ID: 412595
Cookbook: browseurl.jbs
Time: 19:59:17
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

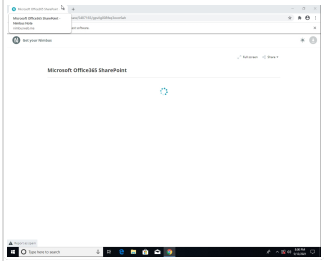
Analysis Report https://nimbusweb.me/s/share/5487165…

Overview

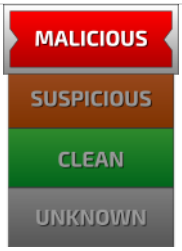
General Information

Sample URL:	http://https://nimbusweb.me/s/share/5487165/gpvilg008fxq3oxcr6eh
Analysis ID:	412595
Infos:	

Most interesting Screenshot:



Detection



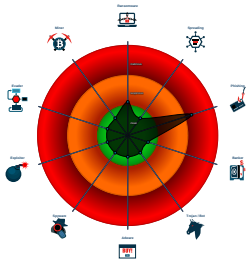
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish29

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 4656 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://nimbusweb.me/s/share/5487165/gpvilg008fxq3oxcr6eh' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1764 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1604,7990105799513037393,10231270219144405014,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

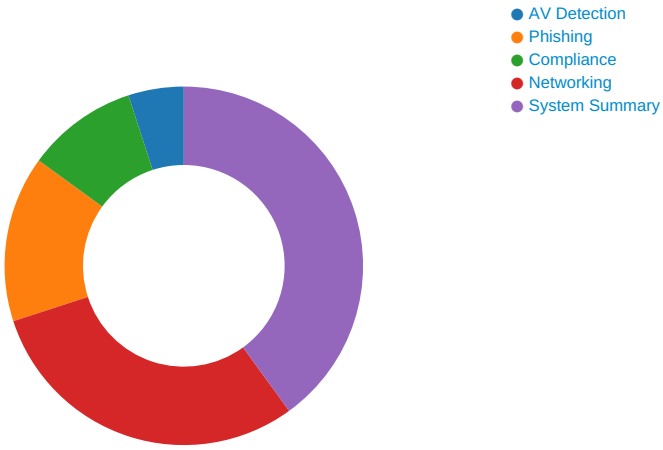
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

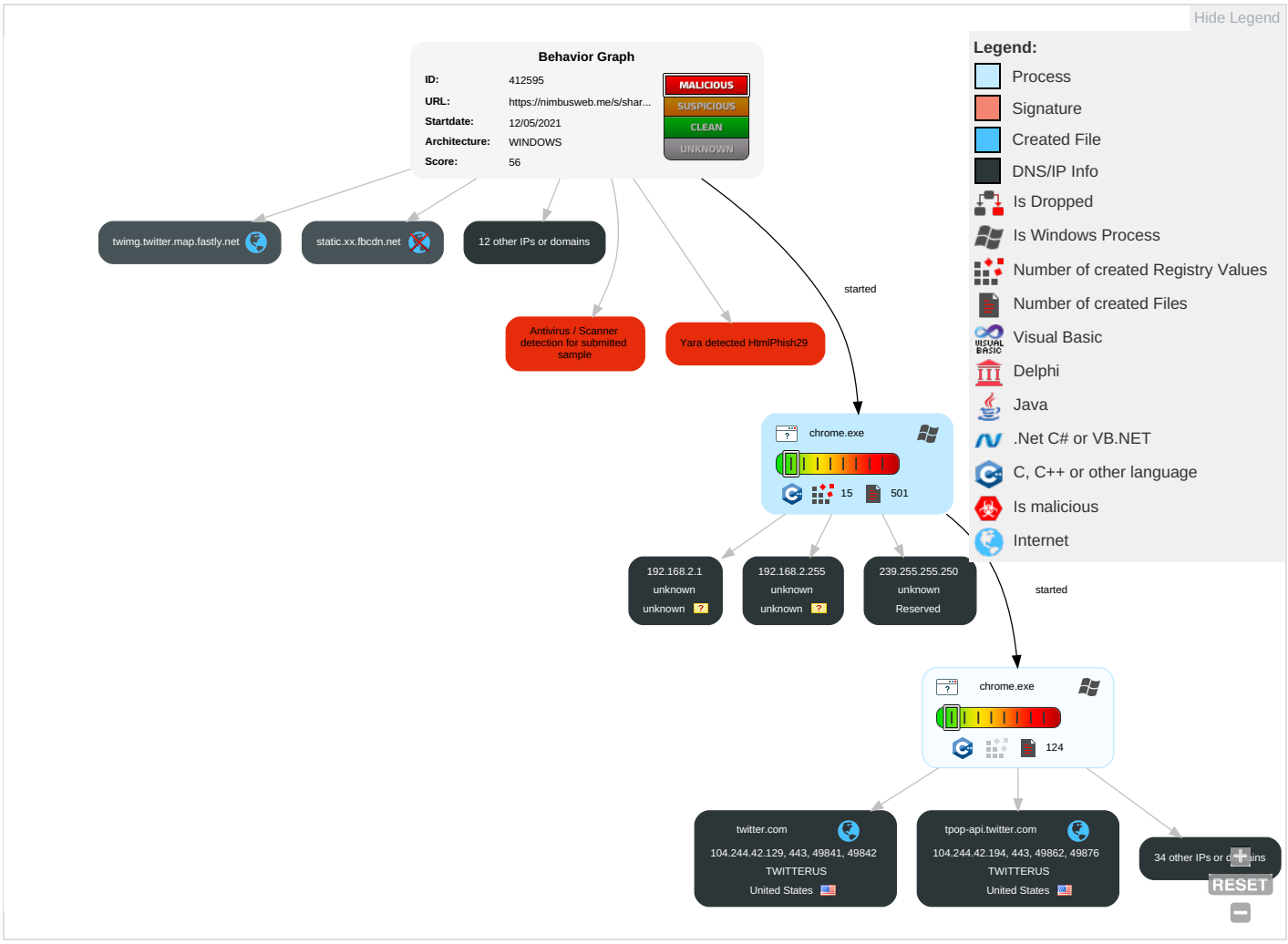
Phishing:

Yara detected HtmlPhish29

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	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

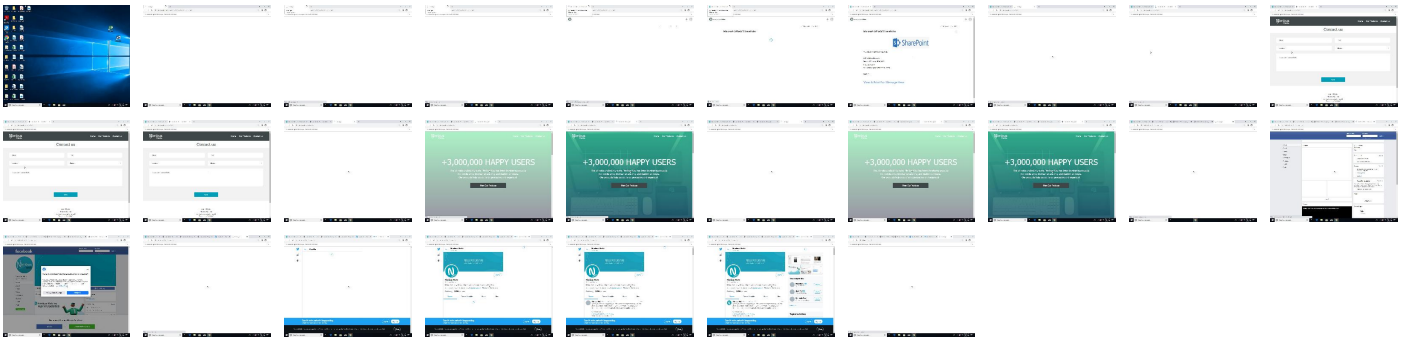
Behavior Graph

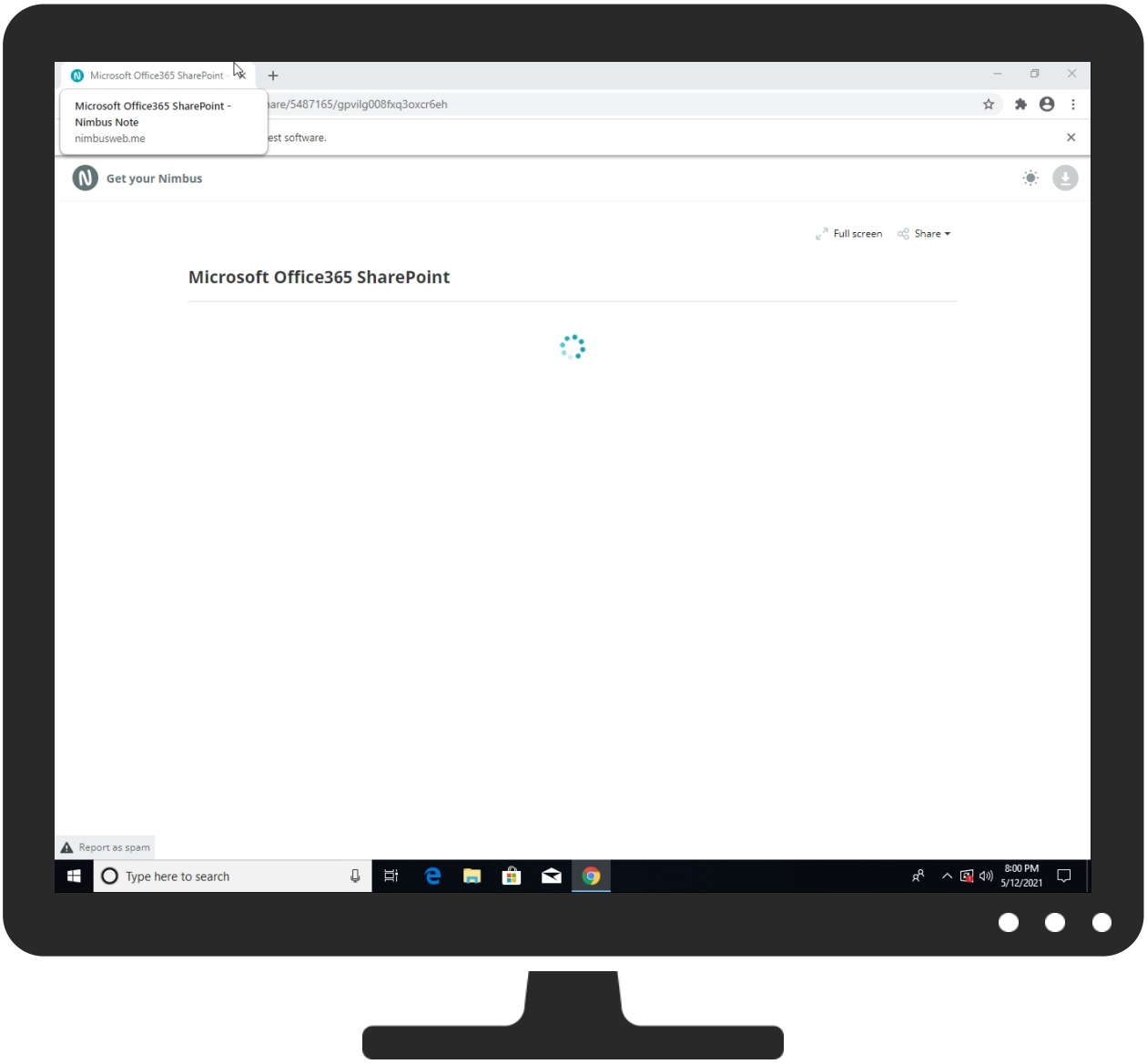


Screenshots

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://https://nimbusweb.me/s/share/5487165/gpvilg008fxq3oxcr6eh	0%	Virustotal		Browse
http://https://nimbusweb.me/s/share/5487165/gpvilg008fxq3oxcr6eh	0%	Avira URL Cloud	safe	
http://https://nimbusweb.me/s/share/5487165/gpvilg008fxq3oxcr6eh	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
text.nimbusweb.me	0%	Virustotal		Browse
nimbusweb.co	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://nimbusweb.co/eh	0%	Avira URL Cloud	safe	
http://https://nimbusweb.co/js/jquery.js	0%	Avira URL Cloud	safe	
http://https://nimbusweb.co/index.phpNimbus	0%	Avira URL Cloud	safe	
http://https://nimbusweb.co/	0%	Avira URL Cloud	safe	
http://https://nimbusweb.me/s/share/5487165/gpvilg008fxq3oxcr6ehMicrosoft	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.de	142.250.185.227	true	false		high
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	104.244.42.129	true	false		high
stats.l.doubleclick.net	74.125.140.157	true	false		high
cs45.wac.edgecastcdn.net	93.184.220.70	true	false		high
text.nimbusweb.me	13.224.193.49	true	false	• 0%, Virustotal, Browse	unknown
nimbusweb.co	54.173.51.37	true	false	• 0%, Virustotal, Browse	unknown
scontent-frt3-1.xx.fbcdn.net	31.13.92.14	true	false		high
tpop-api.twitter.com	104.244.42.194	true	false		high
lil-tex.com	64.4.160.22	true	false		unknown
scontent.xx.fbcdn.net	157.240.9.23	true	false		high
t.co	104.244.42.197	true	false		high
twimg.twitter.map.fastly.net	199.232.136.159	true	false		unknown
scontent-frt3-2.xx.fbcdn.net	157.240.20.19	true	false		high
abs-zero.twimg.com	104.244.43.131	true	false		high
facebook.com	185.60.216.35	true	false		high
nimbusweb.me	13.224.193.106	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
cs510.wpc.edgecastcdn.net	152.199.21.141	true	false		high
dojq4kt8ws9iq.cloudfront.net	13.225.74.128	true	false		high
cs189.wpc.edgecastcdn.net	68.232.34.217	true	false		high
www.facebook.com	unknown	unknown	false		high
abs.twimg.com	unknown	unknown	false		high
pbs.twimg.com	unknown	unknown	false		high
abs-0.twimg.com	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
cdn.polyfill.io	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
video.twimg.com	unknown	unknown	false		high

URLs from Memory and Binaries

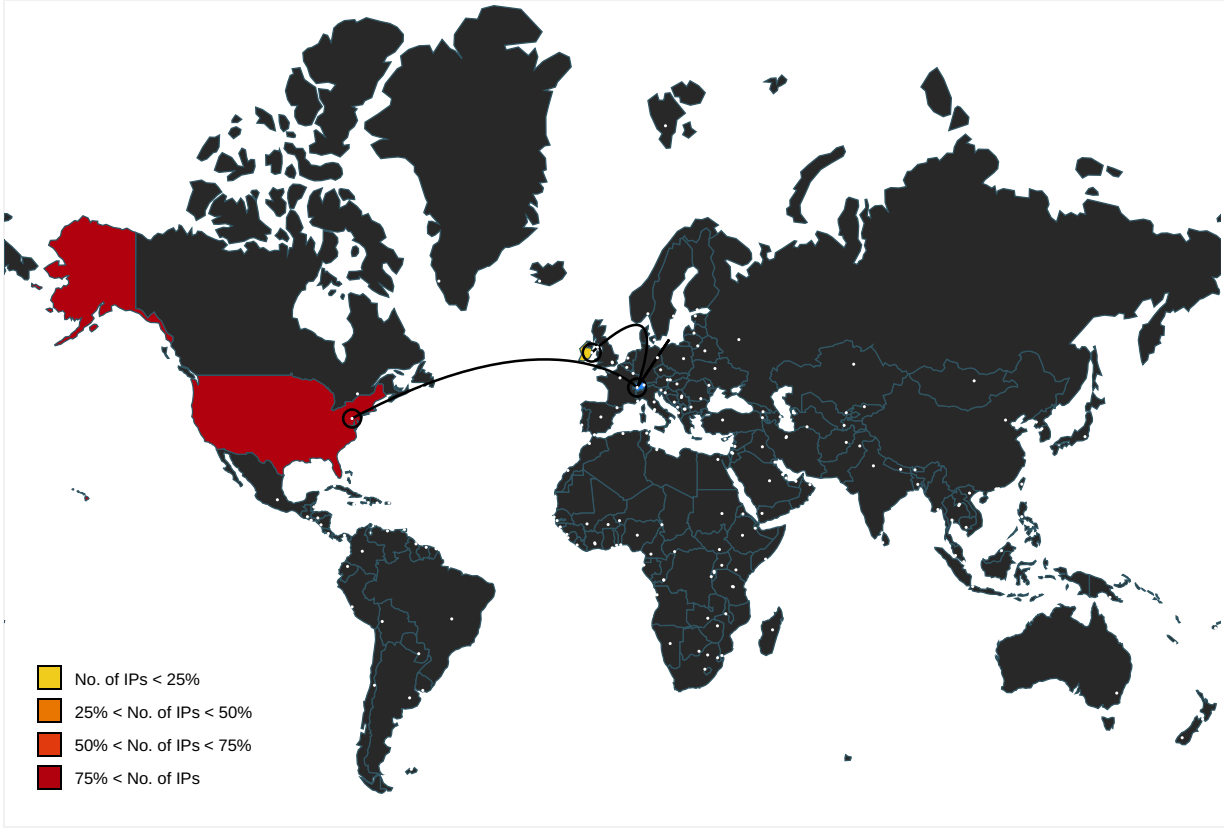
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://abs.twimg.com/responsive-web/client-web/bundle.Compose.bb8e7605.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.TopicPeek.0cc576a5.jsHP	abf138ca59892482_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.ca.647ea0c5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Place.1617e065.jsaD	aed3b57bcf1e856a_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/vendors~main.39dc8d45.jswindow.__SCRIPTS_LOADED__.po	39dbbe6818a53d77_0.0.dr	false		high
http://https://nimbusweb.co/eh	cdb83eebe773cdb3_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://abs.twimg.com/responsive-web/client-web/bundle.SettingsTransparency.02604aa5.jsHP	87644af6b51a6ad1_0.0.dr	false		high
http://https://support.twitter.com/articles/14606#receipts	1143296cb91f4bf0_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-sv.d33ba7a5.js	2cc80dabc69f58b6_1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://abs.twimg.com/responsive-web/client-web/bundle.UserProfile.b77dc905.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yv/r/z3z79uMaXna.js?_nc_x=Ij3Wp8lg5Kz	d107783cb78f491d_0.0.dr	false		high
http://https://nimbusweb.co/js/jquery.js	641ca75826dd58da_0.0.dr, 173a532107de75b5_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.pt.2f9c4b45.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yk/r/rigRDZa6ZK5.js?_nc_x=Ij3Wp8lg5Kz	796754b66abe62b8_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.AccountVerification.1191b445.jsaD	788e600a30af0414_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.gl.3a2abf95.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://upload.twitter.com	2cc80dabc69f58b6_0.0.dr, af47be93e4c33dc6_0.0.dr	false		high
http://https://twitter.com/i/communities/	4c3e81166a1c9a93_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-eu.ddf519a5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/loader.personalizationData.508	25a98aaed0e84a36_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Newsletters.d2caf8e5.jsH	e0762565f86a2f61_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-hr.6f17dcf5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.Display.e95e1ae5.js.map	cbd2b40617cff506_1.0.dr, cbd2b40617cff506_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yI/r/Gatc1qImxiw.js?_nc_x=Ij3Wp8lg5Kz	d3847cb6775d1f00_0.0.dr	false		high
http://https://twitter.com/sw.js	000003.log8.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.Collection.e43b8d95.js.	e2f3da9ce2ca7030_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.hi.644fb9c5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.QuoteTweetActivity.4cad	b8e9acb8bd5fcd01_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.pl.d3a4f2f5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Display.e95e1ae5.jsHP	cbd2b40617cff506_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/shared~loader.DashMenu~bundle.Account.8eb9f6c5.jsHP	f199fccf6f5d7d0b_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Search.a5b9c825.jsaD	6c262850ff790655_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Settings.410a8c05.jsaD	1143296cb91f4bf0_1.0.dr	false		high
http://https://abs.twimg.com/a/1501527574/img/t1/icon_giphy.png	42e0defdcd79b8f8_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iPwL4/yd/l/en_US/d-YpByGjyvG.js?_nc_x=Ij3Wp8lg5Kz	10438f4122c99db4_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.da.cec1d715.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iQ5J4/y7/l/en_US/tv_DX8Bjdmb.js?_nc_x=Ij3Wp8lg5Kz	5e2e4f9692f0b13a_0.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.NotificationDetail.0fe2	db067625080c12d5_1.0.dr, db067625080c12d5_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.UserLists.c2074835.jsa	201e2fc12ec09dc8_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loaders.video.PlayerHls14.388b3825.jsaD	118514efb6047977_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Compose.bb8e7605.jsHP	99280e1025b54c1c_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.TweetMediaDetail.1ae54155.jsaD	76af4c9ea739a4ce_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/polyfills.ae028905.js	2cc80dabc69f58b6_1.0.dr, 49c24b5e17704bab_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yA/r/rOuGauB8Oni.js?_nc_x=Ij3Wp8lg5Kz	307cad7e2ff3c9a7_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.MultiAccount.7a2e5035.jsHP	b4954de4d068713e_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loaders.video.PlayerHls14.388b3825.jsH	118514efb6047977_0.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.ConnectTab.236a7f05.js.	8a461fe04fe0bdda_1.0.dr, 8a461fe04fe0bdda_0.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.Compose.bb8e7605.js.map	99280e1025b54c1c_1.0.dr, 99280e1025b54c1c_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iJX14/yX/l/en_US/FGjX6fUT-lJ.js?_nc_x=Ij3Wp8lg5Kz	41c9dd3e30ed8205_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.UserAvatar.73a69655.js(window.webpackJsonp=wi	7f92e763241338ba_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-ja.b5d0cdc5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.MomentMaker.a38408e5.jsHP	4c3e81166a1c9a93_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.graphQLDarkReads.3b65a465.js	f891c012b896740f_1.0.dr, 2cc80dabc69f58b6_1.0.dr	false		high
http://https://nimbusweb.co/index.phpNimbus	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://abs.twimg.com/responsive-web/client-web/ondemand.CarouselScroller.7d720395.js	bda8dd17fc710252_0.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/loader.NewTweetsPill.ccf1ef05.	e77ded8c0586da6a_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.DMRichTextCompose.60025425.jsaD	9c425572c16cc439_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.SignupModule.e0700225.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.SettingsRevamp.72744715.jsH	860b1c4a9bda0988_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.GraphQLModule.687ef4d5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://nimbusweb.co/	Network Action Predictor.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.NetworkInstrument.60b62	f5429ca304615972_1.0.dr	false		high
http://https://analytics.twitter.com/	f199fccf6f5d7d0b_1.0.dr	false		high
http://https://help.twitter.com/using-twitter/twitter-videos	1143296cb91f4bf0_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/bundle.AudioSpace.b624d325.js.	576f956182b9579c_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.LoggedOutHome.e03f8125.jsHP	e0afe4ed8b51a5c4_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Conversation.dcc35795.js	3d72ac1b4684a384_1.0.dr, 2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.hr.e46d0465.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://nimbusweb.me/s/share/5487165/gpvilg008fxq3oxcr6ehMicrosoft	History-journal.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://abs.twimg.com/responsive-web/client-web/shared~ondemand.SettingsRevamp~ondemand.SettingsInte	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Topics.15861ce5.js	2cc80dabc69f58b6_1.0.dr, 096b3f1f43b9e4e1_1.0.dr	false		high
http://https://abs.twimg.com/sticky/illustrations/lohp_850x623.png	e0afe4ed8b51a5c4_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.EmojiPicker.4b39da65.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.DashMenu.b7bd3c55.jsH	655a9e6639d1dbc5_0.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/loaders.video.VideoPlayerDefau	22380b58c40ed4cc_1.0.dr	false		high
http://https://vmapstage.snappytv.com	2cc80dabc69f58b6_0.0.dr, af47be93e4c33dc6_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.ProfileClusterFollow.9b98ab85.js	2cc80dabc69f58b6_1.0.dr, 068f63fd8d7ad299_1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.twitter.com/articles/14606#receive	1143296cb91f4bf0_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/shared~bundle.SettingsRevamp~bundle.AccountVerificat	70dfd66834f0cd82_0.0.dr, 2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.FleetsNotification.8f9c3b45.jsHP	74afd99e27e2b001_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/y1/r/UDf5Ho3OCQC.js?_nc_x=Ij3Wp8lg5Kz	4cc8080613f306a2_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.UserProfileGraphQL.716e1465.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.SettingsTransparency.02604aa5.jsH	87644af6b51a6ad1_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.ProfileRedirect.dede26e5.js(window.webpackJso	776b48b2b31971cb_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.Logout.613e15a5.jsHP	ac115b6c6a6f0e91_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iJBN4/yi/l/en_US/1d9GRRVXiDO.js?_nc_x=Ij3Wp8lg5Kz	3c3fbfdba30e0e9a_0.0.dr	false		high
http://https://scontent.xx.fbcdn.net	2cc80dabc69f58b6_0.0.dr, af47be93e4c33dc6_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.ComposeScheduling.ff856e65.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.emoji.en.194bb0f5.js	2cc80dabc69f58b6_1.0.dr, e3ef3e6dbd68003f_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.NotificationDetail.0fe25555.js(window.webpack	db067625080c12d5_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.countries-en-GB.9ed5d665.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://support.twitter.com/	f199fccf6f5d7d0b_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/bundle.OAuth.e65bbc35.js	92ff2d2ef2e565c4_1.0.dr, 2cc80dabc69f58b6_1.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loaders.video.PlayerHls13.036d75e5.js(window.webpack	37e4d244e1ddb65f_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/loader.FeedbackSheet.2dee2bd5.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://help.twitter.com/rules-and-policies/twitter-cookies	e94edab5fd1b281c_1.0.dr	false		high
http://https://clients2.googleusercontent.com	69ecee30-51de-4685-91fb-0ff05952b257.tmp.1.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yw/r/JlxOBbYK8JS.js?_nc_x=Ij3Wp8lg5Kz	b920e1f22b8c708f_0.0.dr	false		high
http://https://abs.twimg.com/responsive-web/client-web/ondemand.SettingsRevamp.410ddd85.js	2cc80dabc69f58b6_1.0.dr	false		high
http://https://ton.twitter.com/responsive-web-internal/sourcemaps/client-web/loaders.video.VideoPlayerEvent	692b4935db22bba2_0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.173.51.37	nimbusweb.co	United States		14618	AMAZON-AESUS	false
104.244.42.129	twitter.com	United States		13414	TWITTERUS	false
13.225.74.128	dojq4kt8ws9iq.cloudfront.net	United States		16509	AMAZON-02US	false
31.13.92.14	scontent-frt3-1.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
142.250.185.227	www.google.de	United States		15169	GOOGLEUS	false
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
68.232.34.217	cs189.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
104.244.43.131	abs-zero.twimg.com	United States		54113	FASTLYUS	false
152.199.21.141	cs510.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
13.224.193.106	nimbusweb.me	United States		16509	AMAZON-02US	false
157.240.9.23	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
104.244.42.197	t.co	United States		13414	TWITTERUS	false
185.60.216.35	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
104.244.42.194	tpop-api.twitter.com	United States		13414	TWITTERUS	false
64.4.160.22	lil-tex.com	United States		4927	IMPUUS	false
74.125.140.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
157.240.20.19	scontent-frt3-2.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
185.60.216.19	scontent-frx5-1.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
13.224.193.49	text.nimbusweb.me	United States		16509	AMAZON-02US	false
93.184.220.70	cs45.wac.edgecastcdn.net	European Union		15133	EDGECASTUS	false

Private

IP
192.168.2.1
192.168.2.255
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412595
Start date:	12.05.2021
Start time:	19:59:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://nimbusweb.me/s/share/5487165/gpvilg008fxq3oxcr6eh
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@43/636@32/24
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://nimbusweb.co/contact.php • Browse: http://nimbusweb.co/index.php • Browse: https://nimbusweb.co/index.php • Browse: https://www.facebook.com/nimbuswebme • Browse: http://twitter.com/nimbuswebinc • Browse: https://lil-tex.com/ofc3

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.147.198.201, 13.88.21.125, 142.250.185.206, 142.250.185.78, 216.58.212.173, 2.20.143.16, 2.20.142.209, 95.168.222.144, 95.168.222.76, 142.250.184.195, 142.250.184.196, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 172.217.16.131, 142.250.181.232, 172.217.16.142, 216.58.212.170, 34.104.35.123, 172.217.16.138, 142.250.185.106, 142.250.185.138, 142.250.185.170, 142.250.185.202, 142.250.185.234, 142.250.181.234, 142.250.74.202, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 142.250.184.202, 142.250.184.234, 184.30.24.56, 216.58.212.131, 95.168.222.83 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs2-wac.apr-8315.edgecastdns.net, r1---sn-n02xgoxufvg3-2gbl.gvt1.com, clientservices.googleapis.com, r5---sn-n02xgoxufvg3-2gbs.gvt1.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, r8.sn-n02xgoxufvg3-2gbl.gvt1.com, clients2.google.com, redirector.gvt1.com, www.googletagmanager.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, dualstack.f3.shared.global.fastly.net, www.google-analytics.com, fs.microsoft.com, accounts.google.com, www-google-analytics.l.google.com, content-autofill.googleapis.com, r5.sn-n02xgoxufvg3-2gbs.gvt1.com, www-googletagmanager.l.google.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, r1.sn-n02xgoxufvg3-2gbl.gvt1.com, www.googleapis.com, skypedataprdcoleus16.cloudapp.net, cs2-wpc.apr-8315.edgecastdns.net, edgedl.me.gvt1.com, blobcollector.events.data.trafficmanager.net, r8---sn-n02xgoxufvg3-2gbl.gvt1.com, clients.l.google.com, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:00:12	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	59863
Entropy (8bit):	**7.99556910241083**
Encrypted:	**true**
SSDEEP:	1536:Gs6cdy9E/ABKQPOrdweEz480zdPMHXNY/gLHfIZN:GNOqOrdDdJPAX1LHA/
MD5:	15775D95513782F99CDFB17E65DFCEB1
SHA1:	6C11F8BEE799B093F9FF4841E31041B081B23388
SHA-256:	477A9559194EDF48848FCE59E05105168745A46BDC0871EA742A2588CA9FBE00
SHA-512:	AC09CE01122D7A837BD70277BADD58FF71D8C5335F8FC599D5E3ED42C8FEE2108DD043BCE562C82BA12A81B9B08BD24B961C0961BF8FD3A0B8341C87483CDE7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	MSCF.....,.....I.....b.....R.i .authroot.stl.qqp.4..CK..8T....c_.d....A.F....m"...AH)-.%.QIR..$t)Kd.-QQ*..~.L.2.L.....sx.}...~....$....yy.A.8;....|.%OV.a0xN... .9..C..t.z.,X....,..1Qj..p.E.y..ac`.<.e.c.aZW..B.jy....^]..+)..!...r.X:.O.. ..Y..j.^.8C.....n7R....p!|_.+..<...A.Wt.=. .sV..`.9O...CD./.s.\#.t#..s..Jeiu..B$.....8..(g..tJ....=,...r.d.].xqX4.....g. lF...Mn.y".W.R....K\..P.n._..7.....@pm.. Q....(#.....=.)...1..kC.`.....AP8.A..<....7S.L....S...^.R.).hqS...DK.6.j....u_.0.(4g.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....4E... ....q.QA.0.M<.&.^*aD.....,..]*....5.....\../ d.F>.V....._.J....".....wI..'..z...j..Ds....Z...[.....N<.d.?<....b..,...n.....;....YK.X..0..Z.....?...9.3.+9T.%.l...5.YK.E.V...aD.0...Y../e.7...c. .g....A..=.....+..u2..X.~....O....\=...&...U.e...?...z....$.)S..T...r.!?M..;.....r,QH.B <.(t..8s3..u[.N8gL.%...v....f...W.y...cz-.EQ.....c...o..n.....D*.....2.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.133203739571494
Encrypted:	false
SSDEEP:	6:kKX38pkQSN+SkQlPlEGYRMY9z+4KlDA3RUeSKyzkOt:P8phZkPlE99SNxAhUeSKO
MD5:	B3B1CE1160847D82C19C88A0E6B8252B
SHA1:	537E34EEF8707428559102A72FB411E7D89700A1
SHA-256:	9B25A0C010DF202A82F540D13FFD846EF8AFE8C11BAAD19294CD811D101218B6
SHA-512:	1ED24895D76D1930FACB54ABF3DDAC766B41C0A73196CE73B0DAE9308E557F539A1349827E37BA9447F8C95C8613070414F54525FD359CD50C2DC6CCD3EC64
Malicious:	false
Reputation:	low
Preview:	p..... .....y3..G..(..... .....Y5.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.f.8.8.3.5.9.3.5.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\06c02a36-1839-4a1a-b970-4ffd4da3ea9d.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):	359932
Entropy (8bit):	6.015428432254282
Encrypted:	false
SSDEEP:	6144:KWIBpnU7clv6AY88Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB6:dI3m6dxzurRDn9nfNxF4ijZVtilB6
MD5:	9CA082A77A4694B7844D19E6F104220D
SHA1:	DD8A403D64E1DE44100814AA97FB511FB74D2A80
SHA-256:	3D46F788979DDD497A74354014904BBEB76ADB74861F12BE4C2537BAC155BDF8
SHA-512:	B98A646704F8C29117289DE8B1EC2D090E1EDC9F70C58A84A0B30EF5F67F4FDF9DAAB92D968E89DDDB1DD07D3F056E4ADBA848C74E88EE48A64DCDBCDA092C0
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":1.620874811585009e+12,"network":1.620842413e+12,"ticks":109568154.0,"uncertainty":4733278.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjBylY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13265348408167

C:\Users\user\AppData\Local\Google\Chrome\User Data\1d426e24-3586-4a15-929c-f6acd16a088c.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):	359933
Entropy (8bit):	6.015429298239138
Encrypted:	false
SSDEEP:	6144:HWIBpnU7clv6AY88Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB6:2I3m6dxzurRDn9nfNxF4ijZVtilB6
MD5:	5DCDDCD9B61EC67676691BE566053E2E
SHA1:	9E2A4CD770D418503E35379EF8ED78A3CA292FCB
SHA-256:	2C5769B638ABFB68ABE258A57B00231D6B54E5DEF143C1221B6F5A07350BB192
SHA-512:	4C0D640902F5F9F6E8D0BBEC39B86634C8163A10D8F9A08CA290469C79908121B8F7EEF7378E601189AB1DF5C93D8D909657F6FB551576004FE81A2C684D45A3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\1d426e24-3586-4a15-929c-f6acd16a088c.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620874811585009e+12,"network":1.620842413e+12,"ticks":109568154.0,"uncertainty":4733278.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075352167"},"policy":{"last_statistics_update":"13265348408167

C:\Users\user\AppData\Local\Google\Chrome\User Data\265becc4-aec1-4dbd-bf23-8bb30481749a.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):	359933
Entropy (8bit):	6.015429294115941
Encrypted:	false
SSDEEP:	6144:vWIBpnU7clv6AY88Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB6:OI3m6dxzurRDn9nfNxF4ijZVtilB6
MD5:	FB7E77E54E7C271CAF183333C12C6628
SHA1:	CBE2377EE462BA7D86D1F4D5F5983E4E1E50AB28
SHA-256:	CCDA338CE93428C458E270CAF6F55F8755CB04B2A334DA293DA26DD90823A94B
SHA-512:	85523DB6FAD4A50D71811C464B2A29DA439FAB174F8ED88603E70E5B522B375FE01929777A5D93025E7665045E25E2F173FF39DFBBDC9EE6571E4B2AA776DFC
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":1.620874811585009e+12,"network":1.620842413e+12,"ticks":109568154.0,"uncertainty":4733278.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13265348408167

C:\Users\user\AppData\Local\Google\Chrome\User Data\288326df-9d33-4baa-a11d-caa5cae2000d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7492139986403332
Encrypted:	false
SSDEEP:	384:tb07Dh+g1KR9VKAHCNnrkvTZ30zRgH5QGoHryNXTxktNpsr2rmWC8O5HH/AON1PB:teKl9Kd8lUeL7NdInHOpKL53RH
MD5:	2BE6EEFC3634E4535794CB2BD61E35A3
SHA1:	565A4BD3AB02F814D9F9DFE58CC97ED948ED9647
SHA-256:	A181F6448BE34DC2F2EA4DEE58AE1E53995E1BF934DB65B724033CF5F09CD14E
SHA-512:	E3DF3594A33139D24E2963648285A717726A9D46D3CD5051528467D0E4BBAFB12B109185447508CCA244A5065D361BC2D05A47B1AD1A7F63F14B71AA5E3A4FE0
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.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\386175ce-f032-408c-9f21-83bf7335674d.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):	363512
Entropy (8bit):	6.028041943759616
Encrypted:	false
SSDEEP:	6144:nWIBpnU7clv6AY88Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB6:WI3m6dxzurRDn9nfNxF4ijZVtilB6
MD5:	CEFB65687495F8670EA3D4254A4D33C8
SHA1:	8CDE4604E207D86D8D322EC4952C278BB6DFBEE2
SHA-256:	9AE69754406046D014F83B37D913A73B5EFE3C5E4B22C6939F3F96524AE214C1
SHA-512:	1A0AE7C026F1AB1877688692ADB9D02C208F5446BB1464EB7C788139BB60FE25823ED36B53A3254F6DC0511DC7EB304436ADB91B96DD017E5491F31538CC3B3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\386175ce-f032-408c-9f21-83bf7335674d.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620874811585009e+12,"network":1.620842413e+12,"ticks":109568154.0,"uncertainty":4733278.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075352167"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5ccfba2a-1d39-4eb3-b9bd-7a0291c9417d.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):	359932
Entropy (8bit):	6.015429286603703
Encrypted:	false
SSDEEP:	6144:PWIBpnU7clv6AY88Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB6:uI3m6dxzurRDn9nfNxF4ijZVtilB6
MD5:	DD15EB52FEB92CAF5A53DBE4D3FED006
SHA1:	B58559BFDF79403F181041645E2FB95DBD0F2A74
SHA-256:	C4526EA5E8A0468182E5FECF98224C596D19154B1D23516FAC5974C23598CFA2
SHA-512:	56490839F7C1C49C16F42D0F5F31E7A8E0BCCCF2E9EC458724C633FA63015CEF163E954F7ED2FC1D1CB4AEC2D53C1D6656C857BA64960E9CD09FC3BC7203B1C
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":1.620874811585009e+12,"network":1.620842413e+12,"ticks":109568154.0,"uncertainty":4733278.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13265348408167

C:\Users\user\AppData\Local\Google\Chrome\User Data\80e8bc76-70e8-4886-9c8d-c3a344706d12.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7493575338720997
Encrypted:	false
SSDEEP:	384:9b07Dh+g1KR9VKAHCNnrkvTZ30zRgH5QGoHryNXTxktNpsr2rmWhO5HH/AON1PNN:deKl9KdQIUeL7NdInHOpKL53R5
MD5:	2FFE7D2A910FE4FDDFBFAD0D48DD774B
SHA1:	2EE89EE548175995B85A1BE25B02D354E504F787
SHA-256:	EF19A6A688BE250CE5AB59EF8380A069E2FD5742B9C7E8A760F3B71CAFE64687
SHA-512:	8CF04C123B7491DC17108A3163A56198281DB3D57E6183B3B200277FB36F036D6754E22725CE5CAA4816B0D9BE59A75C3AF401B63EC3433C9F392E8CCF047041
Malicious:	false
Reputation:	low
Preview:	.q.....*...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....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\15524c53-5e86-4c32-a25a-68c9800a64af.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):	2041
Entropy (8bit):	5.589666377765566
Encrypted:	false
SSDEEP:	48:Y1wEU9qeU7ieUr6UUhKUSDKUeVi3eU/kUEUL4UZUeC6wUe6Ueh:kwEUQeU7ieUuUU4USDKUCmeUsfUcUZUM
MD5:	A4862F024DA04A47B54097F4F07D1C88
SHA1:	8DDF3AC0451E2D32BB87CF612AEAE19931802C9B
SHA-256:	09216D2C7EBF6E043887050FEF17C9454A7435CB0EAFD3865DD60E657E26EA0D
SHA-512:	0ED68C454DFF2099311E22098DF5728A8D59F2097F1114F1B9F3CF5E2745B6677B4EE62CB9114E6A78A74054A6D25E5B0C41610E9A3C1A3C96A95233AC3087AC
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1636599647.394073,"host":"Hv7xd3BXVfmdXRm4r4ZaqY31b8zjFN6lIWHeulujc8Y=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874847.394079},{"expiry":1631761246.635135,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874846.635142},{"expiry":1652410846.358574,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874846.35858},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1631761245.740747,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874845.740752},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1c24fcfa-604d-4fc3-864f-5c11f58df60b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\259d92e8-726c-455c-b6f1-ffcb0b3dc601.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):	5694
Entropy (8bit):	5.1836216886030675
Encrypted:	false
SSDEEP:	96:nIrYGQ2Yhfj+SVAqIk0JCKL8+k411ybOTQVuwn:nIra2Yt+S7C4K5k44
MD5:	A8ABBB7B79FF73B895D4EC8A26511DF7
SHA1:	DD909DDD1A863EC0F2FDA39B688E710B67CCA271
SHA-256:	321775199FCB90D133DB7167D7EEDE5C1643E6ED3A336798058228C8A1B60506
SHA-512:	F66F62154F1B2FCEAE2DC91AE9528C242BF92294AD25DEF4F227EF4911314CBDED56F01668F67BE057195A028FC57B5008709C0B02EC7139BF4DC5A6CEEE464 B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265348408497219","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\264bd94f-c9e2-409f-8aa1-f35ee7bae24b.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):	3212
Entropy (8bit):	5.594017326628841

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\264bd94f-c9e2-409f-8aa1-f35ee7bae24b.tmp	
Encrypted:	false
SSDEEP:	96:eUgwEUFLUW6eUfieUK2UUWgUcyUpUSDKUl0nUtlmeUFUZfUcUZUH6URyUrUc:eUgwEUFLU1eURUZUULUBUpUSDKUluUWc
MD5:	16549442F65A69D471F7D1CF297DBE01
SHA1:	15B186B772813C1101E8585FEEB618FE98FEFDCE
SHA-256:	BBE83FE506427374A339B8553F39A07F05E8B27F301A8DB4887F31E3AD9EE916
SHA-512:	E61EAED551054FF23D8F81FC4A2217F1B5EB922F4EC50260329D1BF60A5394357581DF10AAEC79F520C7D8C9000A97E810E8E86083F66FB9DF3079EEEDE7072
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1652410899.10554,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620874899.105546},{"expiry":1636599647.394073,"host":"Hv7xd3BXVfmdXRm4r4ZaqY31b8zjFN6IlWHeulujc8Y=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874847.394079},{"expiry":1652410893.825469,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620874893.825475},{"expiry":1631761246.635135,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874846.635142},{"expiry":1652410876.108116,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874876.108123},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\46c3a4c9-95b7-478a-9d70-a978150a0007.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.536355040714966
Encrypted:	false
SSDEEP:	384:/A5tSLlHjXz1kXqKf/pUZNCgVLH2HfDZrUxHG6nTT3gL4G1:vLlLz1kXqKf/pUZNCgVLH2Hf9rUlG6n0
MD5:	EC60666BC0FC72322A27A181D3921DD2
SHA1:	047B4DB6F2F1200627B967FF53BBE92DC2EEBE16
SHA-256:	86006C8E0A7457BCF8869084A6722FB8C6DDB118044A7C7A3706DA0B4F4098C2
SHA-512:	D094713E3087BF574F22058B629FB3348D9DD5F62A41DD5AD09236EBDB6922BF576E3B1429ABC3EA9AFC98FE21E5F9F54F4D4B0704CDC4C1BB38FB2F621B79 B
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13265348408248338","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\58ab6243-9284-4a80-a9cb-d61a7ce0b377.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):	5049
Entropy (8bit):	4.969914456084576
Encrypted:	false
SSDEEP:	96:nIrdoG2pSVAHIk0JCKL8+k411ybOTQVuwn:nIrl2pSAC4K5k44
MD5:	6F9F698012F22B439A11E54080D98B17
SHA1:	EA6B69B9C2C4556287868AD5D99F72D8EC2ACE4A
SHA-256:	A1E65216D82D59964A028B5D93EE83A4853467CE6EF41971BF7C2E2EB6C33548
SHA-512:	1D17B3C3647A4EC866DEA45AA8017AC3C0E44776D7BF8F908C374C0CB9D826126CB7C8926AEF9A532D73F34CB7ECF0B6B997BA6D584E305BEBCCF81E8E01E BC
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265348408497219","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\60c473eb-1f81-4553-8469-0e85a6307595.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):	2042
Entropy (8bit):	5.586964157228397
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\60c473eb-1f81-4553-8469-0e85a6307595.tmp	
SSDEEP:	48:Y1wEU9qeUfieUKPL6UUhKUSDKUeVi3eU/kUEUL4UZUeC6wUe6Ueh:kwEUQeUfieUK2UU4USDKUCmeUsfUcUZL
MD5:	280E306352386600ABE474A816987625
SHA1:	CF60F93DB63492F525BEBA8D8BE46E487378981F
SHA-256:	E9C21FC96D7370BC558D64409E2C723344D04C0FF25764868E371516F8FA34A5
SHA-512:	748CDB3A0AE1454E9557DD6EA495797F72C3B3D33CB2D7D771BC89769DB424C88B0B14D97540EF6932974288003DE79C396DF91127B4138E6D55761CCD1AE3C
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1636599647.394073,"host":"Hv7xd3BXVfmdXRm4r4ZaqY31b8zjFN6lIWHeulujc8Y=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874847.394079},{"expiry":1631761246.635135,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874846.635142},{"expiry":1652410876.108116,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874876.108123},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1631761245.740747,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874845.740752},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6135cebd-b086-4ae5-8b45-0a892ac95ce0.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):	3214
Entropy (8bit):	5.593610292571949
Encrypted:	false
SSDEEP:	96:yU/wEUFLUW6eUfieUK2UUWgUcyUpUSDKUl0nUtlmeUnUGfUcUZUH6URyUrUc:yU/wEUFLU1eURUZUULUBUpUSDKUluUWT
MD5:	DC1411DF8304736414FC691C95C1DE12
SHA1:	7D677A756E6AFAC8F56631248EA61FEFC1124FDF
SHA-256:	175B0972EE1A45E92F9B42814869D6AA3B240105F3369B62FF6081D93FFD5A17
SHA-512:	2904829536D49DFAAD52B40A361B2EA96E1E43455C836662137DD8031E0DF161B26EBA2C93781EDECB4A02C0FBAEF22ABB43C23DA6407972E515D59A7FC5C18
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1652410903.169397,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620874903.169402},{"expiry":1636599647.394073,"host":"Hv7xd3BXVfmdXRm4r4ZaqY31b8zjFN6lIWHeulujc8Y=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874847.394079},{"expiry":1652410893.825469,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620874893.825475},{"expiry":1631761246.635135,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874846.635142},{"expiry":1652410876.108116,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620874876.108123},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\644b8a4e-6b90-4cbf-93bc-13b02bec21c6.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):	5694
Entropy (8bit):	5.183516529492049
Encrypted:	false
SSDEEP:	96:nIrdGQ2Yhfj+SVA/Ik0JCKL8+k411ybOTQVuwn:nIrh2Yt+S+C4K5k44
MD5:	4239E57A214CE452453BF9ABA709B2EF
SHA1:	8882EFA3ACDCC8B39368AA3ABE07A7677A50094E
SHA-256:	5A89C17E6AD0C823D9FEB0630543DE1C5DC579FA9648B4356C7B5DFA188CD059
SHA-512:	A5297C131067A637515F5895B3361702136071C0F392C6786F2B3A241FE9B9A9FEA11B12E65255D35F9BC75E41733ADFAA291DF93E7CF12D28E25DDBE109B362
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265348408497219","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\69ecee30-51de-4685-91fb-0ff05952b257.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\69ecee30-51de-4685-91fb-0ff05952b257.tmp

MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low

Preview:

{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7429e4c4-0d09-406f-806a-75f75910b77b.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):	5694
Entropy (8bit):	5.183578893485071
Encrypted:	false
SSDEEP:	96:nIrdGQ2Yhfj+SVAdIk0JCKL8+k411ybOTQVuwn:nIrh2Yt+SUC4K5k44
MD5:	B65DBA582FC7AF8D3021D51C72326C3F
SHA1:	08AF22CBCDA4AB91D91DB326F7922CB5FCB1B582
SHA-256:	FA149C7436F5D159C10686560066BE8A7D592954B4EEA3F32A8C68F049FAD5F1
SHA-512:	BDF4520FF052069588AC1E0333351002EF4212D9984747F504BDBB84362CA92F76C4D96179480FC67721F131757FCF1B85E946160B49AB6795E439953E0DA77B
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13265348408497219","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8a30a2d3-86b9-4996-be23-3bd8ea721640.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):	5784
Entropy (8bit):	5.185842138728123
Encrypted:	false
SSDEEP:	96:nIrYtQ2Yhfj+SVAqIk0JCKL8+k4113bOTQVuwn:nIr32Yt+S7C4K5k4j
MD5:	B911A62ACBF30B4545BF8BABBE885859
SHA1:	64DC8D988B4D56760D403DCF7C45BB0BB4FE7C8F
SHA-256:	A98E54EEAACC7ED0F4834C99933153509336F59BD8C2EE79FF63954D491506EE
SHA-512:	753A55B1332F7B308DD3C871F472A1460347802B283EC8DCEAFB81C75ABDBC0202111F8A7969C2D7A706D11DF43600CC52C08CF2D89743D857898AD1D6AE41
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13265348408497219","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.166718191181684
Encrypted:	false
SSDEEP:	6:mXCIq2P923iKKdK9RXXTZIFUtp8vuGZmwP8pPzkwO923iKKdK9RXX5LJ:sCIv45Kk7XT2FUtp8WG/P8pPz5L5Kk73
MD5:	CA2221B8B46761861D66A31375A9ED0C
SHA1:	4D1453C1FAAC5D9A6F6D56BB4EE8C1CF7E41A2EB
SHA-256:	5BDCE85AC41803334D74379B95C50A9D8E1A99808BB822B681998B467EC2E2B8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
SHA-512:	1C432032EEF0CADA07C59A73551D64E29D49ADC1F02A4E0284710A547DF99B509F8C42D2CBE82552B0F322D0A4AF33F5D7C3E9735118F54003F46B463EBCB32
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:00:27.177 1924 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/12-20:00:27.183 1924 Recovering log #3.2021/05/12-20:00:27.185 1924 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):	320
Entropy (8bit):	5.152821764224681
Encrypted:	false
SSDEEP:	6:mX4Kq2P923iKKdKyDZIFUtp8q5ZZmwP8/kwO923iKKdKyJLJ:s5v45Kk02FUtp8q5Z/P8/5L5KkWJ
MD5:	8D4E0A6A0D04FFB9CB467D4DC7DA972E
SHA1:	23338BD371234B0A47FD062E12406157E4E0F05A
SHA-256:	B748821F5ACA8362833ABD73BED311033449CBCEB5D8A6266A43DCC219EA4ED5
SHA-512:	D41B74582C403B934BEC4C3337571019204624C2C88E39ABD93C310DB0CD230AD38C94539654F4A4962A92901BB042A154D4EA642B2002F692CCAFC3E09B2F6
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:00:27.153 1924 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/12-20:00:27.155 1924 Recovering log #3.2021/05/12-20:00:27.158 1924 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\001faf4862a1d632_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.4798310113227355
Encrypted:	false
SSDEEP:	3:m+lQRgla8RzYrSLLiMZJXMLHSm9ocQVoo9RKv1lHCJf+KXwAUbiC/6I/z4mbwPpD:mMXYGL+MHMm5Vx9RK6JfgFiCzbSK6t
MD5:	BF3F9FCD4A538FD8450B5D7EC8ED4F32
SHA1:	659FD1812E962395ECDDE58A7C33104C1BE926B0
SHA-256:	C454FF90A562E531C12B0AA39A7455FBD8D618572184959ECDED16FECC1006CF
SHA-512:	965AEA102CC5651D5B73219EEC349061C99FD62DD03CF39E67C4FAD194969EE0B987049BB33D6233C382CE81E121E71916453AE0032E4878AFBDB0896C2AEE8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...bT.\...._keyhttps://www.google-analytics.com/plugins/ua/linkid.js .https://nimbusweb.me/.&.. /.....T.....@...A.&..gf.e1M&..@.@..W9.3..-.A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\08aa05d82acac63a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	456
Entropy (8bit):	5.83779706875718
Encrypted:	false
SSDEEP:	6:mUPYGL+MIwJJeVxotclQ4v6K6tWUPYGL+MIwJJeVxokeC0Fnibkg64THKQ4vJ6ZD:dLIwvcxdl2fLIwvcxzetFnibRfTHK3q
MD5:	5F4DC96490C59784EA0B8F82F87D5050
SHA1:	B1C112BE1B3207957962D59A5EA659EA976D3D98
SHA-256:	5A938BD1871B6588814DEEE91C24A5D67D089459EE675CB1770972C22251381C
SHA-512:	5548D6CEB9BC7C28931D8285BB2ECB600429ABFEE421A81EBC10798E42FF011C74528D8C511764AE1D1354607A560E1EC0576F94DA93A78FDFF5BDCE13FF042
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...dY]...._keyhttps://www.google-analytics.com/analytics.js .https://nimbusweb.me/.... /.....H.1...t.w.....vT.l|S.._.....A..Eo.....~..Q.....A..Eo.....0\r..m.....H...dY]...._keyhttps://www.google-analytics.com/analytics.js .https://nimbusweb.me/.... /..E..D88A0EFFE9E39945D325B09C5990050059784F323EB44B8D94ABE3C5976EB411....H.1...t.w.....vT.l|S.._.....A..Eo.....q,.'L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0923bdddba973bdf_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\0923bdddba973bdf_0	
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.536884343729466
Encrypted:	false
SSDEEP:	6:mq69Yj018IrAnHQ2xMtuZ/b9HlcW5K6t:hm1tkHQ4bZl5
MD5:	D0D81558589991544F3203520F2C3E29
SHA1:	0CE0035E8805E46F07F331FF747189AE933FB226
SHA-256:	3BA7BEEE812871C8F97306FA04FED2B07D95B38BC367B233ADB2FD54BA135BC1
SHA-512:	1E50EF5A50771D279884013BF3A275CCC48E4846430AB4BF02C00C9FCD09D0B1CAE94D6CE4509C20384A58723AA7EAD8783F84559F52225B4DA3CCD2B3DB97 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...j..;...._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.LottieWeb.cdd0d3d5.js .https://twitter.com/..... /.....Pv.....K..#c....0e....u.q..+.. G....A..Eo.....wr.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\094f0fe38a98afbe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.594780056777972
Encrypted:	false
SSDEEP:	6:my/XYk+f2pomXn/hmJ2mpAMLMsB4yK6t:z++amX/kJZdRn
MD5:	0BA9D447A1AB173FBD1F307C6FC6F02B
SHA1:	0F8244348832F0B998F06E952ECA24E6FFFDCF6A
SHA-256:	515719E957EF3A7497743E78FF07A521DBE22EB1A0A56A23D40A8599A79C3273
SHA-512:	25829AD575DB7BDBDD5F39AD017F9C5C2E9D8CCAA9DEABD505987111C83C0489EAE7A91E9A51546D6339EAB5EFD6D1764843C9134D57A9D4EAF009F2DD511 67
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...2....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y3/r/I2HpdY4t2HZ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....K.....ZA.Bcf.....\{Z.I]N....A.. Eo.....1z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0e0cbc38fb041bb9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.711249305447255
Encrypted:	false
SSDEEP:	6:m0Yk+f2pommAQyDzhmJ22vTU/AXwhiNJLrzlK6t:t++amm+DzkJ7vnU2n/
MD5:	1F33D603B34ADE0D857E23AE05E57AF6
SHA1:	906D0FFB47A4184CFF4C0219ED88C7710619F099
SHA-256:	E19A24B997CEAA569776D4AD579AAAFCBF7103E694B6AD769ADE79A041CC7258
SHA-512:	5310B037E3F792AACB354089F5ADBB7E862EF6B2F8EFE61B504CF767610B7E60AFD9CD7BB17EAEDDDFA0A7A15FE7F4042BC712635D8F2988DC76012C189B5B F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....y....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/ym/r/FmXSR41lxW_.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....H.....J(.....z.....@P..b. .g.L...A..Eo.....P6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0e0fdbb11eb5ee0a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.5342716741032545
Encrypted:	false
SSDEEP:	6:mjYj018IrAE7uPzy7aMzV8y3z8REITElbK6t:e1tnuPzy7Z8M
MD5:	4E6788F4942162602631E62F00DBD187
SHA1:	129B5B7AC58FC895F4CB9DF96E5ACE61FD8B2B04
SHA-256:	A758B62FE5029073B6ED0A5FD3E6A5E878D4B7C57DF31591ACC925D5C0D22997
SHA-512:	1EF9932DCF709F933D392429F90F1F90A151D6634F8A615F1E07313F523D0EF45B6071B63F274D61CDF0C51B059484A55FC7DFDC5E03D7F4CA912516D6CA5298
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0e0fdbb11eb5ee0a_0	
Reputation:	low
Preview:	0\r..m.....j....<....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.AbsolutePower.0355ab85.js .https://twitter.com/..}.. /.....3e.....H.....Q.l....4....r..?..h...A. .Eo.....]..........A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\100a6726e277a519_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.668453031133534
Encrypted:	false
SSDEEP:	6:m2Yk+f2pom9ayRSdwhmJ2qJdmX4sch84xlhK6t:v++am9jkJ6XrU8Ul7
MD5:	520DF3E92A138C6C282507C721AD3A61
SHA1:	029CA6A4A14577F59338C6C893E9C2D12DF90E9A
SHA-256:	7CFEDE8661DD8A780E15EBFE0B6FE24C144D702803AB29F260878E81ED8F35BB
SHA-512:	3AB95CFBC87C4388865AA0019EE27229672CA6C8ABDFD045A11ADC03E914A5385C28890F569DB3B42BDEBD4AE4EF4543D91493A32E497C00E4801CF8389A587 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...h.-....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yu/r/dFoJueKLziG.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.Y... /.....K.....)...1.4>e...t...7.p-tU.._ .5..''..A..Eo.....S.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\102f3a9cb2c0e4fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.7773289869637106
Encrypted:	false
SSDEEP:	6:mqsYk+f2pomW16gkhmJ2oIyN//MkrdgWDzzr0tbK6t:Ds++amM3kkJCeXMgd5Pz0
MD5:	DC4C1C4015B3194DAE13808667501708
SHA1:	F5B66B4DB724FF6547C5E800B781926DE2376CBD
SHA-256:	B7976D9AAC5D1E21714964AE69D6C325143EFB9C6F62E023E9C51F9F83F2BEB5
SHA-512:	22BD84953F635D04BB71C439E1B4424A394398D5D4D33B37F97343CE441893EDEC63C24352E77B7042D078E34EC2D06689EB08103B1375F22574FF9C6261B543
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...f....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i1Fx4/yY/l/en_US/hdv0r8gSN8u.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.... /.....(J.....W|+j..6....9.. .~..:]_.x5W..N.A..Eo.....(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\10438f4122c99db4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.74880517498955
Encrypted:	false
SSDEEP:	6:m4/XYk+f2pomW1SCtbYhmJ2S1Z4YrLe14rK6t:hb++amyBKkJDRq6
MD5:	590CEFC87A7553A5297EB98DB035AFD9
SHA1:	4082E7A0D062E506E854E99E6EA1C0B3A0150414
SHA-256:	D0A3D0FBFA4A27B3ED4A123C2C481FAA5A32AF47488B3BE8DACD1636CC129AA2
SHA-512:	E4C33896B0E43FA98C99DA90C46953C61359647DD980137C4547B10784BF0C1CEC482109F55639E456B726F7AAA8E0E3110ACCCE6E9B098189503803CD02ED0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....@c....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iPwL4/yd/l/en_US/d-YpByGjyvG.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....I.....q.IE?i%...e 4Z.*.....FR.t.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1228880b86b3fe9c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.741513914757168
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1228880b86b3fe9c_0	
SSDEEP:	6:md6EYk+f2pom7VXGhmJ2AGM1kwc9ygrTehK6t:7U++am7QkJPKyg/e7
MD5:	B4E30FCFCF7CC86C96E120532CAE92B6
SHA1:	01989C0BCE8063888A330BACEA235DDA3AD4604B
SHA-256:	9EFCCA827286EAEC7BD5E0A7E2CECAE2D23EB36B84837036DCCDECB3DED227A3
SHA-512:	DB454F2C5D112CB6F7A57385120E55211D29C0CF04C388B19E4A10A12666816E71DA5F4DE275D78DF6CC8EBB222DCB22A7E087B241125793401C51F738D2E59
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y_/r/5IVvs5UXPZj.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/Cz... /.....K.....x...J...D...N..]....C.. .%e....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\165ae26eb3f7eb15_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.684039179971688
Encrypted:	false
SSDEEP:	6:mBYYk+f2pomWpG+wbQyhmJ2P2uMpi0grE/lhK6t:j++amuGQykJaVZQ/N
MD5:	9E17711A72D7F226D0EA18CA0277F978
SHA1:	49D919EF7797BDA5621D5D0D8311050F864FC2FF
SHA-256:	C3C58D6DC75C83AB8DC69830D0A467EDBF72DB862B18C360FC480A623A804E1A
SHA-512:	89A54B76F11FBC9F58736D8BA6B7E5C736F79FB5B5FEE0A2C73989CA3F56BF154A294E1B68E359AFF008C4B583A311579EF543800731384D579113A381E94FAC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....e...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iLl54/yK/l/en_US/xEIrl5YaCtN.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.~... /.....l.....y.k...f.l.v. .W...Z.8`.l..-D...A..Eo.....[.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\16db1b33a5becb53_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.6006277765630506
Encrypted:	false
SSDEEP:	6:mUyl/VYGLSmXZCshmVxcv6GCnqryheh+4bjK6t:kl9DmxsknqeeP
MD5:	0160B2FDAB0EB523D4F7FC76F0FB413C
SHA1:	A51F4E651BD407B67F89724B96AF2F8857A2697D
SHA-256:	A237A4C397937C043C79788E44E574188B3E774381D2E03FEDA2290CBAE35CCE
SHA-512:	9B0928661ED916C53FA3E6AC5648A1A935DC40B032E3BB6EA29776B611D3953729A0F9A07A29A4A53C747E7A61466FE37F123ADF1F4AB38EB62B18B8FE94D3AB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-67774717-30 .https://nimbusweb.me/.9.. /.....Y.....?.....EW`.s...W".z..vc.rI-..H.A..Eo.....[.3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\170e5fa419535e99_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	198
Entropy (8bit):	5.3723455090438
Encrypted:	false
SSDEEP:	3:m+lydE/lA8RzY3QVoFKdeGFVRcQVocR1lHCl1CQaUcDPKaK5mlW///pK5kt:mg/XYgVQGFVvVml1CDPKB4g//hK6t
MD5:	E9B0139B949E07AD82D5904CDD0CA8BE
SHA1:	620D8076731B3764AE4E8EB78B41E11BB947618B
SHA-256:	B4874FDE84E6BAD444D7409DA1AB27DAA0CE6946FDD0EA349568F9ABA8814B02
SHA-512:	2AA1561EF434900050F6A92D4FAC0FD7E0DF036989F3FF48380DFF59B2A25E74261324978A86235D88ED2B2263BBFF6DB630C4B5C4ABF997F322CF73CF0699B1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B.....A...._keyhttps://nimbusweb.co/js/contact-form.js .https://nimbusweb.co/R.W.. /.....=.....w..."..54...-.h...)#.)oF..A..Eo.....Nb.k.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\173a532107de75b5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\173a532107de75b5_0	
File Type:	data
Category:	dropped
Size (bytes):	104432
Entropy (8bit):	5.794439732524701
Encrypted:	false
SSDEEP:	1536:7o1hux2ppZVe5fXoxsf5sJ28CbiuGgxx7B5PjBIxzlTNJOSj+qkqM:E18oKXysWJ28CbXxxTPjGpTTLj+Df
MD5:	8BCA7D9896AF1618C91B3F622AA5D27F
SHA1:	A988AB38E4AF948DE1A28BB2138110E4B888228A
SHA-256:	B5C5374980B42153E330627DE316152D92B8705426E917A1A9B3F35195D93FAF
SHA-512:	FD17E87989DD899F6ED1CF568AEBB0E3B041E28641609F5C90AD3E77698F875A4A872495B7141A30FECD62A4C094630B3FB98750BE63F6C9982897F47694DA07
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....k2,....67825DD6E44EC0BDD40C09F9BAF1077F5D169F641A3FA80B2BBA2C885C436E69.....'..v....O#.....L....&.....`.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....N.....Q.@R2~.....module....Qc."p.....exports...Qc..document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa....!...I.....@.-....0P.....!...https://nimbusweb.co/js/jquery.js...a.....D`....D`....D`.....]....`....&...&..!.&....&.(S....&..`8M.....L`@.....Rc.....8.....M...Qb.Ts.....c.....Qb2.3.....d.....Qb"*(%....e.....Qb:.....f.....Qb^a.@....h.....S...Qb.W.....j.....Qb.....k.....Qb..m....m.....Qb..j.....n.....Qb..be....o.....Qb.....p.....Qb.....q.....Qb.....r.....QbZ.s....t.....R....Qb.;.....v.....Qb:. d....w.....Qb.....x.....Qb.....y..

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):	5.482316890133055
Encrypted:	false
SSDEEP:	6:mwh0lXYGL+MIwJJwMKA1XSJilxhm4uK6t:dGIwvwCUDL
MD5:	FED80AE0A3C6E55821B9901FACDEE022
SHA1:	5386E7EBDCB627FB3D9297D695F421A70AA09709
SHA-256:	4C125DF38AFFF66CF0AD69A5BF0715C34585A125E923B1F6133C0D1662F1DE54
SHA-512:	E7E7051B58B127C8E875D41A2AF7E094B637553825417E3021C8B1D9E5F9166927A260EAFAC30D2D693F0C62B73FD855F2884A29396DC2FAED4C21AD1BEE493
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.....I....._keyhttps://www.google-analytics.com/analytics.js .https://twitter.com/H... /.....D~.....:.&..L...jC...1UR@u<$mz.B...u..A..Eo.....d.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17b3f5e4859efe7d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.7037983517192306
Encrypted:	false
SSDEEP:	3:m+lY/e8RzYkwLf3G9LomZKwMMzV2QufRJ2X7KlflHCjnXYZBTy2ObperPJUWmwFD:mVYk+f2pomZZhmJ2L1LYr4IJy+RK6t
MD5:	97AFFE5AEA4A59FF688B65354BCAC09A
SHA1:	A5F2DB5E07C89F511FD6F76EE74950B79CCE5F1E
SHA-256:	699FADE82FF2D811A1B9EBA27AD75813FEB648093A31F8E907C9E17996F2742E
SHA-512:	FC127FCC846E99B8808618D05D24C2E50B4CACD8993E44187DDA5BEAA66CFFD2D3DCB2719DD999CBCFA8F3DB475209910401B235E7E3272187A846D5D43178 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...Z....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y2/r/KOEzsVWPqCJ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/T.... /.....KI.....5.....d.9"H.....0J.L|K.+..:.,ut.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\186deedaf626762b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	293
Entropy (8bit):	5.637517244172508
Encrypted:	false
SSDEEP:	6:mSoYj018IrAMUJABIHy6JABIHLBRpMWF1VA6nC1I5IchK6t:Y1thULDLHHFfrnr5r7
MD5:	B6EA96BD1EDEA873158C2444DA290CA5
SHA1:	6FFBC1EC91773EC7C6D946E05C682B4A34B8B28C
SHA-256:	3B31A3FA360D64DDF937D5CE1BBEBF6E913569C3E6FC3CA7BF1CE7E92FA19F9A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\186deedaf626762b_0	
SHA-512:	D1F9C64AEB8E6F7F3A0D8CAC289B45EFAC0AD598489A9F61A0FBDE7523A734701D7E7F9C25F445268163E9B78E7A76A1D48F13C729D1AA8B91D5F7F6E5CD31F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~loaders.video.VideoPlayerDefaultUI~loaders.video.VideoPlayerEventsUI.41ff3ce5.js .https://twitter.com/.... /.....t.....>....3....\.\..T.O.Q..... .,.A..Eo....././.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1a2a4bc671e188c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.675548675373817
Encrypted:	false
SSDEEP:	6:mEgEYk+f2pomoXa4u5hmJ21QIy5vvFBlZK6t:PgU++amoXaLkJsy5vP1
MD5:	87F45AC2A2139C23A7AB1E3787D98411
SHA1:	ADD826AB43E495E0AD9CD5AF369362C6F5DE974B
SHA-256:	6B8812F990620C00064FF8446207C112E5BC02F52DFB687B7A17AC02B160BFF7
SHA-512:	BBEF4D3AE980D6F14109611EFBF49D7B17B0E03CD14B68BB25945BD624235473BD4BF89013C97F83BA04C46502861EC3B86E22B49C83E25AF43004A65EEB94EC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...I.{....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y5/r/2K03Q_U3zzt.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.... /.....kI.....}j...V*W..@....l..h.S.I4. ...d2[E.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1bac1f80b920e568_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.668509405395982
Encrypted:	false
SSDEEP:	6:msaYGLSmXZCe6fNvV24NFK6In/lk/q+Nkvl6P4gtbK6tWsaYGLSmXZCe6fNvVI6e:BkL6l92Wstk/FsYNLkL6l9I5/FsA1
MD5:	028D66A06914FD1EAFED056DD93BDA50
SHA1:	87B9335BF91AA70664A58178E0D0D1F741D3AC2E
SHA-256:	E5AD0041B6B3220A7819CA04B8947B9686896E1B3695DDCDF1A108EC33FB00CD
SHA-512:	E55CADEAB3C137E25633FF5D3B320A3CE50C83BC7E2D40B86748AF724A21F71F0CEEDB855C7CB591DD9EE27A0A2565E7F4BF97C23BB307C380CF451100DE4EFE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....!....._keyhttps://www.googletagmanager.com/gtag/js?id=G-0EDVBZYM88 .https://nimbusweb.co/)>9.. /.....cS.-.A....-.T...?.q..$.a..A..Eo..... .....A..Eo.....0\r..m.....S....!....._keyhttps://www.googletagmanager.com/gtag/js?id=G-0EDVBZYM88 .https://nimbusweb.co/h@... /.....2.....cS.-.A....-.T...?.q..$.a..A..Eo.....c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1e5e02b54cd08c1c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.796316662817528
Encrypted:	false
SSDEEP:	6:mb+llVYk+f2pomWnpTMmfrdQzhmJ2wE6yLnythK6t:Mab++amCdQzkJ5
MD5:	34D2C88CDD6995DC327E27EE3BBED762
SHA1:	973C202F6DFE013E8A50159D68818B34EC70AE22
SHA-256:	865ADDA88CC60E0682662EFA1B0C24775073C5605F9E3774B24AF23672B6B834
SHA-512:	C954EB040D01DF113B93610361F0C103FB14AA09F50840719281752CEB818E229B4A0AD7F37455E075AFAC897C9AB15D5E036A13D10B1D0FA6320515502B28FF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....L....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iBFV4/yV/l/en_US/1MLCN1f9jKS.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....K.....L...5.{.8.1A. .z...4Z.....m4....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2017e793a60273f5_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\2017e793a60273f5_0	
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.509238964762185
Encrypted:	false
SSDEEP:	6:mUVXXYj018IrAcNwPpM/y1TG7bnXZxhzrJK6t:pVXP1t+PTiThD
MD5:	EDF2CB047E7A5F75A0652DF9806D337E
SHA1:	DC3C8D68119527705D13A7873F3DE2AB6ED55526
SHA-256:	D88ADC1DF9B951FADC8A78D9907835A04BEE534F4ED46B20F9A4C6AEB2A4C2A4
SHA-512:	6AC510FF8756C1ABF49408936EB9183C763376B32E3338E9CA6789EF49291DA03D5179D82BC0720723965C245683A8D9FB41FB6B6616FD15FBB7A94A1ED9957E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k.....w....._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.InlinePlayer.4b7f25e5.js .https://twitter.com/L... /.....t.....x/.-|.gm\.....bm.b../M...]....<..A..Eo.....6..{.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\21285cbed62f3d53_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.72519520545792
Encrypted:	false
SSDEEP:	6:m8CK9Yk+f2pomeRyhmJ2MM8tOdXstxbK6t:Nl++amIykJZt06N
MD5:	54857713CBF43C93158FAFB4A193F27F
SHA1:	E0A1244A5D8BC5542C5880DCD3DCEC1F5B617CEC
SHA-256:	CBFA5B116AF2F5C67A90AA409D9226DCBC4773466E6D5C571514ABE2AC24070A
SHA-512:	DB3C2D40EB3B68939D199726113D0D80677D5C8FFC734306E488B8A2F0AF2C3DE9CE9FCE537FF88E56A2BD46D1057E2BDC9ED8E43711D8145DDCAD91CA666EA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yB/r/OYZvjrlUuNz.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....H.....V..j....m..J .l..m.+..^.5 YD..c..A..Eo.....u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\21417f20d3c865b2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.589652415565815
Encrypted:	false
SSDEEP:	6:maYk+f2pomDf9hmJ2eWF11El6h9ezAwK6t:D++amDf9kJTC/r2Q
MD5:	1C00E0CDEE15D1D6B54983665F6E67D3
SHA1:	D760C4DD173AB099A404EFF15CDFE01FAD3016AD
SHA-256:	7D0BAD05EDF6BBF8CE4B8B234ED1FBD2B98179A63EFF09060905CAECC2DA2D63
SHA-512:	AE331EC4412D7A95D5DC0A7D76218D19A3EDF332C5B84903BF66C23D89C8816BDC2707102152FC09546840F7C1A2EF466F6A981E34115663774DA8EE8FE6F54
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....Z....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yG/r/waPsvUpeZ_n.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....G.....|.S+..$2.EmG...I.I..i...S a.m..!3.A..Eo.....CY.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\21c18362b967ff60_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.7032954825171105
Encrypted:	false
SSDEEP:	6:mdnYk+f2pom7ShmJ2TyhEEOnndE4hTK6t:OD++am7SkJx4nndrD
MD5:	BC5CC69928CF6A0405967AE4374E24C1
SHA1:	A6D0D643B0FBCB9ABDC0396E2BFE3AC4BC5F1AE2
SHA-256:	8874FE75708CCB7DA143C48F5C016D6AAAE46F3C02FDF605C7B46B77DCC1DB2C
SHA-512:	5C8B1ACDBB3C80FB36E58FE65DBC232EDF5480224F301D8D5F038531F06C64BB880800914566CD004C2AF0EB9EA343EF4790533AF167C10D5C7ED958620A539
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\21c18362b967ff60_0	
Preview:	0\r..m.....h...g....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y_/r/K9apq9Of1R0.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/0.... /.....G.....$.md.,^J....K9.B.....`..x...A..Eo.....A.T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\24f978eb7187aeab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	245
Entropy (8bit):	5.552188276998484
Encrypted:	false
SSDEEP:	6:mis9YgVxWKNpLaUSVxW0/nacH17IpK6t:+xWNxR/nZHBk
MD5:	8980CE822B757A3EDB07EFDC28698A2F
SHA1:	6E34D06678772012C5377CF7E91DDAFFCD77C79A
SHA-256:	8E340EA7BE69EB5CC9084415E6E156E9AD442E4C7A7B1178E18BE3259205370B
SHA-512:	467617F2AC29D39F472636E50C55483E419DB64573DE7B6FDD1162C0570A154C038443C087C1B35AE3B5351277B067C588FE5697A2CB79D3CA1D174EE430D936
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q.....^s...._keyhttps://nimbusweb.me/s/static/assets/ab9dc978a8521f1cda4e.vendors~syntax_codemirror.js .https://nimbusweb.me/.... /.....D).`/m9=.C...z.....o.r0zm$...;..A..Eo.....Rm4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\278dfbd662fe9288_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	5.560346188157901
Encrypted:	false
SSDEEP:	6:mP/PYK7RrnB4diXj1VxOiwxJg2k4KDK6t:izadmxugTN
MD5:	92BF251FD087143C59219A807071206E
SHA1:	B47EAF818D5B75CA7793FC9AB26234CB63B193DD
SHA-256:	93AC5CAFECD0FD8DC6F18FC5B1B263A0BD190CF611534D2811B323F1ECA98F41
SHA-512:	EF0DF94D9C6E964A7145BD826AF396AC411827476C97A3F5AC1FE71ED28C411D45FBDAF02CED81377F15056541DE27147C3ED1B935269D86274A7730F1D7C1E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n...e.\...._keyhttps://dojq4kt8ws9iq.cloudfront.net/s/dist/vendor/webcomponents-bundle.js?v=6.32.0 .https://nimbusweb.me/..... /.....o.....0.....5...S....9.n.Q<.....A..Eo.....d$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\28c363053db13803_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.780688120256478
Encrypted:	false
SSDEEP:	6:mInYk+f2pomUfgzhmJ2K72lgXhUs6Z9hP6thK6t:B++amUfqkJrmkus89F61
MD5:	D8F7A07CAD8DDB178DEA7348F850583A
SHA1:	312C2CA738D2FD9721ED4B0DCD9D81B53D3AD71B
SHA-256:	5BBF3560F3790BD2A7E8B13F52A1BB99B4406D8D893C832ED86625D33F215346
SHA-512:	2A4008E5E62D312638AD83E3205B98CDE14454C43818E22D8AEF442FD6E47823ACA50D671B1728D0823424CA920D6FDA986C8ABA518B7C84D4DCADE70F8392E4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....p*....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yO/r/Y-P0JSv6MwQ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/>.... /.....H.....+.j<.....7DZ.$.e.a.@*.MT.{..K.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a1087bad88acd5c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.727476653466426
Encrypted:	false
SSDEEP:	6:mJud9Yk+f2pomWovILahmJ2mKy2xTfMy4vK6t:xdl++amWmkJcxzC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a1087bad88acd5c_0	
MD5:	B69FC38A99C416CA8E119BEC11C88CC6
SHA1:	E6D459DB0D190281837BF024E96AE801FC92ACA9
SHA-256:	FDB93F84D889CEF1C16CC38AA212AB8AA205936798003EA6977C60565414EF38
SHA-512:	DFA387EC4CBD10B2D7644976DF7CADDEC0168B492472F07AEF10030B7ECD292E041274C7802FCA9135713CC5C9D3BE6F7B04A9AADC6FA3269AD34179E67971 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3itji4/yu/l/en_US/IsKrZKJOSEF.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/0.... /.....uI.....~I..... ..6[.%..z&-.UF%...A..Eo.....h.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\307cad7e2ff3c9a7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.675480826089907
Encrypted:	false
SSDEEP:	6:mNFYk+f2pomRloVhmJ2cUFyKyLigHDskAK6t:m++amRloVkJw0KRgq
MD5:	EF1CF035160FA8D4B6635BD0E0D54085
SHA1:	85549D93A3E7B4BAE41FD42A041D3E7932669342
SHA-256:	97C883C756B8EC399C73DA0681DE758FEB7CA655E10077C9A4879F1FA21AA08F
SHA-512:	446F79A3A0227945858D595E1836221C8DF5243FFAFEDCFABAE52E460B353454DD3C4D7615B3121FFDFA14D3373C1167D6A60E65B8443D4AB915AC9D5F454B7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...U.[@...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yA/r/rOuGauB8Oni.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/_`... /.....I.....!..)...''...gV.@h.B....F. }IEM...A..Eo.....}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\340933ba7ece0b7e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.737258514679918
Encrypted:	false
SSDEEP:	6:my7APYGLSmXZCeqawpCGNFV3fVxe39uWSevgr9K6t:sLqDpD9xet/w
MD5:	9689F97A7562B369FB9868FCF6F3060B
SHA1:	C851FCE4BAECE7D82AC1A6ACC36156F320673448
SHA-256:	AC512BFC9DF6ED63C4015077C75EA2D50C20E8E41DC66A5FDDB465B40F20A2C3
SHA-512:	A587D4206F14BA0DE496788A3DC91E148D0A626D8F5F24A2A52B9A0AE81666F169CD01F8BE2371989CE9998EF5509B132997AC902D7BE83224560E19B25B715A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...Q^<....._keyhttps://www.googletagmanager.com/gtag/js?id=G-7ZKFB3S0PN&l=dataLayer&cx=c .https://nimbusweb.me/{t.. /.....m.....+..K.1Tq..P.z$\N ...).s....f.A..Eo.....D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\380f88a78a7a4954_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.807470053514544
Encrypted:	false
SSDEEP:	6:mpgvSPYk+f2pomWiKt6SokdwhmJ2K1WXiMY2K6t:yb++amLKf+kJJWyMX
MD5:	E636A2CFCD2603BCA50B1533323EA68C
SHA1:	28E6DFFB4F68EB344901C380A1A26122D54DE5A2
SHA-256:	FA2519A45EB3F5A08587E714A032F1426EC269E6F4FF15068247A54AC6F95576
SHA-512:	C44F20B9B7875321E97A50BDA8B92CE81C970456B6EB95FE4137F02E8B2C78701CD24B47A77F7FDB0CD3171838E6ED7B8E3583C0D45A6977D5C01F9E0AA86EE 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....'...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iSUg4/y_/l/en_US/VkzJUAoZf1H.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/6.... /.....bK.....Q.&(.....3.v$;)..7.....G.F.87.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3adc98eb2d659960_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.692920986687845
Encrypted:	false
SSDEEP:	6:mHXYk+f2pomBMYUhmJ2WAvos+GllCMPvpK4t/ZK6t:az++amBGkJLJX/T
MD5:	7710CEDBFE902E76A2CAFB878029FFE1
SHA1:	243544DC597599D17D10009754E282E4ED549CA2
SHA-256:	FCB55D05CA5644AAAB396CFC742B3A2197EFAB841DA90045485AA151179213DF
SHA-512:	B13E6B9073D207BEE82D98D7681E99E5E94E13274DFF55A5EC4D1FBC87A1DCF829246780C72283E09B189CD8D46385B7C5868B3DBB584222529B9E12FA782DF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...a6Q(...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yj/r/-pT3XnketBZ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.h... /.....K.....Z.P....x.}.L-.?b)..-$).Mi .....A..Eo.....W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3c32d591c1ac9b0b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.529794338771203
Encrypted:	false
SSDEEP:	6:mKYGLKdXNQKH8KtWVxxa55zBiJR4XnrqDK6t:KhNQKH8Kt0x8BI
MD5:	5A962C1E5703DB24FAF0DA94B18D562C
SHA1:	EB0C11D91092C495F6C3458EC8281297270A404C
SHA-256:	CE02177C4E9A93C3959E9BC6DCA5FCF639AD535F4061A64F1F5FD9FE9F61E1CE
SHA-512:	8D30454769769648C9F1D96B412F456D66B7C7F62B7999B1921E276FF700AA06CD58715723943BA0A61DFE79AEEE83EB9ACABA1F27150018E2A7B6D6AD34AD9I
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://www.gstatic.com/recaptcha/releases/npGaewopg1UaB8CNtYfx-y1j/recaptcha__en.js .https://nimbusweb.me/[J... /.....#.....Q..TP{.V... <..e.....C.u....l...A..Eo...../Any.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3c3fbfdba30e0e9a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.764764602154959
Encrypted:	false
SSDEEP:	6:mNplXYk+f2pomWvrPmPg3zhmJ2cyIXTRmpgrr5/ZK6t:0++amlOkJ9DRsSp
MD5:	83C3B40925ECCC0EE46218DB6ED55A72
SHA1:	1B6799BA8520BBCCD2ADC1F7C000BE91A49C23C2
SHA-256:	E0438AB3FAF2F5C73AEE0E2BAB753F9602F1C787482EBCC9560511DA43849AA1
SHA-512:	43B8FD73FC5E5F29DA60995FFA01E7963D7C61969B31F818288843D08A4CBC5B4BA999AD4A7B9D415B80BE5EE009EE6678F9599F49F49ACB3FD783D8006CF33
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...i7%....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iJBN4/yi/l/en_US/1d9GRRVXiDO.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/3b... /.....tK.....I.| C^.m$3\n.{Bv....<SY..Z..R...A..Eo.....%.L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3fc7757f1402ccb7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.485498594137141
Encrypted:	false
SSDEEP:	6:mpillPYj018IrAqmWHkpMHLWbXEIvoyA/jl/bK6t:ei/n1tJHk+WTVHOBN
MD5:	CE006A19A683433FA417AE3C242D020D
SHA1:	D9D05CF62A8FE3265537863FE32A8E7A4A3867A7
SHA-256:	24DE2DFE57085B1AB2B3C92140F8B1DC9796AD567540C159D2B88BE3E67BFF0A
SHA-512:	925E6696B3D077F305D2AD2FAA59F426F31136C6A06C354062AE0BAEADEAA29A67E2126E218E64840CDD0474B4AA65279E7DAD39B73C27C65720B5E4A59F35C A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3fc7757f1402ccb7_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m...3..p...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.TimelineRenderer.ae3acb75.js .https://twitter.com/.Km.. /.....b.....s..[...(.m...J1.. .....&...ME.A..Eo.....ai.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4111559035a3e9f2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.781433032076786
Encrypted:	false
SSDEEP:	6:mnyzXYk+f2pomWMebcF5hmJ2tTCzAIpLcgK4HSK6t:wK++am1R5kJZ9lgI
MD5:	A5E9EEA68C9E42801B4CBEC5E11C3B21
SHA1:	57FA870ED5B95234EE160C1BEECE9283FCCD9A6D
SHA-256:	4954E584B08E2319B12E6CD0594EED77F093E9E1A8C9618C4E7637851A47788A
SHA-512:	393B829509CB7EFE4DDB92385DD626550E9A1003B7A0092369D3829BACDFA7614DBBAB7A76B8531442A266FCEF03733DFDA5B7964C3D32449355A2BE69B3B9F 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....k...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iaKm4/yT/l/en_US/y7DnIWCWj62.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.a... /.....J.....x...../#.. W....+..D.f..~....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41c9dd3e30ed8205_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.760706653620249
Encrypted:	false
SSDEEP:	6:mSYk+f2pomWvZ1KuhmJ2yJyXGkOq1mtZxK6t:H++amYrkJjJDqW
MD5:	00289396001F0A191D983A2A8B76A5E9
SHA1:	09C71D1C2B8242109F6CEF4E87AE21AFBCF33AE0
SHA-256:	4554B6FCD7F7F2E9D43F0CC993737823976E3A722D471E610DF405BF8665A6C7
SHA-512:	4F04234C66FC282C4652A24F5B61E00DF804C7F37D8ACDEB86615DDB4A7E01B227310383DF52BE1CFED9099794D3F3CEF8D3B3DA6365248C5729A82F932074F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s..../.a...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iJX14/yX/l/en_US/FGjX6fUT-lJ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.... /.....G.....Un.`.....A.j.b). <.6;..jL;....A..Eo.....v.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\429cba1a3cd71f0c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.538772381689739
Encrypted:	false
SSDEEP:	6:mOk/6EYj018IrAE8v4MSzyXWav/mzbK6t:7kyw1tgwgv+zN
MD5:	2DF252937018D9C2360A6A5C136AE573
SHA1:	53BA505E76965EF79E98648F6EA9759F474F1139
SHA-256:	C35719FBFD884CCF46DC8E46D531FEB296CEB8AD307D9D5C8D4E0E90D21C8F00
SHA-512:	D395031E37491544F3D89F3BB4EEB2739CD5FD06A6A3281C906C3390EC16E628EE2906667C587B8A544131363A49E6D6353685AA2B1D6F2E07543CC0A5BFDD21
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...8....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.AppModules.ddab5b15.js .https://twitter.com/..Y.. /.....[.....4..x..c.....V.y.....+..;? mB..A..Eo.....$-.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\43181d6f6b7a29c1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.544295513487706

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\43181d6f6b7a29c1_0	
Encrypted:	false
SSDEEP:	6:mAus9Yj018IrA6/PE0RpMGQAL/w7rsXfk41K6t:11tDM0RfI7rs8U
MD5:	BA38996BC33E3B7029D5262A3334D10B
SHA1:	AAE42418CD7F1E9FD8694D1CA8825424D4CCA7C7
SHA-256:	B620E94EE7C1BAFF9D496CBD4A5DFB3E761FEBCA39689A9E2C204A8EDD4B4C5A
SHA-512:	CA9E71CF78D858D26DE9293FF189D4F55830763349092EC1C6778FCD16B28447422B0A555539B46556B87810ABE960BCB76FD0D37F295C6F20E3223A4D09905B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...u....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.Typeahead.8ef37475.js .https://twitter.com/m.... /.....x.....A.6.t..T..#....7...wK.. ....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\463c71b300254578_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.7115927537884374
Encrypted:	false
SSDEEP:	3:m+lYhalyOA8RzYkwLf3G9Lom15vyKV2QufRJ2ER1lHCNVlZe8ulggyL2O1+5mGpD:mGPYk+f2pom18KhmJ2bNV19V1+4cK6t
MD5:	15FBD5D0206B7D8F9FEC92C8E963564B
SHA1:	8C8A2F9E4FF769C6C9B8ABB4140239AFD16C4F5F
SHA-256:	62E595DF416E6A3AA216A4D024AB4C388B2FABA513FA57218E188643C3CA84C1
SHA-512:	402406AAD5DB35A2C9834FFCFCA6210D66C56E6761093CC77BD4B8CE6231BBCC9BEC45C3D48E88E408AF3FEBED894294509B4E0A1DC686536544993B6881FD F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...=..O...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yM/r/GOqaipo_LHI.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....H.....H...u..}.R.pK.W.K[C...%. Wi..v...A..Eo.....I.,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\47935f7b9953df3c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.643659745563099
Encrypted:	false
SSDEEP:	6:mMPYk+f2pomZ8DhmJ2BvoUaNTthNIRK6t:Nb++amZ8DkJhZGr
MD5:	F36D5D9D90F5C3AE153CA487F2B35BAE
SHA1:	B6C7F6061B12F3C617218B4B9ABC3FB6C2422FC6
SHA-256:	7E7DB75D9E5320B6345DCE1CE3A48D61E747F3BBFDD7C2025385829FB68062B7
SHA-512:	3C27B5351DD7DBFD04DE4FB99647BAC112E46F06588F94BA67CF76A2519E17791B74A5370B8483A3636098524C7A8D5ACE00C265E054D82BEC26934D39467177
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....6.D...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yr/r/e5deGq8Aq4C.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.f... /.....K.....j?...U.T...G...`..K.D.h. U$0\..M.A..Eo.....h.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\49c24b5e17704bab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.585131734060404
Encrypted:	false
SSDEEP:	6:mY6Yj018IrAzyvLKFvpMObAJ01JGLJzkYYhK6t:FG1t/L2ssizi7
MD5:	DD08D689C04424E866B5D4D6E4E409CA
SHA1:	650FF4930D16335CA1B9DFDC15C05BB6106C3CB1
SHA-256:	D723AD7C64CEF1121E09A3A558DFCCE022B9DAE100B63460958046AF614D1829
SHA-512:	153F3463D010DF03FB4F5EFEAC9270AF050FFDCDC85DE448273AC944E02B78191D7D04ED187FF87B0311C8E9BE6311572C737EE4C1227B21C05AFD92314AC03
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...T.V...._keyhttps://abs.twimg.com/responsive-web/client-web/polyfills.ae028905.js .https://twitter.com/.<M.. /.....W.....+..qa.....v,..K.^.P.H._.9.. A..Eo.....P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a9225483d95e5eb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.55468303912471
Encrypted:	false
SSDEEP:	6:mcfYj018IrAWQ0zMFuTUCytyBBQsc3phK6t:rX1tBQbQot4BdcZ
MD5:	AE6F8DA07FEA103C6D7371725BCBA32F
SHA1:	9B7E1616EDB26CC9B61943E41482FE7BBD0EA6B3
SHA-256:	B5EA5D55CE39C3BD545E4013817D83FB9F0880A745C1F8B4E7D2187D0A019298
SHA-512:	5B3F6CD51A951034EF83A43588180C19BE63D97E03CF119C465417908DF80B93D58676BD27691D35E2D880CA01AF7FFAC61C85844D2550F455ACC99705F2F5B4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d.....8....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.SideNav.ea30e095.js .https://twitter.com/..[.. /.....[.....r...MF.&..v?[z.Z.2.`....l.d ...A..Eo.....Q.^o.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4c16b10bb10a8be2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.4645445771676835
Encrypted:	false
SSDEEP:	3:m+ltTgv8RzYj0KKKXlMMIrASM2ppgvDlMRBAlHCNdlO9XERmBW///pK5kt:m6VYj018IrASdgvpMjzNdqx0hK6t
MD5:	D0E2415BD26F0B3A8F824F1C00619414
SHA1:	69F05533F18ACDAD96DD66C8849D5B4B61EF53CF
SHA-256:	AE04AF91010086981269C00C2392B4945629C30A8DCAB4590FD1DB7EA7CFFE24
SHA-512:	F53C09A24C7169F025CA2DA7CD5EEDBC7D7054CE38D118A0EF214D321993E9EDF2EEBFBE23444C08BB9E201A4186BB6390A46DCF0D6587519765E1AEAA9FE 2C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g.....O....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.WideLayout.68b55ab5.js .https://twitter.com/..a.. /.....`.....F..a..e.}..R...jo..HHe.j d.+b..A..Eo.....y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4cc8080613f306a2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.686126124335653
Encrypted:	false
SSDEEP:	6:m5Yk+f2pomS2Ja6zhmJ2wZhcfpoJuaKhZ/bK6t:w++amSka6zkJFBujN
MD5:	2DA23055D628A1A6ABE471590E923396
SHA1:	1E3604C18A0DC4DEF7F12DE0A6DC790D08CA7A67
SHA-256:	D059B9DB35B84863ABBE62DE9FD0E3E84960EB459786107BABD74E94EFCBF1C6
SHA-512:	F95FB6B80D9D35C404D9857DD90E2FA211978415FA00DD61B5F0C7C1DA8CF6618C418F1E8D481156F53D972BD02256BA448EF0B6CFBA0D2042F47AC92790E75
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....V@...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y1/r/UDf5Ho3OCQC.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/^W... /.....K.....VKQ.. .../.S.(..,...-P{I [/93i.A..Eo.....b.g.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d5beca1fcaa411f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.718494699612942
Encrypted:	false
SSDEEP:	6:mn4XYk+f2pomWGDu3dwhmJ2ouUd7dBk5GOK6t:wE++amSdwkJ79fk5p
MD5:	D62BDD655F8D4BCF20630EE06EB58DAB
SHA1:	0049458926CF1370CDBC014B5989883BCF9428EF
SHA-256:	DA4366E2A3A14882BB61FEB9E4EA91F23ADAE4CCB53AE8F97500B4CBA076B257
SHA-512:	EA004159324B64C03DBEC7E3AD80A694AE386DCFC4E12971496CAA77F1FC0384B645A169B55B2E51EF6F00E5E23C61560EC6971E95AA08D0300056405C18976E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d5beca1fcaa411f_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...C.k....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iCm04/yf/l/en_US/SbRAF_sbhKX.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....J.....U,-7..J.g#8.$.>AW.MzWf.....!.A..Eo.....#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\50e627063c936bdd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.5042033103457015
Encrypted:	false
SSDEEP:	6:mQAlXYj018IrAMUKgLjQL0pMEyx/lUlsknr8xmH4IK6t:WP1thUKgPQI1gyCap
MD5:	E3688AC99CF06306D4C983CE1D7E802A
SHA1:	1B4C1118C93DEDE0CC7CB723F7BB490274245877
SHA-256:	458C3D9050D85DF8DE0C3F27F5C40F643A29B8C447EAD19C010658A126D4DDAC
SHA-512:	742B0E6E283E2B9960652E68C96350DF9E6E2C9D8902AEE07E219F52904D10E6FC547BD093561CB7957F28BFFECD89D589B7EA33A1A036423DAE17D199BD461
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...<.c....._keyhttps://abs.twimg.com/responsive-web/client-web/sharedCore.72796975.js .https://twitter.com/..X.. /.....].....$).7.C....WW.....v7Q3...C.H.n4.. .A..Eo.....H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\51b503b5d6440e91_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.771346861201985
Encrypted:	false
SSDEEP:	6:mLO5Yk+f2pomWu6wzhmJ20y5tHOeAJAK6t:c4++ambkJzwCi
MD5:	35CD479EAC821DDA91788CF58950B50B
SHA1:	F3514D0B4B4F15D230CD4AC5C58A74F09BA560A0
SHA-256:	9AD4C2D36E17AB92EDF7B99703D51F8EA1B520C537B8A334A6693236030B5FDB
SHA-512:	91761F3E9976C9C9F9C02A428D7CA45D229FD664468971076588BF3C4668535A51C9C712DAD55EC5CE7279DEBBB12E90B60E94FDA83E5BF69BA455029730A7F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....kU9...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ipVm4/yo/l/en_US/09OQsWhV8HJ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....I.....0%%.....C8....)?.....F.A.....(.A..Eo.....M#.....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):	236
Entropy (8bit):	5.66714264787457
Encrypted:	false
SSDEEP:	6:mo1XXYk+f2pomcMeo5hmJ2iMVT0h5Rhm4n7lZK6t:Vz++amcMjkJ/BfaK1
MD5:	BD709BE497C240A88AC84184197F6BFD
SHA1:	3AEA2844A2E03BD11694E3F8F8D9313116818220
SHA-256:	23BBF3A9685BF684C8CD7583C3B82922562458D0440C42619D15628F22B8408B
SHA-512:	20511D83812A57BB0F6048CA55341879EA705EC2C948029E20F84C492C1CED292836A2DCE65A3058BC0B18C578BC8EFC6F6FBBC1C65BF7D2DECE0EADF86942 2
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/.s... /.....K.....%%.k.....68q..v+..U^`..A.. <..4m..A..Eo.....;&>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\587845a19e3873e9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.5744988719511

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\587845a19e3873e9_0	
Encrypted:	false
SSDEEP:	6:mjVYj018IrAukGIMqMYl8AZlczK4BUZK6t:AN1tRncZuu
MD5:	47E5AF55F596897B77661673EC80CCE6
SHA1:	83B765FC3A0791662D8D75CEBB59E0310AA2EDDC
SHA-256:	7419E8685C6D9DF6F0A701D373C0543933C245EEC738394295E61F7CC5B66910
SHA-512:	09849EAAD302BAD2735F90875D57BDD86DFD7A533B547759AD068936E7FA569ADA28660771A260ABBB8C9C3945D72FFB7DC403BA7AC56DB3C484985A56B103 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...i....._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.BranchSdk.3c1b92c5.js .https://twitter.com/..\.. /.....`.....a.....iKL...r.%....N...}z ...$.A..Eo.....n.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5a4fc9425c294c5b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.674390031638928
Encrypted:	false
SSDEEP:	6:mtInYk+f2pomWxgE56kDjwhmJ2kKyJKLJw5YvP4X5lDK6t:HD++am2gE9PwkJIfJw+W5r
MD5:	19621A472BA07871FBC21629C865B2C6
SHA1:	E8F500D00906E9591A06840897922F1BFC3AEE03
SHA-256:	47EBCD882C0AF3E20A19E4200A3DEFB41F329207C6A28A53996E2B340DF81C8D
SHA-512:	A42EC43D342CF787D32F9705D3207B546B2472CBFD0CACE4AE0D10E72130C3AE2352F34841A75385999ED53B3A6457DB594BA37D61FF46BC6DE6B00ADD598D 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...._.m..._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iTER4/yS/l/en_US/3gezRsyBCm8.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....5I.....IWl;.RnJ.. (....(..%...z.e.Y.-=%..A..Eo.....+r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d182912050829df_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.6933441454594975
Encrypted:	false
SSDEEP:	6:mYPYk+f2pomfMgoWxzhmJ2iuNtTGXLy3/a/nv1/llhK6t:Nb++am/oykJF2wbyPY1/ll7
MD5:	0D2CAC39C49DED37CABB0962DDF7CC3C
SHA1:	F5810E58A052DA789977E05FA8D1511D4EF5705A
SHA-256:	1BDD3AABD1A4605F7FF5F1ECFAC4BED747F26C6B06CBF4CBE302F16F649DB916
SHA-512:	514E34D9F2B54F8F80AF4D1E51E04B7B6486E5C9DBADC1710CEC4E9BB72993BECB6BC3FD36FB004A8B09FC62B074DD431CC4C71D730A7F57639F4D3508D6D E8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....ql....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y4/r/Vxv31HjompG.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/P.... /.....hJ.....i80!.6....<.2.....t.. v4..C..A..Eo.....9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e2e4f9692f0b13a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.727978503664352
Encrypted:	false
SSDEEP:	6:mr5Yk+f2pomWK2E6iWyawhmJ2ouGXNhhP1UQSCgrLhZK6t:85++amSy5kJrJhBeQSlT
MD5:	629EE842CC17DAA6F0F2901178ADCA2F
SHA1:	C19BA249C680A27EBC884AED81D3823626C2DCEB
SHA-256:	803E16080DED04F39D6433D98A2EE0BC75DA6F452D04FC14116FA188DB1EBDEC
SHA-512:	8CC7C23EACFC0D48530536879B1FB4EAC6D5C4FC1593F7CC9199B4AF7EFA59E5508C2031B048E8B044240B55421B5F827731E085594B143111486BB571997926
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e2e4f9692f0b13a_0	
Preview:	0\r..m.....s...O....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iQ5J4/y7/l/en_US/tv_DX8Bjdmb.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/vr... /.....K.....|J|. /.Q1O.9.R+...b..m-..1.n-....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5f6f227b59756c64_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.699478234053664
Encrypted:	false
SSDEEP:	6:mvbYk+f2pomD8CIZahmJ2eSLO9e9LnnK6t:E/++amrcakJIOq9
MD5:	D0E7CC488E323B88C13869EEF293D7A5
SHA1:	E5CA1F4283D98FEB230D7E18090651EF7668DF15
SHA-256:	6FF67F5740F842D69F82563104F812188905C1E85F447F966DC1ECF0342EC5BB
SHA-512:	064C76DDE1ACE980B7123A67A46908442FE3B2C712D0910531D440618DC23375E6D4FB69D075EC85148EC0F317A796C7E727A16688CDB84FFFA1F2B219CE5C2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...=w.N...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yh/r/wn_IGlUlJbH.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....K.....I...}.<.D.....I..e./T.. ..S...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\606849688d4bb593_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.701818721730682
Encrypted:	false
SSDEEP:	6:mSJ9Yk+f2pomOjPyhmJ2GJyfEZVvXx+4fhEDK6t:N++amrkJrzxQ
MD5:	BD778CB001A2960409A2C5327A639251
SHA1:	AC36DA47F072E14A8288595E80CCDCD777DFD202
SHA-256:	27AB06AE49995BAE65B6829EE9CB9B29FA5164A9D5614910B68001785351D6CA
SHA-512:	575018A2A00A1D17AC5EA1A727430CC0734B088840C41432F1EF09970974D95AEEE92F7ABACC8E90CA524A5532302A890C8EAF405D70583B2B88169E9914FA6E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....{4....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yO/r/ab73kXtVKwb.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/o.... /.....G.....x...a.....J`{.....A. .Eo.....A..Eo.....

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):	236
Entropy (8bit):	5.641473065289216
Encrypted:	false
SSDEEP:	6:m+/VYk+f2pom70XzhmJ246X6Ts+xin/dK6t:FN++am70XzkJm6TC3
MD5:	5F0F284EE7DF20E0B4AB0402747F7D76
SHA1:	2BCDCF950BD3797F1B110942A78B397D948D24E9
SHA-256:	E5E90FE5182C89F6039F7C1859E8C6CBEF3E20DDAD8FF37C48D70F53C8BAD342
SHA-512:	E72BA3BCC29C5DE662E29D908005862613FCC71DA7B29E125DA86C1C7D5F824C2B3766BC702F5B214CB7002E92442D34AF9DEE5295D99AAE4E49B137A1D6C8 9
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/n.... /.....I.....;...L.tUq9..,F....x..H.....).A.. Eo.....j8@.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\638ab953a4a9def7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.757909021449013
Encrypted:	false
SSDEEP:	6:m3vlXYk+f2pomWXT56fXhmJ2Yy5+6xGzAPnK6t:gvN++amMUXkJPs+6xGq

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\638ab953a4a9def7_0	
MD5:	2FDB643C3BBBC21DF6E80C5BEC3AEE69
SHA1:	BFF508ED0745C8181B080D4A7B8E404DC25A9ADD
SHA-256:	AA37609358E7244A5B82518176A25570CA0FE4B40594DB093FC57545E37C53CC
SHA-512:	B45DA198D117103774519E418466C42C29E746B2643FE3FCCD1D159DEDA7B2C87668FD181931561CE83F31174018A445C597F57EE4AE28A653542E7B529AC571
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i2544/yG/l/en_US/kBFwhZE_B0s.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....H.....L...*.Q....z ..z.z.M.w.q..b....A..Eo.....Lif.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\641a65c40e152b65_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.499262526111315
Encrypted:	false
SSDEEP:	6:msBnYK7RrnTgVxXpql/BjHo+k4jaHzbK6t:773exs/to+kaE
MD5:	503245D9E91431FFCEA0B48224951916
SHA1:	E23C8809045B23649B497F1591746EFDFC48B2FC
SHA-256:	732CC1B2E81CEB2C7E95A7360949547F4C64888E7F8339A96A3FA2D31A98BF6C
SHA-512:	84D61FF4E48B7E97AB78DDB6C0769B6C63CE32BCD47E9BA3FA9E4AC373553D2980E62327E0AF7DB7C66E46B3623AB85F5F18D3274E5B9EFD792B8661F5252C 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....v....._keyhttps://dojq4kt8ws9iq.cloudfront.net/s/dist/hammer.min.js .https://nimbusweb.me/..... /.....P.....k..1...'..)..z@eL.....W....4..A..Eo.....V0?b..... A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\641ca75826dd58da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.886838397764225
Encrypted:	false
SSDEEP:	6:mm3YgVVjWFVvVAFH/TxnaTEk44K6tous5hHM1nkIaQcaklem/cx3aTEk4:vTVqFLgH7MlybeNa025/3
MD5:	20E4ECACE7AE49B4DD91884042D7B3C0
SHA1:	7FBE9849ED54BA50F8F46E77D540456E46E87FF6
SHA-256:	F1506A17DDAD59D0E0D856901F60A93B386BBF735FE7740B75FC0AB95726D484
SHA-512:	6E5EE015B7B0997F0C9310081CE543434A1B432523E6CB0B6FEA4C55A62700C4BEA704A299560A98168F030413CF32CDE55BBAB317544B0D66C44A43735E318A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...~.J....._keyhttps://nimbusweb.co/js/jquery.js .https://nimbusweb.co/..Y.. /..... .....y...p...N.Q..k...D\....`.. ....A..Eo.....*.....A..Eo.....Y.. /.H ...67825DD6E44EC0BDD40C09F9BAF1077F5D169F641A3FA80B2BBA2C885C436E69.y...p...N.Q..k...D\....`.. ....A..Eo.....VfHL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6caf33b6bd7e94fc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.650175386496886
Encrypted:	false
SSDEEP:	6:ms8Yk+f2pomzIkhmJ2cWGXr5QkP45lDK6t:E++am0kkJl+kPGr
MD5:	FD20DD8DF8ECB9006FF30F29DCE3F5B6
SHA1:	71DE4D57E2715B485F4450019C4D179367DB757E
SHA-256:	BD1BB16BB3F8683EA50A26356C2D0A42F791086F258C15DEBC5B9E18997EA650
SHA-512:	B83ABDA6CD1A5ED5D7ABD9D237592441D91D3E8C997F08C1A397317FF4EACE869FE310E737BB28B5E2980C05C8B316A43CBEE5912E4A84073FB528E4982CC0 31
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yR/r/LmuezwB8cn0.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.... /.....pI.....c.....W~.nu.}..[..@..=.._ .X....A..Eo.....m../.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6e077c501824184e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.677871753703549
Encrypted:	false
SSDEEP:	6:m7EYk+f2pomXC3iOihmJ28AKO3IF/ZK6t:kU++amXC39ikJJU2/T
MD5:	62B30593867C5E58F84CEB67E2DF1058
SHA1:	BC34BB9ED8CAF8C8C4D48B75CF65F93ADABF740D
SHA-256:	5F643A62294B5688D089550DC784770801FA53D7CC6364DC7F46ADD9B50A46E8
SHA-512:	F5B23ACF350906680078D0608E098CDE3910AEFD07FB386AF2100ECA24F3AD3048D50C58A5975AA81FFCD4DF21B32F267C3E4094856B92012555242323855320
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....7.j...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yX/r/JgRGIalEJI_.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/#u... /.....K.....p.. ..O#....4.|A....%G. ,...A..Eo.....Nd.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6edf3876325017ed_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.701218257959172
Encrypted:	false
SSDEEP:	6:mSYk+f2pombAru5hmJ2yKyqvQPaK4q/ZK6t:r++amfkJ4vQjT
MD5:	58CC39F3A8F5E77C669D6EF24F2943CF
SHA1:	A4FBE2E71CDA60F17812E87604C45BB8F6A86A5B
SHA-256:	07E82BD68686038CBAF2AF31488DD34DB23E3BAD3EF093C48A9E3D33E307346D
SHA-512:	49A759206CC383F4F001C2E84A480A52B67A2ED8E32135E735834626E197BE1060FBF9E97C3D9CCF9035940525FB992B6F624DF19FB6C3A06BE82689051AA3CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...a..:...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y0/r/WM-sXC5KTtF.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/B.... /.....G.....E."!c..i.f.C....j.A..E o.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\71ca85b82fc37bb6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.634784728838115
Encrypted:	false
SSDEEP:	6:m9/VYj018lrAAABIHy6kOM3mnlGSsJwWY+bK6t:a/N1tpDk0sOmN
MD5:	EE852862A4BCA27DC875AD4678ECFDBC
SHA1:	F7AB5566D00E82D4E32309464D2D272E8203EDA2
SHA-256:	673F99010F0BB16E131AC6E7F367E90BC2CB1587794929B91311FA208E70D98C
SHA-512:	B1CAE95AE52309899787D83220C6BF83597B67D8F075468B5EA0C080E804EFE45640F4BA91F7E4707C33CEB017460111642B3388E36C6360C1A69C449DF8FF4A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...#b&#...._keyhttps://abs.twimg.com/responsive-web/client-web/loaders.video.VideoPlayerDefaultUI.98d1c095.js .https://twitter.com/.... /.....t.....e....6... .%.%.2.y.(b..@....]..A..Eo.....L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\772d0e2d35f5552e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.655188014302619
Encrypted:	false
SSDEEP:	6:mUYk+f2pomm0V6zhmJ26YuV3qxvgTnXdK6t:9++amEzkJFYFyX3
MD5:	4D0EAB6A871792B4FB5B8B22340E0EEF
SHA1:	F6075C88E0483D29827EF930DF951BAE84EB9AE4
SHA-256:	C593A2187CBB24C8B35B7502BB36B12DC4EAFBD175E9C74421D3638B61CE25D3
SHA-512:	5113FC3F0E1ECB1307B292D5F23E72A49C5C86EB2868A1A272B6D2AC52211D86C991ACAA9F253335BE18DE70B5A5986B97F7DA6628A5AC877DEA6EFA01625F(E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\772d0e2d35f5552e_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....'.:...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y7/r/T65QLoW8uGK.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....GI.....K..h#..._~&O+E;jq..6~w/4e.*...4.A..Eo.....\.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78b9b6df18d2eae2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.67867950194653
Encrypted:	false
SSDEEP:	6:mdYk+f2pomDszhmJ2QmTk9cNyiwfuNthK6t:8++amDszkJtmA9myvfm1
MD5:	871BC28A265095C5060B7B9D62DA0559
SHA1:	AD00ACBDCD3993647298DE3207A412961233276E
SHA-256:	76EC00D60D7096023E5E0D179735705963BDF760B406FD947F354D6F3E2ACF29
SHA-512:	CD07083373358FE46DB2AA588F4EAB6241B05DC1E6EC70634406EA63C71613D0647F18B25AB23EDDEAAA88DD5D920723A15B61244E459D9772E7048F40258EE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...iS~....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yG/r/jf43jL33vGK.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....LI.....w...9.....K.%...nX.r...^]Q..A..Eo.....=."{.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7923d0bcd78d68b0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.653845309432088
Encrypted:	false
SSDEEP:	6:mXYk+f2pomNpfzhmJ27puyMgSXm4fbK6t:u++amNpbkJArq
MD5:	D0054047C30C6C996F27EEA60C7CBC31
SHA1:	8B73CFFAFF6B4E3AEADBF580F120C3D129716C3F
SHA-256:	2E6A93CF3B6F5CF1E7BD0244426569AA52B7531E92EEDB032CA0098FBED149CE
SHA-512:	3502FDE7419E0E216F981D9A66D7B6EAB1B90A103E4E9570EC72B262DB8733F70467DA612D5458203D1485FAF0116C4106063F57E8CE2DCE43C9E86DC80B8C0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....D.X...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yf/r/YLUhqKHR2Rc.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....eK.....q.?.||....h9Qip-..4.>..p.Qh.H.%.A..Eo.....=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\796754b66abe62b8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.7005318265786915
Encrypted:	false
SSDEEP:	6:mcYk+f2pomybp9hmJ2k3y1Vown3/tnK6t:d++ama7kJbyEwnf
MD5:	96AC363F13A28B8BFFF330CBFF125DDF
SHA1:	2C94DC55AAAC31485667072508C4CE9A9EEA05C0
SHA-256:	097378DA023E80EF8D01D74D7984ADD2C071EC8F96A84CEA6395B32D5816B11D
SHA-512:	94BE0D53E5FD319EC67EF5CE43D53CC2E922BFC6700495D3C3CB76378C6D5716F736C2B66523B6640696A7AA8CF388753D36B44B33D8646A48832A32D97ED81
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....m...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yk/r/rigRDZa6ZK5.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.s... /.....K.....K..F%..<..\..D.....T..W..G".J...A..Eo.....3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7aaa0fbcf5ef3c94_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.612781825249857
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7aaa0fbcf5ef3c94_0	
SSDEEP:	6:maRqEYK7RrnEXj1VxTaTKkFF3/nhlK6t:oSAxTaR
MD5:	499F03F17376950BEA943C81FA7953A3
SHA1:	FCCD28E417B008857773A83378669B137CBBA348
SHA-256:	D03B9DD7470E04868E945361503EFB93206E1AF9567F7D07B45943A67D839AA9
SHA-512:	304565F8A3479D71B18F9225799402DDBAB57A95A17163C4858AEB1AEA45A7A339A858D992B072B3ED45F232D89B49356F2B26E4CA12CA2EE78472D7A2BB4858
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y...0.O...._keyhttps://dojq4kt8ws9iq.cloudfront.net/s/dist/common.js?v=6.32.0 .https://nimbusweb.me/'.... /.....e.....p....._6.>....~.B....^..Z...A..Eo.....@.L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7ad7b31de23151ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.695519198772958
Encrypted:	false
SSDEEP:	6:msXYk+f2pom1CH6Sa6zhmJ2RTEidl+Lrp9K6t:l++am1C06zkJugidzF
MD5:	788D7F975F7BC4F1DE8929C75FD71809
SHA1:	2F1108B88B488C8B6A500EE42A5E7BE261BCFE92
SHA-256:	273682C9BD514F8742620BD2F1B4D4EFFD82AE85C3F13A12FE97E50AA35C45F2
SHA-512:	CFD9B5A4FBF447D6C581097E9654DC7D361422E529A8A49A9DE6316440209C5C314A936B2E984C23A938E98819C39E13855F2114ECEEE7BDA107D3C506C43FD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...x.1{...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yM/r/f9GnCUK_UiC.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..... /.....I.....&5y.....m..&...~.C6.W..|..5..A..Eo.....Z..6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7c9d7e61cbd55ec4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.736071381355032
Encrypted:	false
SSDEEP:	6:mPuEYk+f2pomWJE6suc5hmJ268+A5wXVQ+P4KzlhK6t:Yv++amN9kJFBcyVX/J7
MD5:	089699C0217F5821D4C62351CFEE07ED
SHA1:	84E0758F6A91D11322F2BBB700FB1BF1AA249050
SHA-256:	EE40A5477ED9ED96C2B44135C1FA0D7DA651AAB1E77F2212DBC141DF89BF010A
SHA-512:	CD92C8AF25D187983AFD1B5923667A1AE19859FD8879F956978A90B2331C0A5ACD65BBCAC7B835C587839A1D5D29EE9AE42E7AF3D3B412CD621F52409DBEF70
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...+..b...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i1Mb4/yG/l/en_US/_tf3Dp4sdK2.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.u... /.....K.....d.x.....Yz..G._.G..*J.....A..Eo.....L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d34e82d1fa7c7d2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.622334241439775
Encrypted:	false
SSDEEP:	6:mYYgVxWKNpMzUKVvVxkbFAlpoLreDK6t:1xWR19x+ApoC
MD5:	2582C9A4EA4EFE9FAF10810936198C7A
SHA1:	59D6D5F7FB6B3C43F8F8A1E38EBFA79586200859
SHA-256:	BAAEBE26A547A8FBD08249D2C6697CE06DEEDF6EFB3E2F120243E9AB369BD421
SHA-512:	31E21DE3CF45A965A0EC21DB18B24F563C8187351716819FDB2BAAA7235A8F96C5BD6CB618ABF074DEC1F98F9607ABB4A6C5B6725EFE7260DCF7D93A9DE6A4ED
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i.....Q...._keyhttps://nimbusweb.me/s/static/assets/fe393a50d1a5de4d08f2.vendors~highlight.js .https://nimbusweb.me/.... /..... .....?...MM.S-..`.....P...!}.....A..Eo.....z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\82089636f4b503e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.761680625189936
Encrypted:	false
SSDEEP:	6:m7MYk+f2pomWvCKmhmJ2qlAp/lU/XOn8eC/d5lDK6t:sM++am+mkJqlUP08B
MD5:	9ED3AFF0984DA1E3FFFEFA390FD000F8
SHA1:	395E952DDAF225EB70775C9D844502377EAEF39E
SHA-256:	153D8D08C98D9735A8B3D2B9AA5C521612AC3D2B4AAE4DD40E1B4A1F966E17D6
SHA-512:	F67D969308941274248D93ABDD592C5B00F798A373F6F7C64664733C66B2D021FB6E68BF2560BF1043B5112A47DFF7271150955629F521A4B3426731CB3B511B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iQbs4/yC/l/en_US/aRfo6JTRAVo.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/"h... /.....K.....woK.'.....G..3..Oy.@.K.....A..Eo.....<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\829a9334451bf071_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.736006553699147
Encrypted:	false
SSDEEP:	6:mS+Yk+f2pomWA9bUbohmJ2EAal/TyBJSyQB4BDK6t:Dy++am3KskJr/T4MJk
MD5:	7951E54E4C4EF6CF3CB943EAE1425CC2
SHA1:	DDDA6755BC94BB45FD27E05C47DAF8C8DF91E50F
SHA-256:	93F5E2731B8CCD68AF0A3983552FC85B28B97B212545D6976BA53FA55FA113D5
SHA-512:	A50E3C3B902B491258146687CC6B02AAE3453CF13B30D85907E824B644BA2B21DDA48B01990764BF4D220BB0345B67BAF0D3AF68B776631FD289ADEC0E75F80
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....(....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ilae4/y4/l/en_US/TmINRVi806h.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/c{... /.....%H.....4...}.6oD.l.k=...&.@.E.}yz...%.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\849c3de6865d8565_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.4077673727864335
Encrypted:	false
SSDEEP:	6:mEanYiMs8pMEcTBYj8IcNupgLrzK5XhK6t:Mr3NYgIc8piC7
MD5:	159C7E9FB71693CE5124F92DCDF47981
SHA1:	78FF006350E9A15D07D72223618CF673D0F8BC79
SHA-256:	B2A5A2587168ABBFF0DF554AE8D12902D46A40936A8A19C06053613D645E247B
SHA-512:	D1F3317E73FAD19D71161D4E49A654BF510676F4A9B7545130B29B32FD50633A1D4F2F91FF6C95256138FACC870AF5E06AC26C8A783CAB4F3AC780D397870EDI
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....._keyhttps://twitter.com/i/js_inst?c_name=ui_metrics .https://twitter.com/+.j.. /.....$a.....D...L...9..g.....-...m...oN.B.A..Eo.....^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\87806a7015e261d7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.732195420201014
Encrypted:	false
SSDEEP:	6:mtTYk+f2pomWCc51t2UzhmJ2fyuvkCbmSR9k4LDK6t:8++am+kJ6vkoDbr
MD5:	92A12DC194F7C7CFD99A24B2C9D8813B
SHA1:	40D94492DAB9153FB8EE0283120DA7FA512B1F3C
SHA-256:	D8F0C9FE3FD38B0B466C13D9BF05DC40530503894B1272D117CBD55CE04B8736
SHA-512:	51B70297DBD917938942A820BD1367BB7ABEBF524094EB3CD1E253B7A20274E628E482AB031124F4DC1313E7E969A4072FE23422647A66ACBA78D5D598C59F5E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\87806a7015e261d7_0	
Preview:	0\r..m.....s...I^.h...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i1MJ4/yw/l/en_US/SJKVto5H7se.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.... /.....zI.....o.W ZZ.,.*sg.T..|!....M.{....j.A..Eo.....I.....A..Eo.....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 111

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:00:11.585175037 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:11.626549959 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:11.626633883 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:11.629456043 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:11.641216993 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:11.641287088 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:11.670732975 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:11.673970938 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:11.673996925 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:11.674014091 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:11.674103975 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:11.677517891 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:11.678052902 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:13.078797102 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:13.078946114 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:13.079195023 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:13.120280027 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.120291948 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.120317936 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.122714043 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.123135090 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:13.172003984 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.593271971 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.593296051 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.593313932 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.593333006 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.593350887 CEST	443	49691	13.224.193.106	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:00:13.593368053 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.593410969 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:13.593456030 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:13.594444036 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.653888941 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:13.678674936 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.678709030 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.678850889 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:13.679176092 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.679646015 CEST	443	49691	13.224.193.106	192.168.2.5
May 12, 2021 20:00:13.679730892 CEST	49691	443	192.168.2.5	13.224.193.106
May 12, 2021 20:00:13.825659990 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.826029062 CEST	49704	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.826374054 CEST	49705	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.867134094 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.867243052 CEST	443	49704	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.867305994 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.867325068 CEST	49704	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.867551088 CEST	443	49705	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.867619991 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.867765903 CEST	49704	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.867784023 CEST	49705	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.867909908 CEST	49705	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.877815008 CEST	443	49704	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.877908945 CEST	49704	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.884594917 CEST	443	49705	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.884689093 CEST	49705	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.886336088 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.886419058 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.908878088 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.908920050 CEST	443	49704	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.909060955 CEST	443	49705	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.909326077 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.909343958 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.909358978 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.909481049 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.911176920 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.911258936 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.918328047 CEST	443	49705	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.918365955 CEST	443	49705	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.918382883 CEST	443	49705	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.918446064 CEST	49705	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.924746990 CEST	443	49705	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.924830914 CEST	49705	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.943485975 CEST	443	49704	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.943523884 CEST	443	49704	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.943540096 CEST	443	49704	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.943614006 CEST	49704	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.944885015 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.945653915 CEST	49705	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.946003914 CEST	49705	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.946095943 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.946145058 CEST	49704	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.946526051 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.946584940 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.946625948 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.948144913 CEST	443	49704	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.948225975 CEST	49704	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.986569881 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.986799002 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.986972094 CEST	49703	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.987405062 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.987442017 CEST	443	49703	13.225.74.128	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:00:13.987696886 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.987968922 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.993043900 CEST	443	49705	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.993341923 CEST	443	49705	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.993406057 CEST	49705	443	192.168.2.5	13.225.74.128
May 12, 2021 20:00:13.994096041 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.994126081 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.994144917 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.994168043 CEST	443	49703	13.225.74.128	192.168.2.5
May 12, 2021 20:00:13.994185925 CEST	49703	443	192.168.2.5	13.225.74.128

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:00:00.785805941 CEST	55432	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:00.837704897 CEST	53	55432	8.8.8.8	192.168.2.5
May 12, 2021 20:00:01.693996906 CEST	64936	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:01.745604992 CEST	53	64936	8.8.8.8	192.168.2.5
May 12, 2021 20:00:02.579554081 CEST	52704	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:02.628492117 CEST	53	52704	8.8.8.8	192.168.2.5
May 12, 2021 20:00:03.388493061 CEST	52212	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:03.446543932 CEST	53	52212	8.8.8.8	192.168.2.5
May 12, 2021 20:00:04.334583044 CEST	54302	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:04.386156082 CEST	53	54302	8.8.8.8	192.168.2.5
May 12, 2021 20:00:05.554023981 CEST	53784	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:05.602865934 CEST	53	53784	8.8.8.8	192.168.2.5
May 12, 2021 20:00:11.413202047 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:11.417260885 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:11.424544096 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:11.439138889 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:11.477602005 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 20:00:11.478573084 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 20:00:11.486852884 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 20:00:11.496555090 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 20:00:12.473330975 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:12.532185078 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 20:00:12.539856911 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:12.598721981 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 20:00:12.714968920 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:12.776434898 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 20:00:13.442220926 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:13.500066996 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 20:00:13.735008955 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:13.735878944 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:13.786107063 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 20:00:13.811171055 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 20:00:14.194319010 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:14.245928049 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 20:00:14.635992050 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:14.694371939 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 20:00:15.498413086 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:15.550806999 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 20:00:16.185273886 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:16.243014097 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 20:00:16.591955900 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:16.654448986 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 20:00:16.702385902 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:16.750941038 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 20:00:17.021174908 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:17.056947947 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:17.069767952 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 20:00:17.125591040 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 20:00:17.164254904 CEST	50464	443	192.168.2.5	74.125.140.157
May 12, 2021 20:00:17.218790054 CEST	443	50464	74.125.140.157	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:00:17.218818903 CEST	443	50464	74.125.140.157	192.168.2.5
May 12, 2021 20:00:17.220916033 CEST	50464	443	192.168.2.5	74.125.140.157
May 12, 2021 20:00:17.273200989 CEST	443	50464	74.125.140.157	192.168.2.5
May 12, 2021 20:00:17.273633957 CEST	50464	443	192.168.2.5	74.125.140.157
May 12, 2021 20:00:17.273775101 CEST	50464	443	192.168.2.5	74.125.140.157
May 12, 2021 20:00:17.325824976 CEST	443	50464	74.125.140.157	192.168.2.5
May 12, 2021 20:00:17.325839043 CEST	443	50464	74.125.140.157	192.168.2.5
May 12, 2021 20:00:17.326304913 CEST	50464	443	192.168.2.5	74.125.140.157
May 12, 2021 20:00:17.683505058 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:17.740609884 CEST	53	50394	8.8.8.8	192.168.2.5
May 12, 2021 20:00:18.514467955 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:18.563222885 CEST	53	58530	8.8.8.8	192.168.2.5
May 12, 2021 20:00:21.284379005 CEST	57344	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:21.343955040 CEST	53	57344	8.8.8.8	192.168.2.5
May 12, 2021 20:00:24.650846004 CEST	59261	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:24.708174944 CEST	53	59261	8.8.8.8	192.168.2.5
May 12, 2021 20:00:27.202013016 CEST	57151	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:27.259147882 CEST	53	57151	8.8.8.8	192.168.2.5
May 12, 2021 20:00:27.887595892 CEST	59413	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:27.944557905 CEST	53	59413	8.8.8.8	192.168.2.5
May 12, 2021 20:00:29.010390997 CEST	60516	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:29.076154947 CEST	53	60516	8.8.8.8	192.168.2.5
May 12, 2021 20:00:29.563580990 CEST	51649	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:29.627095938 CEST	53	51649	8.8.8.8	192.168.2.5
May 12, 2021 20:00:32.285783052 CEST	50464	443	192.168.2.5	74.125.140.157
May 12, 2021 20:00:32.363342047 CEST	443	50464	74.125.140.157	192.168.2.5
May 12, 2021 20:00:42.770442009 CEST	65086	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:42.829514027 CEST	53	65086	8.8.8.8	192.168.2.5
May 12, 2021 20:00:48.825649977 CEST	56432	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:48.885854006 CEST	53	56432	8.8.8.8	192.168.2.5
May 12, 2021 20:00:49.865995884 CEST	52929	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:49.914628983 CEST	53	52929	8.8.8.8	192.168.2.5
May 12, 2021 20:00:50.787751913 CEST	64317	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:50.876638889 CEST	53	64317	8.8.8.8	192.168.2.5
May 12, 2021 20:00:50.938740015 CEST	61004	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:50.942653894 CEST	56895	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:50.997821093 CEST	53	61004	8.8.8.8	192.168.2.5
May 12, 2021 20:00:51.001044989 CEST	53	56895	8.8.8.8	192.168.2.5
May 12, 2021 20:00:51.221234083 CEST	62372	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:51.285873890 CEST	53	62372	8.8.8.8	192.168.2.5
May 12, 2021 20:00:54.910948038 CEST	56675	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:54.962533951 CEST	53	56675	8.8.8.8	192.168.2.5
May 12, 2021 20:00:54.987598896 CEST	57172	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:54.991424084 CEST	55267	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:55.017862082 CEST	50969	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:55.048960924 CEST	53	55267	8.8.8.8	192.168.2.5
May 12, 2021 20:00:55.059232950 CEST	53	57172	8.8.8.8	192.168.2.5
May 12, 2021 20:00:55.076910973 CEST	53	50969	8.8.8.8	192.168.2.5
May 12, 2021 20:00:55.195877075 CEST	64362	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:55.260607958 CEST	53	64362	8.8.8.8	192.168.2.5
May 12, 2021 20:00:55.289088964 CEST	54766	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:55.337786913 CEST	53	54766	8.8.8.8	192.168.2.5
May 12, 2021 20:00:55.942625999 CEST	61446	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:55.942672968 CEST	57515	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:55.942749023 CEST	58199	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:55.996172905 CEST	53	57515	8.8.8.8	192.168.2.5
May 12, 2021 20:00:56.001471043 CEST	53	61446	8.8.8.8	192.168.2.5
May 12, 2021 20:00:56.008322001 CEST	53	58199	8.8.8.8	192.168.2.5
May 12, 2021 20:00:56.057265043 CEST	65221	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:56.058305979 CEST	61573	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:56.107558012 CEST	53	65221	8.8.8.8	192.168.2.5
May 12, 2021 20:00:56.118539095 CEST	53	61573	8.8.8.8	192.168.2.5
May 12, 2021 20:00:58.437937975 CEST	56562	53	192.168.2.5	8.8.8.8
May 12, 2021 20:00:58.502007961 CEST	53	56562	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:01:01.721818924 CEST	53591	53	192.168.2.5	8.8.8.8
May 12, 2021 20:01:01.773629904 CEST	53	53591	8.8.8.8	192.168.2.5
May 12, 2021 20:01:03.767790079 CEST	59688	53	192.168.2.5	8.8.8.8
May 12, 2021 20:01:03.819319010 CEST	53	59688	8.8.8.8	192.168.2.5
May 12, 2021 20:01:03.961198092 CEST	56032	53	192.168.2.5	8.8.8.8
May 12, 2021 20:01:04.018474102 CEST	53	56032	8.8.8.8	192.168.2.5
May 12, 2021 20:01:04.725415945 CEST	61150	53	192.168.2.5	8.8.8.8
May 12, 2021 20:01:04.893878937 CEST	53	61150	8.8.8.8	192.168.2.5
May 12, 2021 20:01:09.161449909 CEST	63458	53	192.168.2.5	8.8.8.8
May 12, 2021 20:01:09.210705042 CEST	53	63458	8.8.8.8	192.168.2.5
May 12, 2021 20:01:09.585366964 CEST	53247	53	192.168.2.5	8.8.8.8
May 12, 2021 20:01:09.655751944 CEST	53	53247	8.8.8.8	192.168.2.5
May 12, 2021 20:01:09.818171978 CEST	58544	53	192.168.2.5	8.8.8.8
May 12, 2021 20:01:09.883307934 CEST	53	58544	8.8.8.8	192.168.2.5
May 12, 2021 20:01:10.039529085 CEST	53814	53	192.168.2.5	8.8.8.8
May 12, 2021 20:01:10.097197056 CEST	53	53814	8.8.8.8	192.168.2.5
May 12, 2021 20:01:10.470099926 CEST	51305	53	192.168.2.5	8.8.8.8
May 12, 2021 20:01:10.522067070 CEST	53	51305	8.8.8.8	192.168.2.5
May 12, 2021 20:01:34.600795984 CEST	53670	53	192.168.2.5	8.8.8.8
May 12, 2021 20:01:34.661467075 CEST	53	53670	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 20:00:11.417260885 CEST	192.168.2.5	8.8.8.8	0xc108	Standard query (0)	nimbusweb.me	A (IP address)	IN (0x0001)
May 12, 2021 20:00:13.735008955 CEST	192.168.2.5	8.8.8.8	0x524f	Standard query (0)	dojq4kt8ws9iq.cloudfront.net	A (IP address)	IN (0x0001)
May 12, 2021 20:00:14.194319010 CEST	192.168.2.5	8.8.8.8	0x648d	Standard query (0)	cdn.polyfill.io	A (IP address)	IN (0x0001)
May 12, 2021 20:00:16.591955900 CEST	192.168.2.5	8.8.8.8	0xa021	Standard query (0)	text.nimbusweb.me	A (IP address)	IN (0x0001)
May 12, 2021 20:00:16.702385902 CEST	192.168.2.5	8.8.8.8	0x493b	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
May 12, 2021 20:00:17.056947947 CEST	192.168.2.5	8.8.8.8	0x6e2d	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
May 12, 2021 20:00:17.683505058 CEST	192.168.2.5	8.8.8.8	0x50d9	Standard query (0)	nimbusweb.me	A (IP address)	IN (0x0001)
May 12, 2021 20:00:21.284379005 CEST	192.168.2.5	8.8.8.8	0x9d1f	Standard query (0)	nimbusweb.co	A (IP address)	IN (0x0001)
May 12, 2021 20:00:27.202013016 CEST	192.168.2.5	8.8.8.8	0x9098	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
May 12, 2021 20:00:42.770442009 CEST	192.168.2.5	8.8.8.8	0x8946	Standard query (0)	nimbusweb.co	A (IP address)	IN (0x0001)
May 12, 2021 20:00:48.825649977 CEST	192.168.2.5	8.8.8.8	0xdeb9	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
May 12, 2021 20:00:49.865995884 CEST	192.168.2.5	8.8.8.8	0x932f	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 12, 2021 20:00:50.787751913 CEST	192.168.2.5	8.8.8.8	0xce1	Standard query (0)	scontent-frt3-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 12, 2021 20:00:50.938740015 CEST	192.168.2.5	8.8.8.8	0xf566	Standard query (0)	scontent-frt3-2.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 12, 2021 20:00:50.942653894 CEST	192.168.2.5	8.8.8.8	0xe144	Standard query (0)	scontent-frx5-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 12, 2021 20:00:51.221234083 CEST	192.168.2.5	8.8.8.8	0xf279	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
May 12, 2021 20:00:54.910948038 CEST	192.168.2.5	8.8.8.8	0xf3e3	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 12, 2021 20:00:54.987598896 CEST	192.168.2.5	8.8.8.8	0xe608	Standard query (0)	scontent-frt3-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 12, 2021 20:00:54.991424084 CEST	192.168.2.5	8.8.8.8	0x308d	Standard query (0)	scontent-frx5-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.017862082 CEST	192.168.2.5	8.8.8.8	0xa99a	Standard query (0)	scontent-frt3-2.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.195877075 CEST	192.168.2.5	8.8.8.8	0x6d21	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.289088964 CEST	192.168.2.5	8.8.8.8	0x157e	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.942625999 CEST	192.168.2.5	8.8.8.8	0x3388	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 20:00:55.942672968 CEST	192.168.2.5	8.8.8.8	0x3e92	Standard query (0)	api.twitter.com	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.942749023 CEST	192.168.2.5	8.8.8.8	0xcaa8	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
May 12, 2021 20:00:56.057265043 CEST	192.168.2.5	8.8.8.8	0xa22e	Standard query (0)	t.co	A (IP address)	IN (0x0001)
May 12, 2021 20:00:56.058305979 CEST	192.168.2.5	8.8.8.8	0xdfd2	Standard query (0)	video.twimg.com	A (IP address)	IN (0x0001)
May 12, 2021 20:00:58.437937975 CEST	192.168.2.5	8.8.8.8	0x7a79	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
May 12, 2021 20:01:01.721818924 CEST	192.168.2.5	8.8.8.8	0x4ee0	Standard query (0)	abs-0.twimg.com	A (IP address)	IN (0x0001)
May 12, 2021 20:01:03.767790079 CEST	192.168.2.5	8.8.8.8	0xdd36	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
May 12, 2021 20:01:03.961198092 CEST	192.168.2.5	8.8.8.8	0x2387	Standard query (0)	abs-0.twimg.com	A (IP address)	IN (0x0001)
May 12, 2021 20:01:04.725415945 CEST	192.168.2.5	8.8.8.8	0x2a82	Standard query (0)	lil-tex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:00:11.477602005 CEST	8.8.8.8	192.168.2.5	0xc108	No error (0)	nimbusweb.me		13.224.193.106	A (IP address)	IN (0x0001)
May 12, 2021 20:00:11.477602005 CEST	8.8.8.8	192.168.2.5	0xc108	No error (0)	nimbusweb.me		13.224.193.81	A (IP address)	IN (0x0001)
May 12, 2021 20:00:11.477602005 CEST	8.8.8.8	192.168.2.5	0xc108	No error (0)	nimbusweb.me		13.224.193.125	A (IP address)	IN (0x0001)
May 12, 2021 20:00:11.477602005 CEST	8.8.8.8	192.168.2.5	0xc108	No error (0)	nimbusweb.me		13.224.193.4	A (IP address)	IN (0x0001)
May 12, 2021 20:00:13.811171055 CEST	8.8.8.8	192.168.2.5	0x524f	No error (0)	dojq4kt8ws9iq.cloudfront.net		13.225.74.128	A (IP address)	IN (0x0001)
May 12, 2021 20:00:13.811171055 CEST	8.8.8.8	192.168.2.5	0x524f	No error (0)	dojq4kt8ws9iq.cloudfront.net		13.225.74.23	A (IP address)	IN (0x0001)
May 12, 2021 20:00:13.811171055 CEST	8.8.8.8	192.168.2.5	0x524f	No error (0)	dojq4kt8ws9iq.cloudfront.net		13.225.74.22	A (IP address)	IN (0x0001)
May 12, 2021 20:00:13.811171055 CEST	8.8.8.8	192.168.2.5	0x524f	No error (0)	dojq4kt8ws9iq.cloudfront.net		13.225.74.48	A (IP address)	IN (0x0001)
May 12, 2021 20:00:14.245928049 CEST	8.8.8.8	192.168.2.5	0x648d	No error (0)	cdn.polyfill.io	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:16.654448986 CEST	8.8.8.8	192.168.2.5	0xa021	No error (0)	text.nimbusweb.me		13.224.193.49	A (IP address)	IN (0x0001)
May 12, 2021 20:00:16.654448986 CEST	8.8.8.8	192.168.2.5	0xa021	No error (0)	text.nimbusweb.me		13.224.193.62	A (IP address)	IN (0x0001)
May 12, 2021 20:00:16.654448986 CEST	8.8.8.8	192.168.2.5	0xa021	No error (0)	text.nimbusweb.me		13.224.193.27	A (IP address)	IN (0x0001)
May 12, 2021 20:00:16.654448986 CEST	8.8.8.8	192.168.2.5	0xa021	No error (0)	text.nimbusweb.me		13.224.193.13	A (IP address)	IN (0x0001)
May 12, 2021 20:00:16.750941038 CEST	8.8.8.8	192.168.2.5	0x493b	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:16.750941038 CEST	8.8.8.8	192.168.2.5	0x493b	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
May 12, 2021 20:00:16.750941038 CEST	8.8.8.8	192.168.2.5	0x493b	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
May 12, 2021 20:00:16.750941038 CEST	8.8.8.8	192.168.2.5	0x493b	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
May 12, 2021 20:00:16.750941038 CEST	8.8.8.8	192.168.2.5	0x493b	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:00:17.125591040 CEST	8.8.8.8	192.168.2.5	0x6e2d	No error (0)	www.google.de		142.250.185.227	A (IP address)	IN (0x0001)
May 12, 2021 20:00:17.740609884 CEST	8.8.8.8	192.168.2.5	0x50d9	No error (0)	nimbusweb.me		13.224.193.106	A (IP address)	IN (0x0001)
May 12, 2021 20:00:17.740609884 CEST	8.8.8.8	192.168.2.5	0x50d9	No error (0)	nimbusweb.me		13.224.193.81	A (IP address)	IN (0x0001)
May 12, 2021 20:00:17.740609884 CEST	8.8.8.8	192.168.2.5	0x50d9	No error (0)	nimbusweb.me		13.224.193.125	A (IP address)	IN (0x0001)
May 12, 2021 20:00:17.740609884 CEST	8.8.8.8	192.168.2.5	0x50d9	No error (0)	nimbusweb.me		13.224.193.4	A (IP address)	IN (0x0001)
May 12, 2021 20:00:21.343955040 CEST	8.8.8.8	192.168.2.5	0x9d1f	No error (0)	nimbusweb.co		54.173.51.37	A (IP address)	IN (0x0001)
May 12, 2021 20:00:27.259147882 CEST	8.8.8.8	192.168.2.5	0x9098	No error (0)	clients2.google.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:27.259147882 CEST	8.8.8.8	192.168.2.5	0x9098	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)
May 12, 2021 20:00:42.829514027 CEST	8.8.8.8	192.168.2.5	0x8946	No error (0)	nimbusweb.co		54.173.51.37	A (IP address)	IN (0x0001)
May 12, 2021 20:00:48.885854006 CEST	8.8.8.8	192.168.2.5	0xdeb9	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:48.885854006 CEST	8.8.8.8	192.168.2.5	0xdeb9	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
May 12, 2021 20:00:49.914628983 CEST	8.8.8.8	192.168.2.5	0x932f	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:49.914628983 CEST	8.8.8.8	192.168.2.5	0x932f	No error (0)	scontent.xx.fbcdn.net		157.240.9.23	A (IP address)	IN (0x0001)
May 12, 2021 20:00:50.876638889 CEST	8.8.8.8	192.168.2.5	0xce1	No error (0)	scontent-frt3-1.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
May 12, 2021 20:00:50.997821093 CEST	8.8.8.8	192.168.2.5	0xf566	No error (0)	scontent-frt3-2.xx.fbcdn.net		157.240.20.19	A (IP address)	IN (0x0001)
May 12, 2021 20:00:51.001044989 CEST	8.8.8.8	192.168.2.5	0xe144	No error (0)	scontent-frx5-1.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
May 12, 2021 20:00:51.285873890 CEST	8.8.8.8	192.168.2.5	0xf279	No error (0)	facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
May 12, 2021 20:00:54.962533951 CEST	8.8.8.8	192.168.2.5	0xf3e3	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:54.962533951 CEST	8.8.8.8	192.168.2.5	0xf3e3	No error (0)	scontent.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.048960924 CEST	8.8.8.8	192.168.2.5	0x308d	No error (0)	scontent-frx5-1.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.059232950 CEST	8.8.8.8	192.168.2.5	0xe608	No error (0)	scontent-frt3-1.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.076910973 CEST	8.8.8.8	192.168.2.5	0xa99a	No error (0)	scontent-frt3-2.xx.fbcdn.net		157.240.20.19	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.260607958 CEST	8.8.8.8	192.168.2.5	0x6d21	No error (0)	facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.337786913 CEST	8.8.8.8	192.168.2.5	0x157e	No error (0)	twitter.com		104.244.42.129	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.337786913 CEST	8.8.8.8	192.168.2.5	0x157e	No error (0)	twitter.com		104.244.42.1	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.996172905 CEST	8.8.8.8	192.168.2.5	0x3e92	No error (0)	api.twitter.com	tpop-api.twitter.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:00:55.996172905 CEST	8.8.8.8	192.168.2.5	0x3e92	No error (0)	tpop-api.twitter.com		104.244.42.194	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.996172905 CEST	8.8.8.8	192.168.2.5	0x3e92	No error (0)	tpop-api.twitter.com		104.244.42.130	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.996172905 CEST	8.8.8.8	192.168.2.5	0x3e92	No error (0)	tpop-api.twitter.com		104.244.42.2	A (IP address)	IN (0x0001)
May 12, 2021 20:00:55.996172905 CEST	8.8.8.8	192.168.2.5	0x3e92	No error (0)	tpop-api.twitter.com		104.244.42.66	A (IP address)	IN (0x0001)
May 12, 2021 20:00:56.001471043 CEST	8.8.8.8	192.168.2.5	0x3388	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:56.001471043 CEST	8.8.8.8	192.168.2.5	0x3388	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
May 12, 2021 20:00:56.008322001 CEST	8.8.8.8	192.168.2.5	0xcaa8	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:56.008322001 CEST	8.8.8.8	192.168.2.5	0xcaa8	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:56.008322001 CEST	8.8.8.8	192.168.2.5	0xcaa8	No error (0)	cs2-wac-eu.8315.ecdns.net	cs45.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:56.008322001 CEST	8.8.8.8	192.168.2.5	0xcaa8	No error (0)	cs45.wac.edgecastcdn.net		93.184.220.70	A (IP address)	IN (0x0001)
May 12, 2021 20:00:56.107558012 CEST	8.8.8.8	192.168.2.5	0xa22e	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
May 12, 2021 20:00:56.107558012 CEST	8.8.8.8	192.168.2.5	0xa22e	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
May 12, 2021 20:00:56.107558012 CEST	8.8.8.8	192.168.2.5	0xa22e	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
May 12, 2021 20:00:56.107558012 CEST	8.8.8.8	192.168.2.5	0xa22e	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
May 12, 2021 20:00:56.118539095 CEST	8.8.8.8	192.168.2.5	0xdfd2	No error (0)	video.twimg.com	cs296.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:56.118539095 CEST	8.8.8.8	192.168.2.5	0xdfd2	No error (0)	cs296.wpc.edgecastcdn.net	cs2-wpc.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:56.118539095 CEST	8.8.8.8	192.168.2.5	0xdfd2	No error (0)	cs2-wpc-eu.8315.ecdns.net	cs189.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:56.118539095 CEST	8.8.8.8	192.168.2.5	0xdfd2	No error (0)	cs189.wpc.edgecastcdn.net		68.232.34.217	A (IP address)	IN (0x0001)
May 12, 2021 20:00:58.502007961 CEST	8.8.8.8	192.168.2.5	0x7a79	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:00:58.502007961 CEST	8.8.8.8	192.168.2.5	0x7a79	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
May 12, 2021 20:01:01.773629904 CEST	8.8.8.8	192.168.2.5	0x4ee0	No error (0)	abs-0.twimg.com	abs-zero.twimg.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:01:01.773629904 CEST	8.8.8.8	192.168.2.5	0x4ee0	No error (0)	abs-zero.twimg.com		104.244.43.131	A (IP address)	IN (0x0001)
May 12, 2021 20:01:03.819319010 CEST	8.8.8.8	192.168.2.5	0xdd36	No error (0)	pbs.twimg.com	twimg.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:01:03.819319010 CEST	8.8.8.8	192.168.2.5	0xdd36	No error (0)	twimg.twitter.map.fastly.net		199.232.136.159	A (IP address)	IN (0x0001)
May 12, 2021 20:01:04.018474102 CEST	8.8.8.8	192.168.2.5	0x2387	No error (0)	abs-0.twimg.com	abs-zero.twimg.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:01:04.018474102 CEST	8.8.8.8	192.168.2.5	0x2387	No error (0)	abs-zero.twimg.com		104.244.43.131	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:01:04.893878937 CEST	8.8.8.8	192.168.2.5	0x2a82	No error (0)	lil-tex.com		64.4.160.22	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nimbusweb.co
- twitter.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49764	54.173.51.37	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:00:36.835791111 CEST	5665	OUT	GET /index.php HTTP/1.1 Host: nimbusweb.co 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
May 12, 2021 20:00:36.969046116 CEST	5665	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 12 May 2021 18:00:36 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Location: https://nimbusweb.co/index.php 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 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 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 bgcolor="white"> 301 Moved Permanently <hr> nginx </body></html>

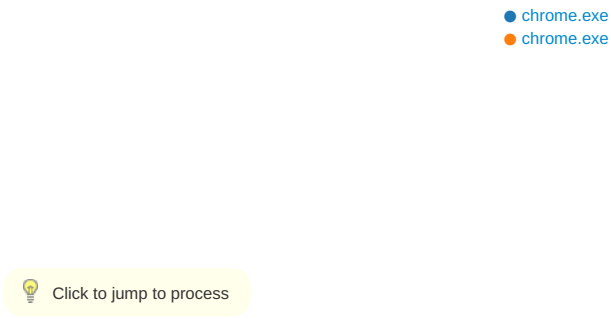
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49841	104.244.42.129	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:00:55.388012886 CEST	9823	OUT	GET /nimbuswebinc HTTP/1.1 Host: twitter.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
May 12, 2021 20:00:55.535681963 CEST	9861	IN	HTTP/1.1 301 Moved Permanently date: Wed, 12 May 2021 18:00:55 UTC server: tsa_devel location: https://twitter.com/nimbuswebinc set-cookie: personalization_id="v1_R08mrlhzcWeaRY69FrW/9A=="; Max-Age=63072000; Expires=Fri, 12 May 2023 18:00:55 GMT; Path=/; Domain=.twitter.com; Secure; SameSite=None set-cookie: guest_id=v1%3A162084245547353324; Max-Age=63072000; Expires=Fri, 12 May 2023 18:00:55 GMT; Path=/; Domain=.twitter.com; Secure; SameSite=None cache-control: no-cache, no-store, max-age=0 content-length: 0 x-connection-hash: 7ec34c088e5acbe4d1b49cb2b5de0f78defa5153e323eaa1882acf6ad06dca94

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4656 Parent PID: 4132

General

Start time:	20:00:07
Start date:	12/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://nimbusweb.me/s/share/5487165/gpvilg008fxq3oxcr6eh'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 1764 Parent PID: 4656

General

Start time:	20:00:08
Start date:	12/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1604,7990105799513037393,10231270219144405014,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly