293877D7682ECD49505597
SHA-256:	E7118325D9CD3FD3B2BA72A03052F99A9D662406460F4261C5157D55D21AA08A
SHA-512:	2E0E74DF6550C273F6E39DA87FD1A042CD046F77B4F50BCEBAB4FE0A7D6EA67175B736991959F1A8BB64AB33BD914A88AD1B349CA83F4A49E260DE00C30D42D3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...HW....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yi/r/VCutbL3vpAh.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/;...u./.....u.....%.%.$N...A.....#1 x...!.A..Eo.....}w.....A..Eo.....'.....O..... .....(S....`^....LL`"....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`..... M`.....Qc...S....Mmiev.....Qb.1tb...__d..,Qi.K".....MediaUploadCommonWwwFalcoEvent.....`.....M`..... Qf..z.....FalcoLoggerInternal..(Qhf.."....getFalcoLogPolicy_DO_NOT _USE.(S.\.`p.... L`.....Qc$Cp.....1839305...1...QcZ|bF....create...$Qg.tx.....media_upload_common_www...Qc^.....exports...K`....Dq....8.....&.]...&...&.]...&...&.]...&. (...&...&.Z.....&.%.-.....(Rc.....I`....DaJ...t.....c.....@.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yi/r/VCutbL3vpAh.js?_nc_x=Ij3Wp8lg5Kz...a.. .....D`....D`....D`.....D...`....&...&..Q.&.(S.D..`@..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6977ef021f3070fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	15099
Entropy (8bit):	6.08263309356728
Encrypted:	false
SSDEEP:	192:9wq3DKgP5TLampMdzsaRs6u25WMbN/VQxvD+BMmS7M5IrPnBta3aIYUx1A+BNU7Z:9ZDK2l+1u2v567qKIYUxjSgI1xyZxWv
MD5:	FC85529BB19D26614EA1AB7F26330878
SHA1:	CA28C3C7D2B65350197F713AB54BD26EFF847D10
SHA-256:	6B1EFA071D53D9B43045A77B1244046A1BFFFAC413041DE6E33595C5B69BA24F
SHA-512:	D7C8350689CF064612DFAAA64CEBB35D136A4C62686569EFE8C38ACAE01AC7D7D30447369EAF3DF07BFA56FF140809FAD8A12DD35E1F246EF5F47BF94342306F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....z]&...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iOA34/yb/l/en_US/Iv2CqzJ2cVt.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/M...u./.....3...Z.....s .p.r..D2.6....]y...A..Eo.....I.....A..Eo.....'.Bl....O....X9..D|4l.....4.....(S.e..`~.....L`p.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.. ...start_js.....`.....M`.....Qc.Al.....1l9sO.....Qb.1tb...__d..4Qk.E..&...MessengerSMBExperimentDebugTypedLogger.....`.....M`.....Qc^..[....Banzai... Qf..=.....Gener atedLoggerUtils.(S.D.`D.....L`.....0Rc.....O.`....I`....Da0...N....(S.....Ia.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@... ...@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@.....@....I.....@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iOA34/yb/l/en_US/Iv2CqzJ2cVt.js? _nc_x=Ij3Wp8lg5Kza.....D`....D`....D`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6a531f9f514baaeb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	255
Entropy (8bit):	5.5664980681468395
Encrypted:	false
SSDEEP:	6:mqiEYGLDlynflGCwiQn7llyp4CeZjEjJ4JPnK6t:AZflGCl27lgpeuwPp
MD5:	B44635D86BC716E8443E4DDB5857B3AA
SHA1:	3351EC73F78F1B740072E2A2A1735DC52A9FA85F
SHA-256:	70CD7183FE3AAFE3E514159330D6A37AC860253097A95ADACAB238A7AB0969E9
SHA-512:	BDE43524207C272DDC747CFAEA29E344E2EF8CC4E4FB09D597EDCCAA63A4C048134790CB1A94AFB6B180D6920EC1C2B404B4810D8C76625273A42D06CE7603B3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{....h....._keyhttps://www.instagram.com/static/bundles/es6/BDClientSignalCollectionTrigger.js/3bd89de73369.js .https://instagram.com/.-..u./.....=._. .cpu.mw..C....(m..a..c.w.A..Eo.....1[.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6afd19f7c12548d8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	17000
Entropy (8bit):	5.735117012495219
Encrypted:	false
SSDEEP:	384:e5FNogRqt/9HdAp3HFw892f012C0E8tJniv:e5FNbRqt/9923vsfVC0E4xiv
MD5:	E1F155D5B34DF5FC2EF78BD28FE7FE90
SHA1:	32F20794929F380E8ADE9A59D92B6302AB6BBCB3
SHA-256:	E3B9FE15E2B19EB38D6FF8118A4C2D51E596F4C51D4EBF38E5F310AB10DC2EBA
SHA-512:	CFF382FB67D2FB3853CCB29DAE089C6D8843C5FC8FE4AB49E8F99708B71E01A21F5EE60DCA519A0FD888474724650BB8BD70E18371880DBB3C054EB466D5BF F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...e.dn...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y3/r/U-5-lZH8FkF.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...u./.....~.....N_b..M.tB.Q.H_....x...ky. /.T.E..A..Eo.....A..Eo.....'..m....O.....@..F.....X.....(S.....`.....L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js .....`.....M`.....Qc.....iZXrL.....Qb.1tb...__d...QdZ.w....IconSource...(S.0.`.....L`.....(S.....M.a.....E.@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/y3/r/U-5- lZH8FkF.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....`x...&...&....&..q.&.(S.@..`<.....L`.....(S.....Ia....l.....d.....@. ...IE..Q.d.....@.....q...Qc^.....exports... K`....Dj....8.....&...&.]...&.]...&.%.-.....(Rc.....I`....Da.....b.....d.....@..@.....&...+D&.(S.H.`L.....L`.....8Rc.....Qb.....h...a$.....I`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6f005559e0633626_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	76024
Entropy (8bit):	6.193094876126621
Encrypted:	false
SSDEEP:	1536:dkwfxCh52YJ6ZPfS95/i0hsmdQqtvqc7g2Gl2mSHs6wWuc:QME6Zs/c0vq92Gl27szc
MD5:	6B4EECA4195538B16AF597DEB66916DA
SHA1:	943173F8E97158F282DE876638DD6366EC8BD487
SHA-256:	5A022F4A0AC2807EFD748F73A5DD822F2EF9E941B9E0D1A2F8637E44EFE17A49
SHA-512:	E742D9EF423DD9B42ADCB6A9F36DCC7456B58D20FAE6596705C2CD1646AC413F01A1B6FEE324BE740B5549852F4B38D7C98A5B5FE7948F10701D757991C17D4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...<UZ.....142EE93DE1B4EE4357A964821CAEB14B6BD099B9C9D27380269A1AC4DD7AB4FB.....'..x....O....'...U.....t.....8.....d..... .....H.....<.....(S.}...`.....L`.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc...K....EHOHQ.....Qb.1tb...__d..$Qg.6.T.. ..VideoPlayerFormatsMap....(S.,.`.....L`.....M...a"..... Qf.(k.....biz_stories_composer..Qc".....inline....Qd...n....topic_live.....!..Qc:).....live_map...Qe.....live_map_sidebar. . Qf>.....live_map_listview.....Qe...#....live_map_tooltip..,Qir.Va....live_map_tooltip_from_listview....(QhN..S....live_map_tooltip_from_map..... Qf.C.0....video_home_ inline.....Qc2..)....chained...$QgV.....page_live_video_module.... Qf..:s....chained_suggestion.....QeB.....embedded_video....$Qg..@<....embedded_video_preview....$ Qg.L.$....embedded_video_from_ufi...$Qg:Bu.....ufi_comment_attachment.....Qe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6f86a0170f447fa9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	145536
Entropy (8bit):	6.081116191510408
Encrypted:	false
SSDEEP:	3072:6eqPz7kWFpxfnq7LNAwo6++Mb/aBTTOVEUs2dSXdjNow+DqBDSf2NYo49wsrTrYA:6FPzy7L5IsObZ
MD5:	7100417C8D4BE1866B10B688E9430F90
SHA1:	048424245E8BBD5245F73402B167FCACFD997BAE
SHA-256:	00EA54D33C78CBAD526891E727FDC3D1B6A96AF924737302C76528C6463BE457
SHA-512:	16134ABD2C80947B410A459BCBDDAD8639D83FFEDA53A1184B52B1BCF126A495A760E7242329905D9FEC3A263CB264BE27AF7411BAEFAA25467396017958419
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...Z..t....90C4CC710E85B38B272A3434BA3FFFAEFAF272FEBA2D3966972386571FEE8EFA.....'.....O/....6.....L..... .....,...D.....x.....,.....(S.a...`z.....L`n.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js..... `.....M`.....Qc.^.....kbQ/j.....Qb.1tb...__d..(Qh...a....PhotoZoomCropImageConstants..(S.0.`.....L`.....a.....QbV.....TOP...Qb..f.....top...Qc.8.....MIDDLE....Qc.b.. ....middle...(Qh*..|....DRAG_INSTRUCTION_POSITION.....K`....Df....8.....}..)&.%.-.....(Rc.....I`....Da.....b.....s....@.-....dP.....X...https://static.xx.fbcdn.ne t/rsrc.php/v3itji4/yN/l/en_US/POy4OSHUNA_.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`X...D`.....`....&...&..A.&.(S.P.`Z....$L`.....HRc .....Qb.....h.....S...Qb:..4....j.. .c.....I`....Da..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6fd9163c22acd2b8_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\6fd9163c22acd2b8_0	
Size (bytes):	10408
Entropy (8bit):	6.006526262010284
Encrypted:	false
SSDEEP:	192:rIN5OnFP20fysfxxzSZmMlUQ25VjybFrAs+5jUlTBaypz9rte3NdBQ:r6MR20q83zkP2r+tX62TBaypPeddG
MD5:	6344EE1E565594A4945F39E93DD87F6D
SHA1:	CA581EC599837FDEE62CC2C5A28800B2288094DF
SHA-256:	4E8653DB2ADB36D297B453CA156BE39DCCCAC14B80C007F87817168B940CC408
SHA-512:	FCB9CA36806A032B14886BF6AA45BFCDE8DC98A5A9DDF5735668869A623D0B8F8B93548873E053135B469311764E3D33FF84BB9BB6186302B075193C4E456D4F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....0/....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yE/r/lS8zae5G9_Y.js?_nc_x=lj3Wp8lg5Kz .https://facebook.com/...u./.....w...h....pc.Yc..x@/.m(!=..JJ...A..Eo.....A..Eo.....'..5....O.....'...pX.....(S.-...`.....xL`8.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.k2.....TXV17.....Qb.1tb...__d...Qe..vf....BaseInput.react...`.....M`.....QcB.....React.....QcN.....stylex....Qc.]D.....testID...(S.p.`.....$L`.....HRc .....O.....Qb.....h.....S.c.....I`....Da.....(S.....Ia-.....(..h.....@.....@.....@.....M.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yE/r/lS8zae5G9_Y.js?_nc_x=lj3Wp8lg5Kz...a.....D`....D`....D`.....`n...&...&....&..Q..D&.(S.p.`.....$L`.....@Rc.....O.....b.....I`....Da....F....(S.....Ia.....d.....@.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\74921b3da4070251_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	379
Entropy (8bit):	6.013930181582315
Encrypted:	false
SSDEEP:	6:mRyEYk+f2pomWjV6xm/GhmJ2MMM/AGJD3n+K6tWR8rFWXHHTujBhwGcx0JD3ns5:vU++amLkJAXrFWXHz4Xwj
MD5:	7C980B65E45437582E4B65A1429BE318
SHA1:	912150F4B1BA1E27D06F6F9EC7BA3668032715CE
SHA-256:	BDAB35B137159C4AC88B80F59D030A0511C9ACFB200FE0BA4171C35DB2B1B79D
SHA-512:	3DC99EBF8EA3D461418642CFED2F31A2DB339A87711EC0C7F95E3CE6D9B419582BB3F32A27782F0E4C7E0DB7BB4005BB3F44B0408AB8FB0C940BF66F259A135C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...5Bh8...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iFJA4/y_/l/en_US/aOGyzlMDcOb.js?_nc_x=lj3Wp8lg5Kz .https://facebook.com/1...u./.....x9f.....W_.....=.f.A..O..u...A..Eo.....Q.....A..Eo.....1...u./.....9C0CBF3EBE3B91F54C09E8A47C22018992FDEAD4630BA37D77C7CCDC51D35E8A.x9f.....W_.....=.f.A..O..u...A..Eo.....:...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7506bc5effcaeb50_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	64083
Entropy (8bit):	6.020758577830787
Encrypted:	false
SSDEEP:	768:3fff1T+el676ueOjd5QHwfuGkkZJJr6BIvZNtQgMsLL7WSvrDMbwtVGthloKlgxf:3nd46ueNClJ6UTtQg5L/rjVGl5l0f
MD5:	8A75079DC9ACDAED904920C2F28A2D0D
SHA1:	8F7E14FEF2C845ABA8877C037EF667AFB095AD4C
SHA-256:	BEF08A43E8CEA199751E4509F3C498DA87CD9B7A44850AA02E06E15A82D36BC3
SHA-512:	8A09ED86CBE61635F53A6534348AF2674F632D1A7A56FF28D7F7EBD87614FEA91D1378960F1F539AF8A96F8D0ED0BC6CF048043190D6EB55627E6912D3EE822E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....Y\....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iSUg4/yW/l/en_US/QUdFdbF8LuY.js?_nc_x=lj3Wp8lg5Kz .https://facebook.com/....u./.....+..X.g.8.q\w....u..:..(..".u...A..Eo.....d.....A..Eo.....'.k%....O....x....!'.....H.....(S....`:.....L`~.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js.....`.....M`.....Qc.....mBWbo.....Qb.1tb...__d..@Qn...Z2...FleetBeaconSubscriptionNetwork_LogMutation.graphql...(S.8.`&.....L`.....(S.....Ia.....IE.@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iSUg4/yW/l/en_US/QUdFdbF8LuY.js?_nc_x=lj3Wp8lg5Kza.....D`....D`....D`.....`....&...&....&..a0&.(S...8.`&.....L`.....(S...Ia,...<...IE..A1d.....@.....Qc^.....exports...K`....Dh....8.....&.\..&.%.-.....(Rc.....I`....Da.....b.....,...d.....@..@.....&..!

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7511033aad8ca3b4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6267
Entropy (8bit):	5.6717201764064695
Encrypted:	false
SSDEEP:	96:4kz1riCK0Y3TccI83fkTDdmDvbOBVbO86081RX8xFlRtOI0VfbfKYoQy0y:4kz1rW/IgjOHphCMxhV0JfKYoSy
MD5:	2E587612C0A0D52179826E6284742D70
SHA1:	CAEE6F207C9559333A4486DBE6E9603785886083

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7511033aad8ca3b4_0	
SHA-256:	04FCB5646123A5D4111AEE45817BE584CA3D9D23BE996707A250633B9947D091
SHA-512:	DF5D60F888F9DA3BD78B9E551027813BA174DB212D546F545214267BE3EF96AF2247A0A27BC8B55BDC516DF337F70EA349D7D6AE3D3CFA51919E64F6A99BFB9 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...7'|....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iLl54/y4/l/en_US/u5b7Jnjloqb.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....u./.....7ju@.....pw. ..H.....sB._.A..Eo.....).....A..Eo.....'.U.....O.....g.....(S....`j....XL`(.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js... ..`.....M`.....QcB.\|....Y3BFH.....Qb.1tb...__d..$Qgnq.....getInlineBoundingRect.....`.....M`.....Qbb.....Rect.(S.<.`.....L`.....0Rc.....O.`....I`....Da....R....(S.....Ia..... ...M...a..@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3iLl54/y4/l/en_US/u5b7Jnjloqb.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`....D`.....`r...&...&....&..!.&.(S.E...`@ .....L`L.....RcT....."....Qb.....h.....O....S...Qb:..4....j.....Qb.p.....k.....QbN.....l.....Qb.....m.....Qb...o....n.....Qb.....o.....Qb.<.....p.....Qb2.J....q.....Qb.Sp.....r.....QbN

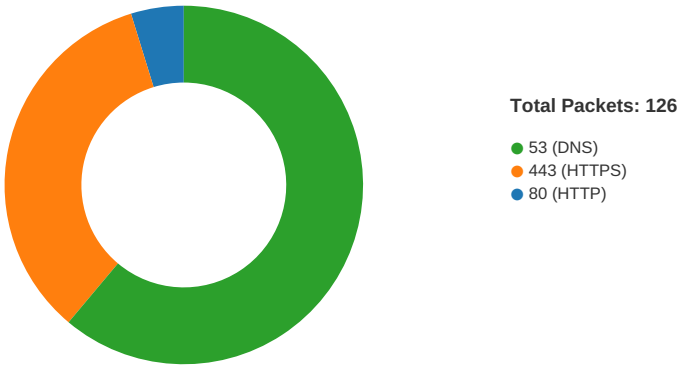
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75e1b5e53cdd2d27_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	11336
Entropy (8bit):	5.835545187100427
Encrypted:	false
SSDEEP:	192:bEML0iGEz/4LLU8otLffkOSETmusKzp8j2+mlkk+3WZ1Wt+BWU7W:bEIYk4Hm7tTXt8j3muoXYUq
MD5:	D026D3ACE86B3925746E5026DE599060
SHA1:	EFC835DA399F55F3CBC33630F323FD6EE75EDFC5
SHA-256:	CDD902CA294A404ED46DCE9AC834A9FB92AED0872E925E762EB7408ABF1E9710
SHA-512:	5AEF7B03277BE5DCE11353CECFE59A30B282BB1B60332B7FE109A874A6A6BD5CD1FC2CCF27AF5AF8EB72FFD345499CB595DF4ACC6D9D5A061DFCA20A9C3C B908
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...JB....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yo/r/5rMGhdMwSK9.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...u./.....W.....Rx...q..=.p....R.K...t.^. .E=....A..Eo.....'V%.....A..Eo.....'..&....O....*.....O.....d.....(S....`.....pL`4.....Qbj$.....self..Q.`>n.....CavalryLogger.....Qc.h,.....start_js. ....`.....M`.....Qc.....v7nDf.....Qb.1tb...__d..(QhFx.A....PresenceViewerCapabilities.....`.....M`.....Qd.)!.....ArbiterMixin..Qe.dSm....PresenceConfig...(S.|.`.....(L`.....8Rc..... .....O.....a.....I`....Da.....Qc..I[....assign.....a.....C.(S.....5.a.....Pd.....assign.get.a....O.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3 /yo/r/5rMGhdMwSK9.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....y....`....&...&....&..1.&.(S....`.....8L`.....HRc .....O...Qb.....h.....S...Qb:..4....j...c.....I`..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 8, 2021 20:25:52.633488894 CET	49728	80	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.634272099 CET	49729	80	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.678246975 CET	80	49728	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.678407907 CET	49728	80	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.678724051 CET	80	49729	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.678747892 CET	49728	80	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.678860903 CET	49729	80	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.724129915 CET	80	49728	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.827898979 CET	80	49728	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.835372925 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.869415045 CET	49728	80	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.878880024 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.878985882 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.879259109 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.922668934 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.929845095 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.929908037 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.929968119 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.929981947 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.941921949 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.941996098 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.942205906 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.985591888 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.985651016 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:52.985711098 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:52.986015081 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.026457071 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.029289961 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.126358032 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.126462936 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.126539946 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.126611948 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.126686096 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.126703978 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.126764059 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.247648954 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.249349117 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.254055023 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.254410982 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.290977955 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.292637110 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.297333002 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.297629118 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.396888971 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.396949053 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.396996975 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.397017956 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.401921988 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.401985884 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.402021885 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.403601885 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.403671980 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.403716087 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.405322075 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.405419111 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.405440092 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.407073021 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.407125950 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.407206059 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.408749104 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.408852100 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.408883095 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.410469055 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.410525084 CET	443	49730	23.185.0.4	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 8, 2021 20:25:53.410582066 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.410609961 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.410660982 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.410800934 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.412153959 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.412205935 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.412286043 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.413863897 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.413925886 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.413969994 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.415590048 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.415652037 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.415697098 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.417263985 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.417324066 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.417361975 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.418968916 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.419008017 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.419375896 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.420670033 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.420723915 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.420769930 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.422373056 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.422482967 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.431386948 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.440262079 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.440324068 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.440344095 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.440377951 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.440424919 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.440479994 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.440509081 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.440589905 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.445364952 CET	443	49730	23.185.0.4	192.168.2.6
Feb 8, 2021 20:25:53.445430994 CET	49730	443	192.168.2.6	23.185.0.4
Feb 8, 2021 20:25:53.445462942 CET	443	49730	23.185.0.4	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 8, 2021 20:25:45.221710920 CET	56061	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:45.270418882 CET	53	56061	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:46.280059099 CET	58336	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:46.333157063 CET	53	58336	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:47.188265085 CET	53781	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:47.247883081 CET	53	53781	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:52.549247026 CET	55299	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:52.552670956 CET	63745	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:52.556946993 CET	50055	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:52.561078072 CET	61374	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:52.609257936 CET	53	55299	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:52.616765022 CET	53	50055	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:52.617671013 CET	53	63745	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:52.632482052 CET	53	61374	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:52.999654055 CET	50339	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:53.067841053 CET	53	50339	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:53.194586992 CET	63307	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:53.255873919 CET	49694	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:53.259810925 CET	53	63307	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:53.315570116 CET	53	49694	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:53.672465086 CET	50010	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:53.737888098 CET	53	50010	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:53.896784067 CET	63718	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:53.955246925 CET	53	63718	8.8.8.8	192.168.2.6

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 8, 2021 20:25:54.411523104 CET	62116	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:54.460241079 CET	53	62116	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:54.545629978 CET	63816	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:54.613068104 CET	53	63816	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:56.202172041 CET	55014	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:56.266948938 CET	53	55014	8.8.8.8	192.168.2.6
Feb 8, 2021 20:25:57.542294025 CET	56628	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:25:57.604666948 CET	53	56628	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:02.231687069 CET	54683	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:02.285479069 CET	53	54683	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:08.359838963 CET	64021	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:08.411046982 CET	53	64021	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:09.291347980 CET	56129	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:09.340004921 CET	53	56129	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:10.054495096 CET	58177	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:10.119472980 CET	53	58177	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:10.863219976 CET	50700	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:10.913734913 CET	53	50700	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:11.799091101 CET	54069	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:11.863730907 CET	53	54069	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:15.836270094 CET	61178	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:15.893456936 CET	53	61178	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:16.694888115 CET	57017	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:16.746459007 CET	53	57017	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:17.496007919 CET	56327	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:17.547188997 CET	53	56327	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:18.377974987 CET	50243	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:18.439625978 CET	53	50243	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:19.585757971 CET	62055	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:19.637084007 CET	53	62055	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:20.171071053 CET	61249	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:20.221378088 CET	65252	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:20.226974964 CET	64367	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:20.227628946 CET	55066	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:20.231957912 CET	53	61249	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:20.281564951 CET	53	65252	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:20.284279108 CET	53	64367	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:20.288923979 CET	53	55066	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:20.784142017 CET	60211	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:20.852643013 CET	53	60211	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:23.652072906 CET	56570	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:23.710720062 CET	53	56570	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:24.523927927 CET	58454	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:24.572618008 CET	53	58454	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:25.088176966 CET	55180	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:25.088947058 CET	58721	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:25.089514971 CET	57691	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:25.139466047 CET	53	55180	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:25.148842096 CET	53	58721	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:25.151662111 CET	53	57691	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:25.299313068 CET	52943	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:25.302967072 CET	59489	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:25.350061893 CET	53	52943	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:25.362382889 CET	53	59489	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:27.357177973 CET	64022	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:27.408349991 CET	53	64022	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:27.512366056 CET	60023	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:27.523125887 CET	57193	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:27.571492910 CET	53	60023	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:27.585177898 CET	53	57193	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:29.667967081 CET	50248	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:29.733191013 CET	53	50248	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:30.225605965 CET	64413	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:30.285609961 CET	53	64413	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 8, 2021 20:26:31.029550076 CET	60429	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:31.096110106 CET	53	60429	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:31.182950020 CET	60345	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:31.245186090 CET	53	60345	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:32.107492924 CET	58730	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:32.164712906 CET	53	58730	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:32.657753944 CET	57226	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:32.707012892 CET	53	57226	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:33.599519968 CET	57880	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:33.664319038 CET	53	57880	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:34.126111984 CET	60850	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:34.177537918 CET	53	60850	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:34.339936972 CET	53187	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:34.409400940 CET	53	53187	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:35.186882019 CET	55830	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:35.253047943 CET	53	55830	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:35.304821014 CET	55145	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:35.365176916 CET	53	55145	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:36.737760067 CET	64091	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:36.786305904 CET	53	64091	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:37.296865940 CET	55728	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:37.358901978 CET	53	55728	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:38.538053036 CET	55694	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:38.601622105 CET	53	55694	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:40.948251963 CET	53926	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:41.007416964 CET	53	53926	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:50.075344086 CET	65531	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:50.136709929 CET	53	65531	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:50.527008057 CET	65437	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:50.594053984 CET	53	65437	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:51.536128998 CET	51318	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:51.600739002 CET	53	51318	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:52.903230906 CET	60888	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:26:52.966881037 CET	53	60888	8.8.8.8	192.168.2.6
Feb 8, 2021 20:26:53.404536009 CET	60889	443	192.168.2.6	108.177.15.156
Feb 8, 2021 20:26:53.456913948 CET	443	60889	108.177.15.156	192.168.2.6
Feb 8, 2021 20:26:53.456964970 CET	443	60889	108.177.15.156	192.168.2.6
Feb 8, 2021 20:26:53.458538055 CET	60889	443	192.168.2.6	108.177.15.156
Feb 8, 2021 20:26:53.512032032 CET	443	60889	108.177.15.156	192.168.2.6
Feb 8, 2021 20:26:53.513330936 CET	60889	443	192.168.2.6	108.177.15.156
Feb 8, 2021 20:26:53.565872908 CET	443	60889	108.177.15.156	192.168.2.6
Feb 8, 2021 20:26:53.579478979 CET	60889	443	192.168.2.6	108.177.15.156
Feb 8, 2021 20:26:53.581309080 CET	60889	443	192.168.2.6	108.177.15.156
Feb 8, 2021 20:26:53.634288073 CET	443	60889	108.177.15.156	192.168.2.6
Feb 8, 2021 20:26:53.634330034 CET	443	60889	108.177.15.156	192.168.2.6
Feb 8, 2021 20:26:53.634769917 CET	60889	443	192.168.2.6	108.177.15.156
Feb 8, 2021 20:27:06.939956903 CET	58474	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:06.997497082 CET	53	58474	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:07.610533953 CET	64575	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:07.669711113 CET	53	64575	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:08.131999969 CET	59092	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:08.180676937 CET	53	59092	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:08.199198961 CET	57483	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:08.267695904 CET	53	57483	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:08.559040070 CET	53830	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:08.585527897 CET	60889	443	192.168.2.6	108.177.15.156
Feb 8, 2021 20:27:08.618992090 CET	53	53830	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:08.662916899 CET	443	60889	108.177.15.156	192.168.2.6
Feb 8, 2021 20:27:09.033103943 CET	49809	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:09.081895113 CET	53	49809	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:09.685209990 CET	52814	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:09.747241974 CET	53	52814	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:10.227988005 CET	51069	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:10.287957907 CET	53	51069	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 8, 2021 20:27:10.879354000 CET	56526	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:10.930008888 CET	53	56526	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:11.571029902 CET	50512	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:11.628118038 CET	53	50512	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:12.007980108 CET	51679	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:12.065447092 CET	53	51679	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:21.927844048 CET	56071	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:21.929682016 CET	58950	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:21.988430977 CET	53	56071	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:21.992706060 CET	53	58950	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:22.118452072 CET	57035	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:22.188558102 CET	53	57035	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:22.312496901 CET	54122	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:22.371587038 CET	53	54122	8.8.8.8	192.168.2.6
Feb 8, 2021 20:27:38.744983912 CET	56759	53	192.168.2.6	8.8.8.8
Feb 8, 2021 20:27:38.803793907 CET	53	56759	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 8, 2021 20:25:52.561078072 CET	192.168.2.6	8.8.8.8	0x83f7	Standard query (0)	www.abmcovidvaccine.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:25:53.896784067 CET	192.168.2.6	8.8.8.8	0x93fb	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:25:54.411523104 CET	192.168.2.6	8.8.8.8	0x50e6	Standard query (0)	www.abmcovidvaccine.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:25:56.202172041 CET	192.168.2.6	8.8.8.8	0xd933	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:18.377974987 CET	192.168.2.6	8.8.8.8	0xa507	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:19.585757971 CET	192.168.2.6	8.8.8.8	0x59f7	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:20.171071053 CET	192.168.2.6	8.8.8.8	0x81ae	Standard query (0)	scontent-frx5-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:20.221378088 CET	192.168.2.6	8.8.8.8	0x536	Standard query (0)	external-frt3-2.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:20.226974964 CET	192.168.2.6	8.8.8.8	0x40a	Standard query (0)	scontent-frt3-2.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:20.227628946 CET	192.168.2.6	8.8.8.8	0x274a	Standard query (0)	scontent-frt3-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:20.784142017 CET	192.168.2.6	8.8.8.8	0x5bf1	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:23.652072906 CET	192.168.2.6	8.8.8.8	0xc4bb	Standard query (0)	scontent.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:24.523927927 CET	192.168.2.6	8.8.8.8	0xeae4	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.088176966 CET	192.168.2.6	8.8.8.8	0x2c3e	Standard query (0)	api.twitter.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.088947058 CET	192.168.2.6	8.8.8.8	0x47c9	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.089514971 CET	192.168.2.6	8.8.8.8	0x7c90	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.299313068 CET	192.168.2.6	8.8.8.8	0xd78f	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.302967072 CET	192.168.2.6	8.8.8.8	0xe85d	Standard query (0)	video.twimg.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:27.357177973 CET	192.168.2.6	8.8.8.8	0xb90b	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:27.512366056 CET	192.168.2.6	8.8.8.8	0x919b	Standard query (0)	scontent-frx5-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:27.523125887 CET	192.168.2.6	8.8.8.8	0xb92d	Standard query (0)	scontent-frt3-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:29.667967081 CET	192.168.2.6	8.8.8.8	0x8	Standard query (0)	external-frt3-2.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:30.225605965 CET	192.168.2.6	8.8.8.8	0x2579	Standard query (0)	scontent-frt3-2.xx.fbcdn.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:31.029550076 CET	192.168.2.6	8.8.8.8	0x3a37	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:31.182950020 CET	192.168.2.6	8.8.8.8	0x5a7	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 8, 2021 20:26:32.107492924 CET	192.168.2.6	8.8.8.8	0x7a59	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:32.657753944 CET	192.168.2.6	8.8.8.8	0x5443	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:33.599519968 CET	192.168.2.6	8.8.8.8	0x240b	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:34.339936972 CET	192.168.2.6	8.8.8.8	0x38b0	Standard query (0)	media-exp1.licdn.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:35.186882019 CET	192.168.2.6	8.8.8.8	0x731f	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:35.304821014 CET	192.168.2.6	8.8.8.8	0x2008	Standard query (0)	media-exp1.licdn.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:36.737760067 CET	192.168.2.6	8.8.8.8	0xbeac	Standard query (0)	instagram.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:37.296865940 CET	192.168.2.6	8.8.8.8	0x5c82	Standard query (0)	www.instagram.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:38.538053036 CET	192.168.2.6	8.8.8.8	0x24cd	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:40.948251963 CET	192.168.2.6	8.8.8.8	0x5c6d	Standard query (0)	www.instagram.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:52.903230906 CET	192.168.2.6	8.8.8.8	0x7b48	Standard query (0)	www.abmcovidvaccine.com	A (IP address)	IN (0x0001)
Feb 8, 2021 20:27:38.744983912 CET	192.168.2.6	8.8.8.8	0x597e	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 8, 2021 20:25:52.632482052 CET	8.8.8.8	192.168.2.6	0x83f7	No error (0)	www.abmcovidvaccine.com		23.185.0.4	A (IP address)	IN (0x0001)
Feb 8, 2021 20:25:53.955246925 CET	8.8.8.8	192.168.2.6	0x93fb	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:25:53.955246925 CET	8.8.8.8	192.168.2.6	0x93fb	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Feb 8, 2021 20:25:53.955246925 CET	8.8.8.8	192.168.2.6	0x93fb	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Feb 8, 2021 20:25:53.955246925 CET	8.8.8.8	192.168.2.6	0x93fb	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Feb 8, 2021 20:25:53.955246925 CET	8.8.8.8	192.168.2.6	0x93fb	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Feb 8, 2021 20:25:54.460241079 CET	8.8.8.8	192.168.2.6	0x50e6	No error (0)	www.abmcovidvaccine.com		23.185.0.4	A (IP address)	IN (0x0001)
Feb 8, 2021 20:25:56.266948938 CET	8.8.8.8	192.168.2.6	0xd933	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:25:56.266948938 CET	8.8.8.8	192.168.2.6	0xd933	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.33	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:18.439625978 CET	8.8.8.8	192.168.2.6	0xa507	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:18.439625978 CET	8.8.8.8	192.168.2.6	0xa507	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:19.637084007 CET	8.8.8.8	192.168.2.6	0x59f7	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:19.637084007 CET	8.8.8.8	192.168.2.6	0x59f7	No error (0)	scontent.xx.fbcdn.net		157.240.9.23	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:20.231957912 CET	8.8.8.8	192.168.2.6	0x81ae	No error (0)	scontent-frx5-1.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:20.281564951 CET	8.8.8.8	192.168.2.6	0x536	No error (0)	external-frt3-2.xx.fbcdn.net	scontent-frt3-2.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:20.281564951 CET	8.8.8.8	192.168.2.6	0x536	No error (0)	scontent-frt3-2.xx.fbcdn.net		157.240.20.19	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 8, 2021 20:26:20.284279108 CET	8.8.8.8	192.168.2.6	0x40a	No error (0)	scontent-frt3-2.xx.fbcdn.net		157.240.20.19	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:20.288923979 CET	8.8.8.8	192.168.2.6	0x274a	No error (0)	scontent-frt3-1.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:20.852643013 CET	8.8.8.8	192.168.2.6	0x5bf1	No error (0)	facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:23.710720062 CET	8.8.8.8	192.168.2.6	0xc4bb	No error (0)	scontent.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:24.572618008 CET	8.8.8.8	192.168.2.6	0xeae4	No error (0)	twitter.com		104.244.42.1	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:24.572618008 CET	8.8.8.8	192.168.2.6	0xeae4	No error (0)	twitter.com		104.244.42.65	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.139466047 CET	8.8.8.8	192.168.2.6	0x2c3e	No error (0)	api.twitter.com	tpop-api.twitter.com		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:25.139466047 CET	8.8.8.8	192.168.2.6	0x2c3e	No error (0)	tpop-api.twitter.com		104.244.42.130	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.139466047 CET	8.8.8.8	192.168.2.6	0x2c3e	No error (0)	tpop-api.twitter.com		104.244.42.2	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.139466047 CET	8.8.8.8	192.168.2.6	0x2c3e	No error (0)	tpop-api.twitter.com		104.244.42.194	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.139466047 CET	8.8.8.8	192.168.2.6	0x2c3e	No error (0)	tpop-api.twitter.com		104.244.42.66	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.148842096 CET	8.8.8.8	192.168.2.6	0x47c9	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:25.148842096 CET	8.8.8.8	192.168.2.6	0x47c9	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:25.148842096 CET	8.8.8.8	192.168.2.6	0x47c9	No error (0)	cs2-wac-eu.8315.ecdns.net	cs672.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:25.148842096 CET	8.8.8.8	192.168.2.6	0x47c9	No error (0)	cs672.wac.edgecastcdn.net		192.229.233.50	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.151662111 CET	8.8.8.8	192.168.2.6	0x7c90	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:25.151662111 CET	8.8.8.8	192.168.2.6	0x7c90	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.350061893 CET	8.8.8.8	192.168.2.6	0xd78f	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.350061893 CET	8.8.8.8	192.168.2.6	0xd78f	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.350061893 CET	8.8.8.8	192.168.2.6	0xd78f	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.350061893 CET	8.8.8.8	192.168.2.6	0xd78f	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:25.362382889 CET	8.8.8.8	192.168.2.6	0xe85d	No error (0)	video.twimg.com	cs296.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:25.362382889 CET	8.8.8.8	192.168.2.6	0xe85d	No error (0)	cs296.wpc.edgecastcdn.net	cs2-wpc.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:25.362382889 CET	8.8.8.8	192.168.2.6	0xe85d	No error (0)	cs2-wpc-eu.8315.ecdns.net	cs189.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:25.362382889 CET	8.8.8.8	192.168.2.6	0xe85d	No error (0)	cs189.wpc.edgecastcdn.net		68.232.34.217	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:27.408349991 CET	8.8.8.8	192.168.2.6	0xb90b	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 8, 2021 20:26:27.408349991 CET	8.8.8.8	192.168.2.6	0xb90b	No error (0)	scontent.x x.fbcdn.net		157.240.9.23	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:27.571492910 CET	8.8.8.8	192.168.2.6	0x919b	No error (0)	scontent-frx5-1.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:27.585177898 CET	8.8.8.8	192.168.2.6	0xb92d	No error (0)	scontent-frt3-1.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:29.733191013 CET	8.8.8.8	192.168.2.6	0x8	No error (0)	external-frt3-2.xx.fbcdn.net	scontent-frt3-2.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:29.733191013 CET	8.8.8.8	192.168.2.6	0x8	No error (0)	scontent-frt3-2.xx.fbcdn.net		157.240.20.19	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:30.285609961 CET	8.8.8.8	192.168.2.6	0x2579	No error (0)	scontent-frt3-2.xx.fbcdn.net		157.240.20.19	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:31.096110106 CET	8.8.8.8	192.168.2.6	0x3a37	No error (0)	facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:31.245186090 CET	8.8.8.8	192.168.2.6	0x5a7	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:31.245186090 CET	8.8.8.8	192.168.2.6	0x5a7	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:32.164712906 CET	8.8.8.8	192.168.2.6	0x7a59	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:32.164712906 CET	8.8.8.8	192.168.2.6	0x7a59	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:32.164712906 CET	8.8.8.8	192.168.2.6	0x7a59	No error (0)	cs2-wac-eu.8315.ecdns.net	cs672.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:32.164712906 CET	8.8.8.8	192.168.2.6	0x7a59	No error (0)	cs672.wac.edgecastcdn.net		192.229.233.50	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:32.707012892 CET	8.8.8.8	192.168.2.6	0x5443	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:33.664319038 CET	8.8.8.8	192.168.2.6	0x240b	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:33.664319038 CET	8.8.8.8	192.168.2.6	0x240b	No error (0)	cs1404.wpc.epsiloncdn.net		152.199.21.118	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:34.409400940 CET	8.8.8.8	192.168.2.6	0x38b0	No error (0)	media-exp1.licdn.com	2-01-2c3e-005c.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:34.409400940 CET	8.8.8.8	192.168.2.6	0x38b0	No error (0)	cs1404.wpc.epsiloncdn.net		152.199.21.118	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:35.253047943 CET	8.8.8.8	192.168.2.6	0x731f	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:35.365176916 CET	8.8.8.8	192.168.2.6	0x2008	No error (0)	media-exp1.licdn.com	2-01-2c3e-005c.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:35.365176916 CET	8.8.8.8	192.168.2.6	0x2008	No error (0)	cs1404.wpc.epsiloncdn.net		152.199.21.118	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:36.786305904 CET	8.8.8.8	192.168.2.6	0xbeac	No error (0)	instagram.com		52.22.200.157	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:36.786305904 CET	8.8.8.8	192.168.2.6	0xbeac	No error (0)	instagram.com		3.220.76.115	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:36.786305904 CET	8.8.8.8	192.168.2.6	0xbeac	No error (0)	instagram.com		34.197.183.108	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:36.786305904 CET	8.8.8.8	192.168.2.6	0xbeac	No error (0)	instagram.com		3.224.36.18	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:36.786305904 CET	8.8.8.8	192.168.2.6	0xbeac	No error (0)	instagram.com		34.192.95.2	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 8, 2021 20:26:36.786305904 CET	8.8.8.8	192.168.2.6	0xbeac	No error (0)	instagram.com		3.210.57.193	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:36.786305904 CET	8.8.8.8	192.168.2.6	0xbeac	No error (0)	instagram.com		18.214.241.0	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:36.786305904 CET	8.8.8.8	192.168.2.6	0xbeac	No error (0)	instagram.com		35.171.109.191	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:37.358901978 CET	8.8.8.8	192.168.2.6	0x5c82	No error (0)	www.instagram.com	z-p42-instagram.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:37.358901978 CET	8.8.8.8	192.168.2.6	0x5c82	No error (0)	z-p42-instagram.c10r.facebook.com		185.60.216.174	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:38.601622105 CET	8.8.8.8	192.168.2.6	0x24cd	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:38.601622105 CET	8.8.8.8	192.168.2.6	0x24cd	No error (0)	scontent.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:41.007416964 CET	8.8.8.8	192.168.2.6	0x5c6d	No error (0)	www.instagram.com	z-p42-instagram.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Feb 8, 2021 20:26:41.007416964 CET	8.8.8.8	192.168.2.6	0x5c6d	No error (0)	z-p42-instagram.c10r.facebook.com		185.60.216.174	A (IP address)	IN (0x0001)
Feb 8, 2021 20:26:52.966881037 CET	8.8.8.8	192.168.2.6	0x7b48	No error (0)	www.abmcovidvaccine.com		23.185.0.4	A (IP address)	IN (0x0001)
Feb 8, 2021 20:27:38.803793907 CET	8.8.8.8	192.168.2.6	0x597e	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- www.abmcovidvaccine.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49728	23.185.0.4	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 8, 2021 20:25:52.678747892 CET	104	OUT	GET / HTTP/1.1 Host: www.abmcovidvaccine.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Feb 8, 2021 20:25:52.827898979 CET	116	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html Location: https://www.abmcovidvaccine.com/ Server: nginx X-Pantheon-Styx-Hostname: styx-fe4-a-695744c5c6-wzlfh X-Styx-Req-Id: 05692159-6a34-11eb-ad43-d2fb8bff6f1f Cache-Control: public, max-age=86400 Content-Length: 162 Date: Mon, 08 Feb 2021 19:25:52 GMT Connection: keep-alive X-Served-By: cache-mdw17326-MDW, cache-hhn4043-HHN X-Cache: HIT, MISS X-Cache-Hits: 1, 0 X-Timer: S1612812353.715658,VS0,VE104 Vary: Cookie, Cookie Age: 6630 Accept-Ranges: bytes Via: 1.1 varnish, 1.1 varnish Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 8, 2021 20:25:52.929908037 CET	23.185.0.4	443	192.168.2.6	49730	CN=abmcovidvaccine.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jan 25 22:35:58 CET 2021	Sun Apr 25 23:35:58 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 8, 2021 20:25:54.564218998 CET	23.185.0.4	443	192.168.2.6	49744	CN=abmcovidvaccine.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jan 25 22:35:58 CET 2021	Sun Apr 25 23:35:58 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4696 Parent PID: 1560

General

Start time:	20:25:49
Start date:	08/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://www.abmcovidvaccine.com'
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 6224 Parent PID: 4696

General

Start time:	20:25:50
Start date:	08/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1312,15472918294386558836,11097865136599668024,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1740 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: chrome.exe PID: 7200 Parent PID: 4696

General

Start time:	20:26:31
Start date:	08/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1312,15472918294386558836,11097865136599668024,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5688 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Copyright null 2021