ID: 321356
Cookbook: browseurl.jbs
Time: 23:01:14
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

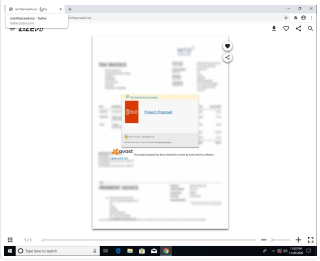
Analysis Report https://faxfax.zizera.com/remittanceadv…

Overview

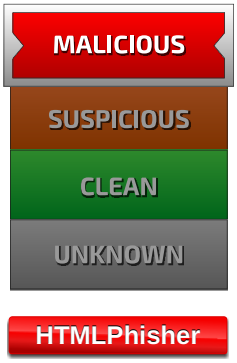
General Information

Sample URL:	http://https://faxfax.zizera.com/remittanceadvice
Analysis ID:	321356

Most interesting Screenshot:



Detection

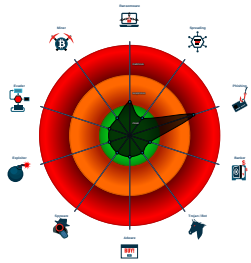


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish_10
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5904 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://faxfax.zizera.com/remittanceadvice' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2308 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1540,3317695339915788095,555655226975024704,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

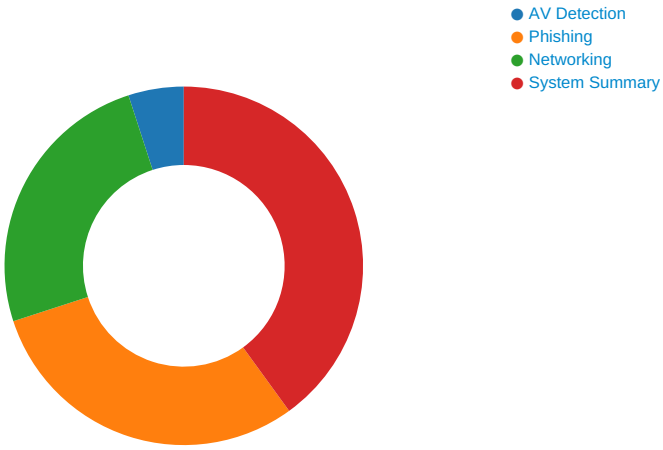
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

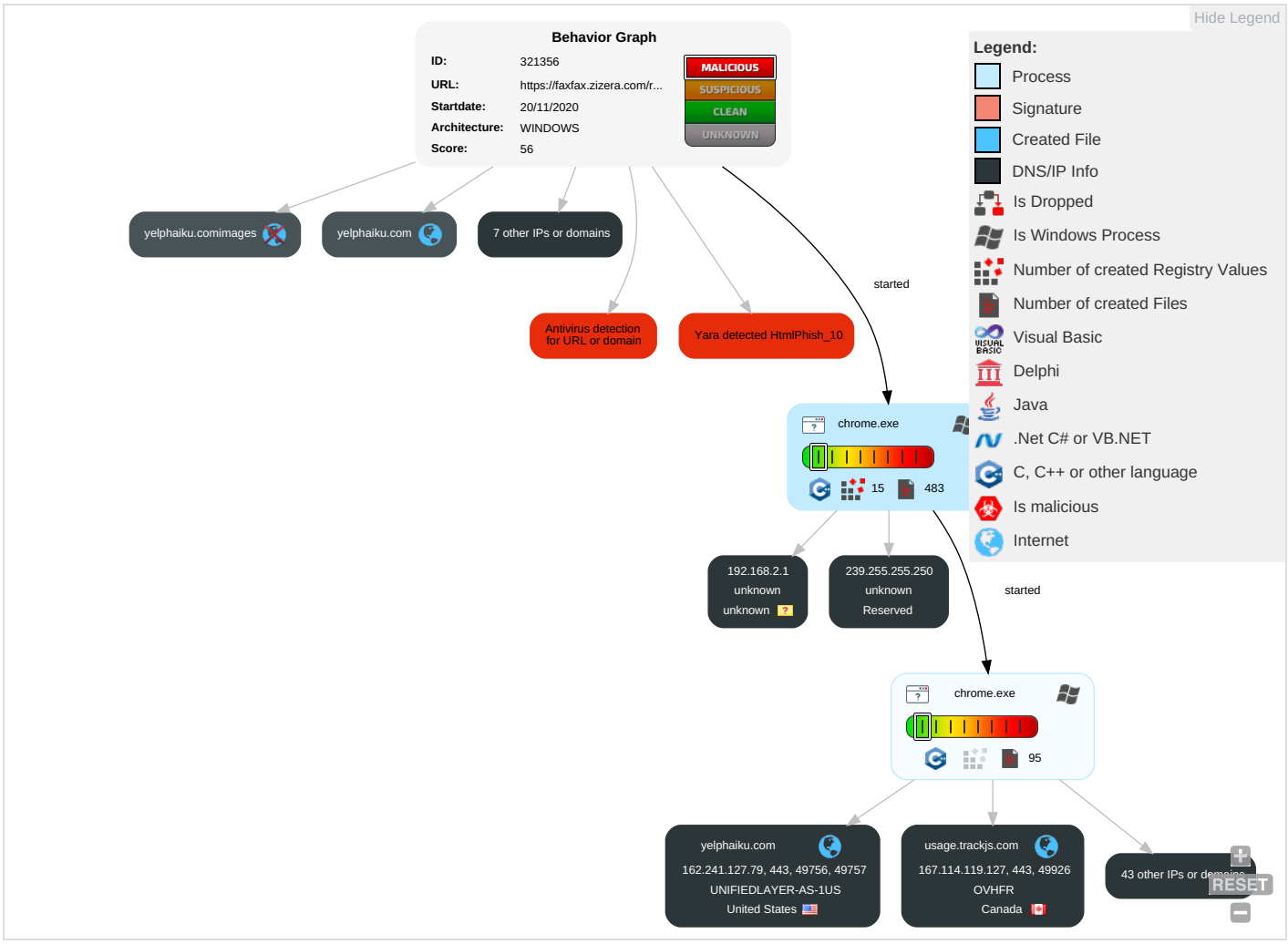
Phishing:

Yara detected HtmlPhish_10

Mitre Att&ck Matrix

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

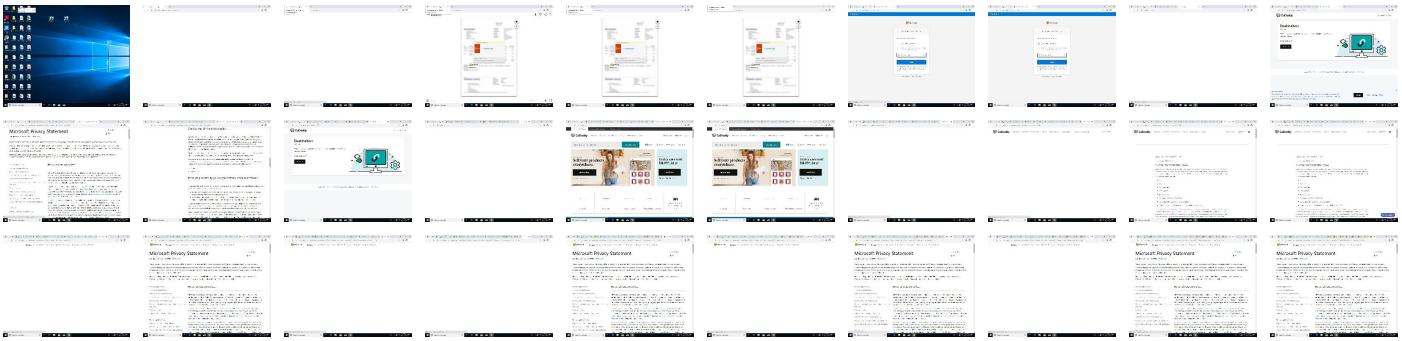
Behavior Graph

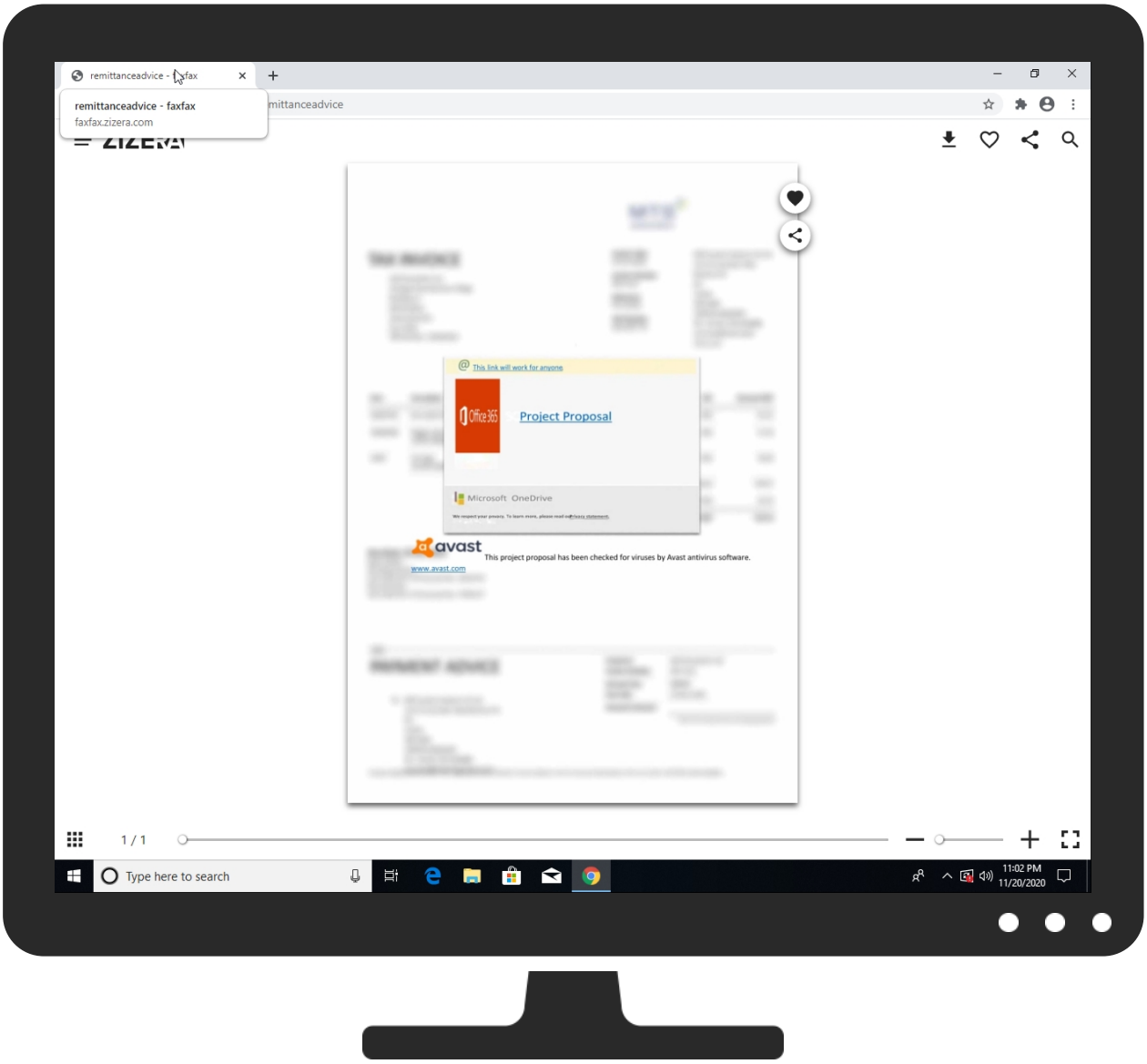


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://faxfax.zizera.com/remittanceadvice	0%	Virustotal		Browse
http://https://faxfax.zizera.com/remittanceadvice	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
x.co	1%	Virustotal		Browse
assets.onestore.ms	0%	Virustotal		Browse
vikinggenetics-my.sharepoint.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://yelphaiku.com/office/mfile/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://:websiteId.onlinestore.godaddy.com/admin/shipping_methods	0%	Avira URL Cloud	safe	
http://https://shortener.godaddy.com1_https://shortener.godaddy.com	0%	Avira URL Cloud	safe	
http://x.co/8923bsuydn	0%	Avira URL Cloud	safe	
http://https://yelphaiku.com/office/mfile/Sharing	0%	Avira URL Cloud	safe	
http://https://assets.onestore.ms/	0%	Avira URL Cloud	safe	
http://https://lpcdn.lpsnmedia.net(_https://lpcdn.lpsnmedia.net	0%	Avira URL Cloud	safe	
http://https://yelphaiku.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pagead46.l.doubleclick.net	172.217.16.194	true	false		high
auth.split.io	184.73.218.177	true	false		high
bullet-pandi-1110328995.eu-west-1.elb.amazonaws.com	34.255.187.247	true	false		high
va.v.liveperson.net	208.89.12.87	true	false		high
cdn.trackjs.netdna-cdn.com	94.31.29.32	true	false		high
shortener.godaddy.com	45.40.140.1	true	false		high
yelphaiku.com	162.241.127.79	true	false		unknown
partnerad.l.doubleclick.net	172.217.21.226	true	false		high
d3cvrokiq7pmri.cloudfront.net	13.224.93.109	true	false		high
x.co	45.40.140.1	true	false	• 1%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
events-prod-1-1033355748.us-east-1.elb.amazonaws.com	34.196.246.142	true	false		high
googlehosted.l.googleusercontent.com	172.217.16.193	true	false		high
dz87sht31vgqa.cloudfront.net	13.224.93.31	true	false		high
usage.trackjs.com	167.114.119.127	true	false		high
img1.wsimg.com	unknown	unknown	false		high
lpcdn.lpsnmedia.net	unknown	unknown	false		high
securepubads.g.doubleclick.net	unknown	unknown	false		high
www.googletagservices.com	unknown	unknown	false		high
events.split.io	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
img6.wsimg.com	unknown	unknown	false		high
assets-a.zizera.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
vikinggenetics-my.sharepoint.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
www.godaddy.com	unknown	unknown	false		high
yelphaiku.comimages	unknown	unknown	false		unknown
www.youtube.com	unknown	unknown	false		high
events.api.godaddy.com	unknown	unknown	false		high
gui.godaddy.com	unknown	unknown	false		high
bam-cell.nr-data.net	unknown	unknown	false		unknown
sdk.split.io	unknown	unknown	false		high
accdn.lpsnmedia.net	unknown	unknown	false		high
js-agent.newrelic.com	unknown	unknown	false		high
faxfax.zizera.com	unknown	unknown	false		high
cdn.trackjs.com	unknown	unknown	false		high
googleads.g.doubleclick.net	unknown	unknown	false		high
spoprod-a.akamaihd.net	unknown	unknown	false		high
tags.tiqcdn.com	unknown	unknown	false		high
streaming.split.io	unknown	unknown	false		high
lptag.liveperson.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.godaddy.com/	false		high
http://https://www.godaddy.com/contact-us	false		high
http://https://yelphaiku.com/office/mfile/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://shortener.godaddy.com/error_404	false		high
http://x.co/8923bsuydn	false	• Avira URL Cloud: safe	unknown

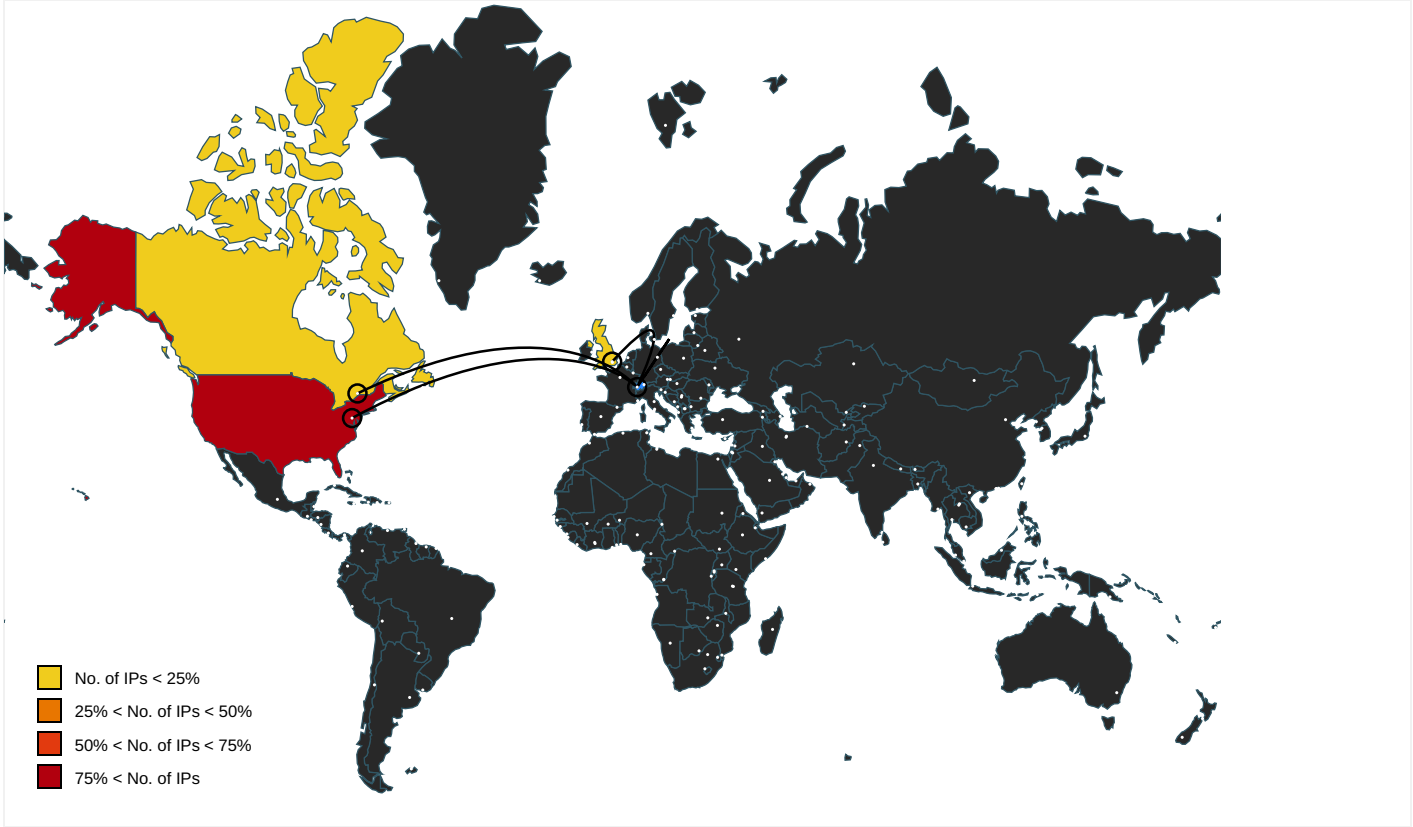
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lptag.liveperson.net/lptag/api/account/30187337/configuration/applications/taglets/.jsonp?v=	183955bae54e77e3_0.0.dr	false		high
http://https://www.godaddy.com/legal/agreements/privacy-policy?target=_blankPrivacy	History-journal.0.dr	false		high
http://https://sdk.split.io/api	ffae120ac1988083_0.0.dr	false		high
http://https://faxfax.zizera.com/remittanceadviceremittanceadvice	History-journal.0.dr	false		high
http://https://www.godaddy.com	000003.log6.0.dr	false		high
http://https://:websiteId.onlinestore.godaddy.com/admin/shipping_methods	000003.log6.0.dr	false	• Avira URL Cloud: safe	low
http://https://shortener.godaddy.com/error_40/N	Current Session.0.dr	false		high
http://https://img6.wsimg.com/wrhs/19613ac22420404c34b7162ef50370cf/tti.min.jsaD	1dcc732920861c78_0.0.dr	false		high
http://https://faxfax.zizera.com/remittanceadvice2	History Provider Cache.0.dr	false		high
http://https://img1.wsimg.com/cdn/Image/Mobile/InApp/1/en-US/b81bd5b1-f196-4b39-901c-b6111398dfda/Publish.p	000003.log6.0.dr	false		high
http://https://accdn.lpsnmedia.net/api/account/30187337/configuration/setting/accountproperties/?cb=lpCb446	702495c6e2e78b0c_0.0.dr	false		high
http://https://securepubads.g.doubleclick.net/	Network Action Predictor.0.dr	false		high
http://https://img6.wsimg.com/wrhs/d6c7b1acb132140b70d61ad9ce6bc527/heartbeat.min.js	75f1105a42981b97_0.0.dr	false		high
http://https://github.com/babel/babel/issues	001b7dfda48b5f6d_0.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/babel-core/5.8.23/browser.min.jsaD	001b7dfda48b5f6d_0.0.dr	false		high
http://https://img1.wsimg.com/cdn/Image/Mobile/InApp/1/en-US/f05bc5f4-5704-4a99-a741-df2c5453cc73/CardBg6.p	000003.log6.0.dr	false		high
http://https://img1.wsimg.com/dc-assets/live-engage/images/link-icon-hover.png	ffae120ac1988083_0.0.dr	false		high
http://https://securepubads.g.doubleclick.net/gpt/pubads_impl_2020111801.js?21068793	d3eaba701bf0be20_0.0.dr	false		high
http://https://img1.wsimg.com/dc-assets/live-engage/images/link-icon.png	ffae120ac1988083_0.0.dr	false		high
http://https://zizera.com/T	31754e45cfd28c3a_0.0.dr	false		high
http://https://img6.wsimg.com/wrhs/2a8723002f286c722aab4069a3c0bc9c/utilityheader.min.js	ca9e60488bdc5258_0.0.dr, 4e7ced3c9971ec86_0.0.dr	false		high
http://https://sso.godaddy.com/logout?realm=idp	ca9e60488bdc5258_0.0.dr	false		high
http://https://sso.godaddy.com?realm=idp&app=mya&path=	ca9e60488bdc5258_0.0.dr	false		high
http://https://img6.wsimg.com/wrhs/19613ac22420404c34b7162ef50370cf/tti.min.js	1dcc732920861c78_0.0.dr	false		high
http://https://events.split.io/api	ffae120ac1988083_0.0.dr	false		high
http://https://zizera.com/f	2e3d5cdfef0b6238_0.0.dr	false		high
http://https://www.godaddy.com/help/shortener-1000035v	Current Session.0.dr	false		high
http://certs.godaddy.com/repository/1301	ED02812CD7D061716B0BBE6F31979D00_FAC544846B8B5FE851FF6BF0CF2990220.1.dr	false		high
http://https://godaddy.com/help/contact-us	000003.log6.0.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js	0ad5e255cfc99a9c_0.0.dr, 094e2d6bf2abec98_0.0.dr	false		high
http://https://godaddy.com/y8	80e4f13fb63695ca_0.0.dr	false		high
http://https://shortener.godaddy.com1_https://shortener.godaddy.com	000003.log6.0.dr	false	• Avira URL Cloud: safe	low
http://https://www.googletagservices.com/	Network Action Predictor.0.dr	false		high
http://https://www.godaddy.com/	000003.log0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://faxfax.zizera.com/remittanceadvice	History-journal.0.dr	false		high
http://https://ajax.aspnetcdn.com/	Network Action Predictor-journal.0.dr	false		high
http://https://img1.wsimg.com/liveengage/v2/tag/3.2.2/liveengage.js	0995e489bf59c488_0.0.dr	false		high
http://https://mya.godaddy.com	ca9e60488bdc5258_0.0.dr	false		high
http://https://img1.wsimg.com/cms/sales/js/sales-cms-m5dfhHAYxYelydH0TOQilVeHUgw_6MEeM366phtlfb01.min.js	e8081f3cea3392c6_0.0.dr	false		high
http://https://accdn.lpsnmedia.net/api/account/30187337/configuration/setting/accountproperties/?cb=lpCb415	ef34c246df0e42bc_0.0.dr	false		high
http://https://img6.wsimg.com/wrhs/1cdb971aba0e6f81bcd65741b66a16ea/uxcore2.min.js	d8fbe577ab80525e_0.0.dr	false		high
http://https://img1.wsimg.com/dc-assets/help/2.379.18-d325e66/js/flamingo.min.js	308b6aa73c0feee0_0.0.dr	false		high
http://https://yelphaiku.com/office/mfile/Sharing	History-journal.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://ola.godaddy.com/:websiteId/services/new	000003.log6.0.dr	false		high
http://https://assets.onestore.ms/	Network Action Predictor-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://godaddy.com/c	3332cf6ef51dd1a9_0.0.dr	false		high
http://https://godaddy.com/d	406a0f0498fb7a87_0.0.dr	false		high
http://https://img6.wsimg.com/wrhs/b0de8fce1ace6e77cf5891d58d0aafc2/uxcore2.min.jsaD	8c4ebfa60d7b4172_0.0.dr	false		high
http://https://godaddy.com/JIR	4e7ced3c9971ec86_0.0.dr	false		high
http://https://img1.wsimg.com/cms/sales/js/sales-cms-m5dfhHAYxYelydH0TOQilVeHUgw_6MEeM366phtlfb01.min.jsaD	e8081f3cea3392c6_0.0.dr	false		high
http://https://lpcdn.lpsnmedia.net(_https://lpcdn.lpsnmedia.net	000004.log.0.dr	false	• Avira URL Cloud: safe	low
http://https://img6.wsimg.com/wrhs/e099922f63ddb7a5d4027821f53ee78f/tcc.min.js	1056dc81b557cff9_0.0.dr, b1e45d6786b73622_0.0.dr	false		high
http://https://tags.tiqcdn.com/utag/godaddy/godaddy/prod/utag.1355.js?utv=ut4.42.202011101205aD	3332cf6ef51dd1a9_0.0.dr	false		high
http://https://godaddy.com/s	0995e489bf59c488_0.0.dr	false		high
http://https://godaddy.com/u	47ccc19b4da77a8d_0.0.dr	false		high
http://https://dcc.godaddy.com	ca9e60488bdc5258_0.0.dr	false		high
http://https://accdn.lpsnmedia.net/api/account/30187337/configuration/le-campaigns/zones?fields=id&fields=z	80e4f13fb63695ca_0.0.dr	false		high
http://https://godaddy.com/m	d3eaba701bf0be20_0.0.dr	false		high
http://https://img6.wsimg.com/wrhs/2a8723002f286c722aab4069a3c0bc9c/utilityheader.min.jsaD	ca9e60488bdc5258_0.0.dr	false		high
http://https://faxfax.zizera.com/lite/assets/js/chunk-vendors.753f9ae2.js	a1898ca8587555c5_0.0.dr	false		high
http://https://godaddy.com/i	aa261b7c4be61a46_0.0.dr	false		high
http://https://img6.wsimg.com/	Network Action Predictor-journal.0.dr	false		high
http://https://websites.godaddy.com/launch?account_uid=:accountId&path=addsection§ionType=FUNDRAISING	000003.log6.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js	762ca5cdd3b40fce_0.0.dr, 041e202bfc772cc8_0.0.dr	false		high
http://https://godaddy.com/E	183955bae54e77e3_0.0.dr	false		high
http://https://godaddy.com/A	f562afac76b4b973_0.0.dr	false		high
http://https://img1.wsimg.com/cdn/Image/Mobile/InApp/1/en-US/b4b78951-160c-4fbe-b348-b66a42826fbf/Chownow.p	000003.log6.0.dr	false		high
http://https://img1.wsimg.com/cdn/Image/Mobile/InApp/1/en-US/70d6d604-9554-4082-98b8-39e2628706cf/Delivery.	000003.log6.0.dr	false		high
http://https://ola.godaddy.com/:websiteId/settings/business_hours	000003.log6.0.dr	false		high
http://https://godaddy.com/8	02454aa6d8da3fb1_0.0.dr	false		high
http://https://shortener.godaddy.com//	QuotaManager.0.dr	false		high
http://https://babeljs.io/	001b7dfda48b5f6d_0.0.dr	false		high
http://https://www.godaddy.com/Domain	History-journal.0.dr	false		high
http://https://godaddy.com/V	4d6125cbda70b6f0_0.0.dr	false		high
http://https://pro.godaddy.com	ca9e60488bdc5258_0.0.dr	false		high
http://https://lpcdn.lpsnmedia.net/le_re/3.43.0.1-release_5028/jsv2/UISuite.js?_v=3.43.0.1-release_5028	aa261b7c4be61a46_0.0.dr	false		high
http://https://yelphaiku.com/	Network Action Predictor-journal.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://godaddy.com/N	08b95bf8e6dd7b84_0.0.dr, d6862ab8bd2f679c_0.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.jsaD	041e202bfc772cc8_0.0.dr	false		high
http://https://img1.wsimg.com/liveengage/v2/tag/3.2.2/liveengage.jsaD	ffae120ac1988083_0.0.dr	false		high
http://https://lpcdn.lpsnmedia.net	000004.log.0.dr	false		high
http://https://account.godaddy.com	ca9e60488bdc5258_0.0.dr	false		high
http://https://cdn.trackjs.com/agent/v3/latest/t.js	08b95bf8e6dd7b84_0.0.dr	false		high
http://https://img1.wsimg.com/cdn/Image/Mobile/InApp/1/en-US/0b124caa-f0d8-4d86-8e7b-1050053b71f9/CardBg3.p	000003.log6.0.dr	false		high
http://https://zizera.com/	a1898ca8587555c5_0.0.dr	false		high
http://https://godaddy.com/4	9064f3a5056d6bb1_0.0.dr	false		high
http://https://websites.godaddy.com/en-US/editor/:websiteId/:homepageId	000003.log6.0.dr	false		high
http://https://godaddy.com/m(	c487f9ceefa38302_0.0.dr	false		high
http://https://accdn.lpsnmedia.net/api/account/30187337/configuration/setting/accountproperties/?cb=lpCb507	1cb141e79f5601dc_0.0.dr	false		high
http://https://godaddy.com/1	7f58cad8484a3ffb_0.0.dr	false		high
http://https://img1.wsimg.com/cdn/Image/Mobile/InApp/1/en-US/e4a8ca06-9bc6-453c-afeb-7baa374845ab/Reminder.	000003.log6.0.dr	false		high
http://https://www.godaddy.com/BDomain	Current Session.0.dr	false		high
http://https://godaddy.com/)	c3de3858c26638d5_0.0.dr	false		high
http://https://img1.wsimg.com/cdn/Image/Mobile/InApp/1/en-US/61119dc6-2b69-47e5-b9fc-8ca7652c4466/Product.p	000003.log6.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.127.79	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false
184.73.218.177	unknown	United States		14618	AMAZON-AESUS	false
94.31.29.32	unknown	United Kingdom		33438	HIGHWINDS2US	false
13.224.93.109	unknown	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
167.114.119.127	unknown	Canada		16276	OVHFR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.16.194	unknown	United States		15169	GOOGLEUS	false
172.217.16.193	unknown	United States		15169	GOOGLEUS	false
208.89.12.87	unknown	United States		11054	LIVEPERSONUS	false
172.217.21.226	unknown	United States		15169	GOOGLEUS	false
142.250.74.194	unknown	United States		15169	GOOGLEUS	false
45.40.140.1	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false
13.224.93.31	unknown	United States		16509	AMAZON-02US	false
34.255.187.247	unknown	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321356
Start date:	20.11.2020
Start time:	23:01:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://faxfax.zizera.com/remittanceadvice
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:	19
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@49/259@37/17

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://yelphaiku.com/office/mfile/ • Browse: http://x.co/8923bsuydn • Browse: https://go.microsoft.com/fwlink/?linkid=845480 • Browse: https://shortener.godaddy.com/error_40/ • Browse: https://www.godaddy.com • Browse: https://www.godaddy.com/contact-us • Browse: https://www.godaddy.com/help/shortener-1000035 • Browse: https://www.godaddy.com/legal/agreements/privacy-policy?target=_blank • Browse: https://privacy.microsoft.com/en-us/privacystatement#maincookiessimilartechnologiesmodul/# • Browse: https://privacy.microsoft.com/en-us/privacystatement#maincookiessimilartechnologiesmodul/#maincookiessimilartechnologiesmodule • Browse: https://privacy.microsoft.com/en-us/privacystatement#maincookiessimilartechnologiesmodul/#mainenterprisedeveloperproductsmodule • Browse: https://privacy.microsoft.com/en-us/privacystatement#maincookiessimilartechnologiesmodul/#mainnoticetoendusersmodule • Browse: https://privacy.microsoft.com/en-us/privacystatement#maincookiessimilartechnologiesmodul/#mainmicrosoftaccountmodule • Browse: https://privacy.microsoft.com/en-us/privacystatement#maincookiessimilartechnologiesmodul/#mainreasonsweshare personaldatamodule • Browse: https://privacy.microsoft.com/en-us/privacystatement#maincookiessimilartechnologiesmodul/#mainwherewestoreandprocessdatamodule • Browse: https://privacy.microsoft.com/en-us/privacystatement#maincookiessimilartechnologiesmodul/#mainhowtoaccesscontrolyourdatamodule
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.147.198.201, 172.217.16.142, 172.217.18.13, 216.58.206.14, 74.125.173.136, 173.194.151.123, 216.58.208.36, 172.217.18.99, 216.58.212.163, 172.217.18.106, 216.58.212.170, 142.250.74.202, 172.217.23.170, 172.217.21.234, 216.58.205.234, 172.217.23.138, 172.217.18.10, 172.217.18.170, 216.58.207.42, 216.58.207.74, 216.58.206.10, 172.217.16.170, 216.58.210.10, 172.217.23.106, 216.58.212.138, 205.185.216.10, 205.185.216.42, 92.122.213.216, 92.122.213.248, 13.107.136.9, 192.124.249.24, 192.124.249.23, 192.124.249.22, 192.124.249.36, 192.124.249.41, 2.17.185.233, 2.20.221.183, 23.37.61.47, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 95.100.71.196, 162.247.243.146, 162.247.243.147, 51.11.168.160, 88.221.62.148, 23.210.249.93, 92.122.213.219, 92.122.213.200, 84.53.167.109, 152.199.19.160, 92.122.213.194, 92.122.213.247, 23.210.248.85, 151.101.2.2, 151.101.66.2, 151.101.130.2, 151.101.194.2, 178.249.101.23, 178.249.97.99, 178.249.97.98, 216.58.205.238, 172.217.23.142, 172.217.18.14, 216.58.207.46, 216.58.207.78, 172.217.16.206, 172.217.16.174, 216.58.210.14, 172.217.23.110, 216.58.212.142, 172.217.18.110, 216.58.212.174, 142.250.74.206, 172.217.23.174, 40.67.251.132, 20.54.26.129, 172.217.16.131, 173.194.187.106, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, assets.onestore.ms.edgekey.net, r3---sn-4g5ednsy.gvt1.com, tls12.newrelic.com.cdn.cloudflare.net, clientservices.googleapis.com, i.s-microsoft.com.edgekey.net, tags.tiqcdn.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net,

wns.notify.windows.com.akadns.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, clients2.google.com, db5p.wns.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, update.googleapis.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, ocsp.godaddy.com.akadns.net, au-bg-shim.trafficmanager.net, a1778.g2.akamai.net, e10583.dspg.akamaiedge.net, events.api.godaddy.com.edgekey.net, fs.microsoft.com, content-autofill.googleapis.com, 17825-ipv4e.farm.prod.sharepointonline.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, statics-marketingsites-wcus-ms-com.akamaized.net, www.googleapis.com, r3.sn-4g5ednsy.gvt1.com, assets.onestore.ms.akadns.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, wildcard-ipv6.godaddy.com.edgekey.net, youtube-ui.l.google.com, blobcollector.events.data.trafficmanager.net, a1531.g2.akamai.net, spoprod-a.akamaihd.net.edgesuite.net, c.s-microsoft.com-c.edgekey.net, clients.l.google.com, privacy.microsoft.com.edgekey.net, r5.sn-4g5edn7y.gvt1.com, spo-0004.spo-msedge.net, e2997.a.akamaiedge.net, e2836.g.akamaiedge.net, e6001.dscx.akamaiedge.net, e8091.a.akamaiedge.net, i.s-microsoft.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, r5---sn-4g5e6nsr.gvt1.com, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, mscomajax.vo.msecnd.net, redirector.gvt1.com, emea1.notify.windows.com.akadns.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, client.wns.windows.com, f2.shared.global.fastly.net, accounts.google.com, cs22.wpc.v0cdn.net, f4.shared.global.fastly.net, accdn.lpsnmedia.livepersonk.akadns.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, cds.d2s7q6s2.hwcdn.net, r5---sn-4g5edn7y.gvt1.com, lptag.liveperson.cotcdb.net.livepersonk.akadns.net, skypedataprdcoleus16.cloudapp.net, gui-ipv6.godaddy.com.edgekey.net, c.s-microsoft.com, global-wildcard.wsimg.com.edgekey.net, privacy.microsoft.com, go.microsoft.com.edgekey.net, lpcdn.lpsnmedia.livepersonk.akadns.net, e13678.dscg.akamaiedge.net, r5.sn-4g5e6nsr.gvt1.com, ocsp.godaddy.com, e13678.dspb.akamaiedge.net, www.microsoft.com, 17825-ipv4.farm.prod.aa-rt.sharepoint.com.spo-0004.spo-msedge.net

- Report size exceeded maximum capacity and may have missing behavior 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
23:02:14	API Interceptor	3x 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\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1731
Entropy (8bit):	7.3079915112818385
Encrypted:	false
SSDEEP:	48:panitq/q8utQKOxdIvnita8lnitq1+Zvl3oXS9As5RmEWqu5H99:pWbKSz1+boavLJpu5
MD5:	BCB7F0085D0CD8973B81545E507D1594
SHA1:	E7C9F5C6CB5901E13CED4873E06B352A0C4FCF3B
SHA-256:	8ECE21D9181E71101530B7F659EF47325030E3CF93FE368976DB65FBC4749516
SHA-512:	D962D02A65AFD0CA2F837CC16FB6514AA7F185556ADE82A9729B01C4AF85E805D9188E0692F09813057633660F4C740F4839E144588EBF9CB993F86F1DDA96B3

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771

Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G2..20201120195135Z0d0b0:0...+.....#o..K.....#....+...:....g(.....An .....20201120195135Z....20201122075135Z0...*.H.....H#.V.....1..j.5B.4.....yAl.'b....O.@.....z1.s..h1..'.$b..d.X..^.s.%..p..!H3....r..7.Z..Vp..O:B.2PD..y...ws.V.a[....+..&..1..2K.....c..'.J..e.jzj..jNh.L.xo%..6...5E.w..:.^....<..L.....D.....7..A7..f>../..2...<..&.g@,....bG.Y.l..CZ.....0...0...0..g.....f...p.t0...*.H.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.110/..U...(Go Daddy Root Certificate Authority - G20...200909070000Z..210909070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G20..."0...*.H.....0.....'.....^Y.u..U.qU..".....-]XG(qk#.+....J...G.3

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	low
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\ED02812CD7D061716B0BBE6F31979D00_FAC544846B8B5FE851FF6BF0CF299022

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1778
Entropy (8bit):	7.332093289951811
Encrypted:	false
SSDEEP:	48:+ni/xTM4lMGynitxUni/1+Zvl3oXS9A0d5RxEOaKlhEe07P:9xTM4lMGl/1+boaFLeHK4W
MD5:	3552F544FE2E36344CBA0E31D8CC47C2
SHA1:	15F3BF54C68434F25C41C688DBB0CFC0B3954263
SHA-256:	4E5E7FCFD642890D35944DF0FDAD81039F513048672FE47C7F3F13D68D8EBDB1
SHA-512:	6AF27580D6E314FA882DBF346A154E559D9B6614069E3313DE5108BF946034881820D77CC5F56F9BFBFB9AF694190E573AFC5517736BC368B08E0B4A3226B730
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0...z0x1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy Inc.1+0)..U..."Go Daddy Validation Authority - G2..20201119224849Z0l0j0B0...+....._lkv...8..f..R34N..@.'..4.0.3..l.,.....Z..&.....202011192248492....20201121104849Z0...*.H.....r..Z...D.p.O5W.....>..po.t...-..5.v.4.xl..F..<...ZA...k....U.,w.....#.....$!..M.M.4.N-..)../.h$....x1...,!6J.`.d.J}...&...x@.....*....Q.a.....e.....e.....Q$.-=^G.Mq..=.].O... cq....J...5.*8>v.1.....L.p..h..2ZF...'.W..O....0...0...0.....X...I0...*.H.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.1-0+..U...$http://certs.godaddy.com/repository/1301..U...*Go Daddy Secure Certificate Authority - G20...200909070000Z..210909070000Z0x1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy Inc.1+0)..U..."Go Daddy Validation Authority - G20.."0...*.H.....0.....'.....^Y.u..U.qU.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	900
Entropy (8bit):	3.7826824336398652
Encrypted:	false
SSDEEP:	24:QwyPV13MhmyFqIegUQUaBIRqwyPV13MhmyFqIegUQUaBIN:QwkV1XyF17BQqwkV1XyF17BI
MD5:	00196E0D8C0864FC2F06F09AD0B01EDB
SHA1:	27B6E4BBF3EB3395E8B619F9A06E09C7E115A882
SHA-256:	4819CBB6DAB59C27187EA11B091F180AF013EC89652C6262B879584ED3A4FC67
SHA-512:	305F91F52581C0104250EB6B013A08FB49ED04350FC3E2A7D2B447927CCF05C00EE898815063BF585F21EDB3C42BF9D50BE8CE3F94C81259C445660206FDBDA1
Malicious:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Reputation:	low
Preview:	p..... .....@...(..... .....=3.v.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.I.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".e.7.c.9.f.5.c.6.c.b.5.9.0.1.e.1.3.c.e.d.4.8.7.3.e.0.6.b.3.5.2.a.0.c.4.f.c.f.3.b."...p..... .....@...(.....=3.v.....L.....L.... .....=3.v.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.I.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".e.7.c.9.f.5.c.6.c.b.5.9.0.1.e.1.3.c.e.d.4.8.7.3.e.0.6.b.3.5.2.a.0.c.4.f.c.f.3.b."...

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):	3.123186963792904
Encrypted:	false
SSDEEP:	6:kKn30wwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:f3HkPlE99SNxAhUegeT2
MD5:	B49043D1256C9A151F0C1E341810A30B
SHA1:	E18071A206715AD507A894A9FA6CAE21D2936DAE
SHA-256:	D4A5C344B8E1F0DB76EACBA06F567B27A0DF722C5EC64D7E584C9A078190C301
SHA-512:	AD90B19A2C86F7F7A74129B2B90DA55A9BE82F21F7710AD5DB63CC2CBA70AFED1A1DF7D9F46B8703C5B038DE78F132059EDE99D9C39187A991D9ED6739E1374
Malicious:	false
Reputation:	low
Preview:	p..... .....N}=...(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\ED02812CD7D061716B0BBE6F31979D00_FAC544846B8B5FE851FF6BF0CF299022	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	964
Entropy (8bit):	3.7748002882266687
Encrypted:	false
SSDEEP:	24:Y+Ihn8B0tQpusnu8+mH5MXho4+Ihn8B0tQpusnu8+mH5MX4:Y40Susu8+mOXh940Susu8+mOX4
MD5:	6E1A580F80EBEAC43C416C0929DA5CAB
SHA1:	A6B2608A7CF93CFBBC807C94F09DC9D81D9EC286
SHA-256:	5F8C97D00F5077088230819C16B65E163C01D38549134E7916237F1DA619722F
SHA-512:	539C50F0AE99BD9887F2B87DF74596C12359EAF73379CFCE74294F9CAB5D42909A88660C227282D471E2353FDA36B9B562E72BC6F6A2EC20FF0FE96A604419A7
Malicious:	false
Reputation:	low
Preview:	p..... ..... .@...(..... .....%%.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.o.w.S.D.B.G.M.E.Q.w.Q.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.S.2.C.A.1.f.b.G.t.2.6.x.P.k.O.K.X.4.Z.g.u.o.U.j.M.0.T.g.Q.U.Q.M.K.9.J.4.7.M.N.I.M.w.o.j.P.X.%.2.B.2.y.z.8.L.Q.s.g.M.4.C.C.Q.D.d.W.r.k.P.J.h.%.2.F.D.%.2.B.A.%.3.D.%.3.D..."..1.5.f.3.b.f.5.4.c.6.8.4.3.4.f.2.5.c.4.1.c.6.8.8.d.b.b.0.c.f.c.0.b.3.9.5.4.2.6.3."...p..... ..... .@...(.....%%..... .....%%.. .....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.o.w.S.D.B.G.M.E.Q.w.Q.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.S.2.C.A.1.f.b.G.t.2.6.x.P.k.O.K.X.4.Z.g.u.o.U.j.M.0.T.g.Q.U.Q.M.K.9.J.4.7.M.N.I.M.w.o.j.P.X.%.2.B.2.y.z.8.L.Q.s.g.M.4.C.C.Q.D.d.W.r.k.P.J.h.%.2.F.D.%.2.B.A.%.3.D.%.3.D..."..1.5.f.3.b.f.5.4.c.6.8.4.3.4.f.2.5.c.4.1.c.6.8.8.d.b.b.0.c.f.c.0.b.3.9.5.4.2.6.3."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\058b77b9-7b11-4235-8b18-1725e27b629e.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):	162442
Entropy (8bit):	6.082647230960439
Encrypted:	false
SSDEEP:	3072:6K8A2NNCxQM9b0q+szv+tnMIKFcbXaflB0u1GOJmA3iuR7:L8rExQM9b7fD+ZMTaqfIlUOoSiuR7
MD5:	D675FE7CB3D9812D3882AFD796EC72B2
SHA1:	FF6F7E315E58B6DA1814644352825618BCEB69E0
SHA-256:	FD1F297E5185E06D0A25D5C44AF21E70A29F54C482C834D55769EA699665F167
SHA-512:	8B8002EB8AF80E7BBC5F3B867ABAE00790EC3912FF076CD7C416C5AC8A504F90D45CA32C030DCCDD6FB4DB234595406DF742A7DA443E9A4C0DB8B241E965B3F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\058b77b9-7b11-4235-8b18-1725e27b629e.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":1.605942124658599e+12,"network":1.605909726e+12,"ticks":97659647.0,"uncertainty":4288194.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\08935f9b-1148-4377-85f3-29382f741775.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96680
Entropy (8bit):	3.7513745293229643
Encrypted:	false
SSDEEP:	384:ybgYAflCsCimdRVOUD+NrrwvHN3AflcHV8GcLr2hbFcxwRx1ArqnmiliNzTTsOZf:St26llCasM8e78rprtJw3v+lKyAAAj5+
MD5:	3D7C9CD3FC5FC5830E647C7070D2FF38
SHA1:	EA7C004BD06EE4CA261221B78CECCFA3B48E1BD8
SHA-256:	341CB8BF079D59FDECB4C4A7E04D43EE26B1E76912902096EC7B3BD3084B9644
SHA-512:	F1847841234FF9353306CE91EA4F44245F3278A63EF30A9A9087DA8900F2D8C2947E6A338D08FA48B4CA6529777918AB2360891F76B701462DC41957D75310FF
Malicious:	false
Reputation:	low
Preview:	.y.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\174595ff-5b5e-410a-932a-c531a13135b3.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):	162694
Entropy (8bit):	6.0830786022883645
Encrypted:	false
SSDEEP:	3072:SHA2NNCxQM9b0q+szv+tnMIKFcbXafIB0u1GOJmA3iuR7:ErExQM9b7fD+ZMTaqfIlUOoSiuR7
MD5:	69B85EE48006357E28E13FC208FE780F
SHA1:	E8FB2A68A09A9D90E6D8F40627E794C00CDB3B16
SHA-256:	2A258908F88B608D59AEACB2D28764850D22687B8A24D520B5C6040E6BCBD4BD
SHA-512:	824F8F9AA261821450AC584BC3C2296A1E18942CA7573AC1E9CDDA63AEAC3D4D0FB7E30D52808807B20F2CBC958C93B0C5E3D18B283606368F27C79066CFCF
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":1.605942124658599e+12,"network":1.605909726e+12,"ticks":97659647.0,"uncertainty":4288194.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016053797"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\233de033-a5ca-4e8b-a6a9-acc4b5bc13ad.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):	162443
Entropy (8bit):	6.082648713246698
Encrypted:	false
SSDEEP:	3072:6uuA2NNCxQM9b0q+szv+tnMIKFcbXafIB0u1GOJmA3iuR7:furExQM9b7fD+ZMTaqfIlUOoSiuR7
MD5:	0F29E443F5EBA4579AEE55B910612378
SHA1:	5D1636D294BF8D52AE4DDF942D494D1378219364
SHA-256:	D3A0838DD1221E598755A28369D678167D6D1D6E820F76FBF1AE0134823FC574
SHA-512:	4FC82F090686B1DA91E1933B6A9731A9AF2183891BBD2CFC1BD308CAF06973F1C5427A58F2A4DA52820F81A1DA95A1E0C2B8EE74AB39D3252839377BADC84D5D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\233de033-a5ca-4e8b-a6a9-acc4b5bc13ad.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":1.605942124658599e+12,"network":1.605909726e+12,"ticks":97659647.0,"uncertainty":4288194.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\3ec07da2-964a-43d9-b79d-cc9e4cb83b42.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94696
Entropy (8bit):	3.751043935495676
Encrypted:	false
SSDEEP:	384:pbgYAflCsCedyD+NrrwvHN3AflcHV8GcLr2hbFcxwRx1ArqnmiliNzTTsOZRLNO+:B66llCasM8e78rprtJw3v+lKyAAAj5S
MD5:	029E81DA34A2A9E8C7089D41CE2B0CCC
SHA1:	B8A1483D309EE59FC98390C2B8E7220C2124CE30
SHA-256:	0FA34A7D57C9C23C7E4B1BE2CA118EF12459ACB398724B35DC7C31E4B0452B43
SHA-512:	03483794D3AF5D4ABC99FBF9B49707954C5014D5E8E49D16CC523520AC31744D89939153BB39EC2AB42530C096CAA16A685C69DF3E1E02C21745261651258078
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....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\85fc3b39-a83a-4f02-a91e-1a9abc8e69de.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97400
Entropy (8bit):	3.751232955362115
Encrypted:	false
SSDEEP:	384:AbgYAflCsCimdRVOUD+NrrwvHN3AflcHV8GcLr2hbFcxwRx1ArqnmiGYiNzTTsO5:It26llCakM8e78rprtJw3v+lKyAAAj5+
MD5:	D0D11E87EEF25B9D6E4D497FFB872C07
SHA1:	2B1A07C172DD35163F907B8180DDDC21F5ACD723
SHA-256:	61445DBC4FFAD0DE27BB85D60F05015E6571D11EE1B1E2B60C6A26DD3271AEFE
SHA-512:	8C0796BECE33853B406A921F9EA60CB86A807DE6FDFB205152D265E456A3C7AB26326E56388000542C2CBBDE099AEE5496D0EFED0C9078F9B5A0FBDF28BF0BB
Malicious:	false
Reputation:	low
Preview:	t|.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\8f0bc30d-bbf6-479f-bd97-049e4eaeba68.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):	162443
Entropy (8bit):	6.082646494490048
Encrypted:	false
SSDEEP:	3072:6QKA2NNCxQM9b0q+szv+tnMIKFcbXafIB0u1GOJmA3iuR7:RKrExQM9b7fD+ZMTaqfllUOoSiuR7
MD5:	F2ADF96847E0A8B9434D0D6AFFFFEA4E
SHA1:	1A5268AD4B7F377B5DA756AC2185CAA3F76748DB
SHA-256:	58A05ABEBEA801A730FAC701D7040C21C7C7D7498D001359B59B4292E18C4A79
SHA-512:	103E1973B05BE55F98C174A04D86F3639801F2926FB93024902451FE1F118C4B7517B38FDC6EB20785A34DF80A9BD9FA484DCBF82C772A73ADCF9A5886FB1C01
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\8f0bc30d-bbf6-479f-bd97-049e4eaeba68.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":1.605942124658599e+12,"network":1.605909726e+12,"ticks":97659647.0,"uncertainty":4288194.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\910ec822-a774-446a-923b-58fdec1c4f78.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):	162443
Entropy (8bit):	6.0826477984936815
Encrypted:	false
SSDEEP:	3072:SXgA2NNCxQM9b0q+szv+tnMlKFcbXafIB0u1GOJmA3iuR7:SgrExQM9b7fD+ZMTaqfllUOoSiuR7
MD5:	42DB97F72F21DE0469E07930BF9DE1D9
SHA1:	B31704FC20570DED5312FD59B67612EB5DD65B0F
SHA-256:	BF1E99260014CD8BE1373E9D844115836CAF4CF21FE56F8472821D017F109725
SHA-512:	35F2051B25F5A1A3D448BF6166CC0332C3A910B6504EE994140043700FF82737EC3F2236D11090E9AD4DF830D6A78C7DF5F13196AA0B7130B1156005D7A773C1
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":1.605942124658599e+12,"network":1.605909726e+12,"ticks":97659647.0,"uncertainty":4288194.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016053797"},"plugins":{"metadata":{"adobe-flash-player":{"displ

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):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2aa3bb6f-4943-4b34-b430-fb8c3a6e69c5.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):	3379
Entropy (8bit):	5.586824665332237
Encrypted:	false
SSDEEP:	96:JjNtKYoUnUEUyUUYUNN8yUBeU7UT0U2LmU13KUSLUwPeU9UEOUUUUUD:JjNtgUnUEUyUUYUNNNUBeU7UT0UVUJKb
MD5:	26C50755F4B16B62194B7F26E83D4922
SHA1:	14D590E4F008D6D8DAA96DA01E29BC5288417704
SHA-256:	371F58AE739BA14C7420E63BF0F4EBFF94025A50C73312AB3B0AF8B766482CD5
SHA-512:	57B4871E8E6F51FF27B607B1CC471E3D613056279DEB40F6BE4F34F4385645A8D17E10814C7BFEAA1B12E13FAAFA0970A55DD31B12C0DA7C017EE320CED269E0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2aa3bb6f-4943-4b34-b430-fb8c3a6e69c5.tmp

Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606546940.14427,"expect_ct_observed":1605942140.14427,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606546965.680003,"expect_ct_observed":1605942165.680003,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"i6EzVJ0YOuFitKi1H1fJOhaYEje1+rp8Ha8Wptqbs9U=","nik":[]}],"sts":[{"expiry":1637478148.071604,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1605942148.071609},{"expiry":1637478140.284505,"host":"BWcRzD1rdb9DyxV7WYSJDw+D13HhObs/0NAgU0+PWE4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1605942140.284509},{"expiry":1621722140.144263,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\316a5d9f-5b34-448a-be79-08e6588a464a.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):	22612
Entropy (8bit):	5.535507131761424
Encrypted:	false
SSDEEP:	384:f/YtTLtOoLlG2pJXrm1kXqKf/pUZNCgVLH2HfDTirUBKHGuHnT4Ko0J/tkk4f:fQhEoLlGoNrm1kXqKf/pUZNCgVLH2Hfn
MD5:	F61AB5A1FB9AA6FA44F6FD34292D13E5
SHA1:	B6E235855B7EF32F8E33F1A1F1D20DBD912B26FA
SHA-256:	E662EE8AE3D045DA67C8F804DE6124866801433C459ADBD5B790751FA8CAC3AE
SHA-512:	9086DF634770B903B9543AF2CAD1951AFCD07CD9D36DA53A0BA044F6AC389B14AFF517F537A76A794EC4638D8DFA1390F367C37561B6CD4806EDCDEF25B1A34
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":"13250415721966354","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\37e267a5-87e1-45e5-8590-088deeaf574b.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):	5679
Entropy (8bit):	5.177772960716545
Encrypted:	false
SSDEEP:	96:nS8V7iC4D5bZ7p8cVHok0JCKL8ow2kW18tbOTQVuwn:nS8IC4z7p8co4KG2kWe1
MD5:	C8D69136BB97F24F2BD342528ED16D44
SHA1:	2A59FF368B4DF93AC990E2F15240BEFDA9B9FA66
SHA-256:	099619E70DDD46B6E713337F144D3EF1C478CEB23F40EAFC5B3072E0AEFF3E35
SHA-512:	37182895CA7BBA83DBAE0717EA35F0A58B98DFE3D310E0240ED5C952E1172EE0EEDDA2F6F79AD8C6DB13E66A314CFCD2A6F31AC3FE45700CDCAFA85CB0D9111
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250415722189180","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3af1a4e3-fcba-41eb-9ee4-ed2233ae70fd.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):	5631
Entropy (8bit):	5.178790471218498
Encrypted:	false
SSDEEP:	96:nS87biC4D5bZ7p8cVook0JCKL8ow2kW18tbOTQVuwn:nS86C4z7p8cB4KG2kWe1
MD5:	1B38EEA9352F6F8F24F1CFBE4D800B81
SHA1:	26BFA2242F9C9D76E112F172E494D7AF71442CBF
SHA-256:	6E7B7559D3CD3E05A8F3A48866A362BE7F1AE119504ED161CBDF5285DF38668A
SHA-512:	E38A13B03B2182211E1BCF741A0F53F2C1DB1D41C8C7CFE3B57D644322ACFAC5F58684AE5497D995423994588B186AA3FF12FD205CB15F07F82FC2C25BB3346
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3af1a4e3-fcba-41eb-9ee4-ed2233ae70fd.tmp

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13250415722189180","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3e4c45d0-a654-420f-9b6e-70db56b368b3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	5239
Entropy (8bit):	4.850037918993215
Encrypted:	false
SSDEEP:	96:JOCXGDHzQvmJ4TbiRAyaMwfop6RGppmeFEE96p55HFK83AozRck6DgxViu1i+UVt:JOCXGDHzQvmJ4TbwAyaMwfop6RIpAE9z
MD5:	0C459D52180C7158111133677F8293EB
SHA1:	BB3576E605B0460B021ED9DCBD2F812F1E4F7B38
SHA-256:	3284296CCC28B3E8C7088E1F4C9BCFE158629BACD513EECF6998252F91B29CA2
SHA-512:	1A1C4E2E195293C7A7C40343A3CF9F8044F23EBB41EC1B0A405407D69A1D4813AB7F9F4540EA4385904781A1332F396E145E79B8C7FCD870DF8EBE2D579E9D5
Malicious:	false
Reputation:	low

Preview:

{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253007724503620","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253007724533242","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253007724718991","port":443,"protocol_str":"quic"},{"advertis

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\68462b93-fdb1-4b66-a19c-8de8601b71e3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5707
Entropy (8bit):	5.180720727591055
Encrypted:	false
SSDEEP:	96:nS8FCgiC4D5bZ7p8cVuok0JCKL8ow2kW18tbOTQVuwn:nS8gHC4z7p8cr4KG2kWe1
MD5:	3026E323F3227C3CEF66EAB8C23900EE
SHA1:	F1EA71D51E067B4854DFD0482607C127A5ECF6DC
SHA-256:	75898F7E2DABEB1CFADEF496DDD131EC48691A52A11D876FDB730F8A208D5180
SHA-512:	5EAC259065C088FCECA72FEAE531A1D1FAB40ECA69FA94BBE7632B47E58CEC729237B8B8B61951547C168E088AA73DB063A4DA8DBDD29903248B4D6F630713BD
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13250415722189180","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6cc68452-46b2-433f-865e-2078f344bfd4.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):	5680
Entropy (8bit):	5.178087399034418
Encrypted:	false
SSDEEP:	96:nS8F7iC4D5bZ7p8cVVok0JCKL8ow2kW18tbOTQVuwn:nS84C4z7p8cm4KG2kWe1
MD5:	F607B1E8CEEA53A6045F611231C8C81F
SHA1:	C44E46234AA1355FF3D7AF3370EC90BB94FB4B3E
SHA-256:	721B27183C9B7285881A78DF534E127041CBF78AFA905C4BB63EDBBC4F07F946
SHA-512:	D6428A84696D3C9955924911CDE5934CCA9CE0C6583AD0BA7B27049E15502A8096D3F4B3EBDE7C52AE54842F5915343437725861A67E2280B47037F7D0840827
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6cc68452-46b2-433f-865e-2078f344bfd4.tmp

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13250415722189180","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7a3d6950-20cf-47dd-8fc1-27ec1e6bbcfa.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):	5680
Entropy (8bit):	5.178133661895999
Encrypted:	false
SSDEEP:	96:nS85l7iC4D5bZ7p8cV5ok0JCKL8ow2kW18tbOTQVuwn:nS82C4z7p8cS4KG2kWe1
MD5:	804DA4F3498C7FC2531B6F3CACB32D98
SHA1:	44D2AEA1D8E199810F5CDC8A676DBA6C37C86034
SHA-256:	FA6286A63F7886582CD8187104F6C82535A827C9BE6D9DE2BE4191E95919F3FF
SHA-512:	2C38DF42ACF2B7AA09F81AF5D45F614722CD530DED8B429342C17BE50B38BE513D68948F22F4D6601894A2CA927835CAE79C5988D62D682D9BCDB21D6765F7E D
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13250415722189180","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7dca2324-0762-42fa-aa87-27e7dc26b4c8.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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low

Preview:

{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\845380e7-b065-4c56-9c2a-2a442fce6c21.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):	3379
Entropy (8bit):	5.586886485646753
Encrypted:	false
SSDEEP:	96:JDKYoUnUEUyUUYUg8yUCeUCUI0UlLmU13KU7LUyPeU9UEOUUUUUD:JDgUnUEUyUUYU6UCeUCUI0U0UJKU7LU4
MD5:	A728CDE94D9996AFB57A896924FFF7A2
SHA1:	EA59AFC799347A8B129ADDDCBB5CEE2F3ED80E08
SHA-256:	7173ABB6E6277F541DDD139DCC4FE922955368FA00A04DE51FB7BF4433896452
SHA-512:	38451ECF25657721EF2C0E1AAEC9C9535B9A09048D3BFD1D0762236D9E24A408BF43C2E7F32C9510D971518918AB3FB91588F2C48FA5C2624EFF113101633DF7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\845380e7-b065-4c56-9c2a-2a442fce6c21.tmp	
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606546940.14427,"expect_ct_observed":1605942140.14427,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606546976.190463,"expect_ct_observed":1605942176.190463,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"i6EzVJ0YOuFitKi1H1fJOhaYEje1+rp8Ha8Wptqbs9U=","nik":[]}],"sts":[{"expiry":1637478148.071604,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1605942148.071609},{"expiry":1637478140.284505,"host":"BWcRzD1rdb9DyxV7WYSJDw+D13HhObs/0NAgU0+PWE4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1605942140.284509},{"expiry":1621722140.144263,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.155774061144442
Encrypted:	false
SSDEEP:	6:0UUUE9+q2PWXp+N23iKKdK9RXXTZIFUtwHUQn2WZmwyHUQCh39VkwOWXp+N23iK1:tNE9+va5Kk7XT2FUtw0kJ/y0L39V5f51
MD5:	042898FEF01F63EEF0940FCB9CEEE27A
SHA1:	642B728421FB580DAA951BD3BEC6189EA0B45F28
SHA-256:	E4CDAF2351296214809843B22BDF6C73AA6317D27D739FE673F1BB0F0C134CA2
SHA-512:	E30F2C0E0539316EBF2F1B9EB1A6959C6CAFA44DFC93BE6FCE5560062E96E04F6C08CE0B5A4C425FF696202A30634AFFCC9BDC2582960DD46D4C32D7DBDD08C
Malicious:	false
Reputation:	low
Preview:	2020/11/20-23:02:07.114 140c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2020/11/20-23:02:07.152 140c Recovering log #3.2020/11/20-23:02:07.153 140c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.137248993832362
Encrypted:	false
SSDEEP:	6:0UkL+q2PWXp+N23iKKdKyDZIFUtwHUI/SzKWZmwyHUgLVkwOWXp+N23iKKdKyJLJ:tkL+va5Kk02FUtw0I/SmW/y0gLV5f5K1
MD5:	BBCE732B76E99B2C4F1707C61F85E051
SHA1:	2604FFD0159EA6BD5D56FF253E503F3C4DC1F9BF
SHA-256:	683B8F84818EDCEC949B08B5B345CCCBB6F375283747BA78C316AF60AABB2953
SHA-512:	DEA43D2DE0CB780B3102D9AB7B1E6087408A4607CFFA60FBB46E8B3FE0D22AA7CD9CB9C260428CA26F53D23A4C7D0B003235FDF895DCDC08CC432D623CE7F24C
Malicious:	false
Reputation:	low
Preview:	2020/11/20-23:02:07.104 125c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2020/11/20-23:02:07.107 125c Recovering log #3.2020/11/20-23:02:07.108 125c 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\001b7dfda48b5f6d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	829864
Entropy (8bit):	6.0574786631987205
Encrypted:	false
SSDEEP:	6144:7iXX6AAscbdCoDDhDkdSXf6jqrNB60/TF51UDDpGW/E+VjQy4wMEnzoB:eXqAZC9p8eMcmDp5My4wMEnzoB
MD5:	F3EAC19AF2A5B82DDDA6A76F85757FCD
SHA1:	FA241C62B3679CEA317ACCA808EC481381185FFB
SHA-256:	9FD882AF7858DBAF1F9E75B5EFB682893D4464608E03C02785FF55306B10A79D
SHA-512:	A5B6C60751A983B8BD85BF6B31F7F51ADF80CA5B460A503BF064FF1F9B6B1917CEB812A59DE68C4C8436C69AE092EB6BF25F4D67E3A057A28FA5318BC27C4596
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....LJ.....42236B44E112E764AF7E535F4FED12B2F182B78050A8D73EE34CADF128F75423.....'.....O.... .....R.....`E..(....d..x.....p..... .....|.....l.....P.....|.....H..... .....t.....d..... .....D.....l.....P.....p...h..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\02454aa6d8da3fb1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	606
Entropy (8bit):	5.516077594916151
Encrypted:	false
SSDEEP:	12:RJlhl5liLX3DpTJlhl5lcJNcrTJlhl5l6tEK3A87:RNlSzDpTNl+NATNlm3A87
MD5:	B845FB1D18FC27E32F8923AF5D3A9D8E
SHA1:	AD94E21A1332AD875D56B1733387D36B477E3B6D
SHA-256:	E55B33084EAC069CB9C14EFC6D678DB49BDBB6C9778C7B0814444B0F25835F9C
SHA-512:	8E6F7DA0EDE9F776C2813BDFB168EEE41440EDB33D1FFC4B8FDD789EB030AFD5F1D96672A5F566F17D8827BFCCA95CF11B8391CD734366152F3B5C0AF873C0 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F....._keyhttps://js-agent.newrelic.com/nr-1184.min.js .https://godaddy.com/.._.../.....u.....m..B.%.]y..t.k.1.....x..A..Eo.....t.....A..Eo.....0 \r..m.....F....._keyhttps://js-agent.newrelic.com/nr-1184.min.js .https://godaddy.com/.$L.../.....t.....m..B.%.]y..t.k.1.....x..A..Eo.....i..}.....A..Eo.....0\ r..m.....F....._keyhttps://js-agent.newrelic.com/nr-1184.min.js .https://godaddy.com/8..../.....$.....m..B.%.]y..t.k.1.....x..A..Eo.....$*.y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\041e202bfc772cc8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96664
Entropy (8bit):	5.817541273500728
Encrypted:	false
SSDEEP:	1536:9AcvuhYf5Ey+8NhnbgKGyEQ9lWhGbJ7h9h4WCg3n3cCp:puOWyTbgKGytlrJVvnC+n33
MD5:	B620F85483FBAAB5999827000CAA055F
SHA1:	EF555C2B99EDD30079497D4A5D66E1486BDE9E2A
SHA-256:	BB1AC8E5BFC71FB268671DCD90B889F3EC8FFC53CFA1C823CD42702E6619408B
SHA-512:	825729D93849B2CA469E9A6F3C9A3ECC4392F8FD94A2D6857FCBBF86CCEA430B1C6D97C0FF44177ADCE76B0CE004AEB6F28F124C10E5CB420E6ABFDFD3221 F3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....z....AE8CA336DD3BB037CCAE2DE0844B15BB3405AF03760159AA8A2B8773C21270E2.....'..R....O!...@x....U.....\...."..... (..... .....l.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....j.....Q.@...2....module....Qc>..f....exports...Qc"..G... .document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa..../...I.....@.-....PP.1.....A...https://cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/j query.min.js...a.....D`....D`....D`.....M....`...&...&..!.&...&.(S...."..`.E.....L`.....Rc`.....(.....M...Qbvdx9....d.....Qb.6."....e.....Qb..|.....f.....Qb.....h.....S...Qb.5.....j. ....Qb...U....k.....QbB(X.....l.....Qb.....m.....Qb.B.....n.....Qb...o....o.....Qb:fR:....p.....Qb.....r.....Qb..T.....s.....Qbr.._....t.....R....Qb.....v.....Qb.L.-....w.....Qb^h

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\069eeec3b24f9036_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	281
Entropy (8bit):	5.683219220817051
Encrypted:	false
SSDEEP:	6:mW89YcBB8LjFkevPXQICACJePRiNEaMVXqZgXgOach+KSxAS2nK6t:sgnNHXxCACkpiNE9VWCn0KSxw
MD5:	EB421FDACEB74398B4217FA48FEBDBAB
SHA1:	A588CCE6E510D375F73D6D24D81C13921EF18D98
SHA-256:	06110D1394E07BF29FC9E83700F676982A6370EA4EB455987DE1C8DC71193F24
SHA-512:	1100ED7D607D3625D4EED5F57267368553C5926232558E0DD96463401D5725F47B4CF5F205809D02577AD6A81BADB7B999C3BB8B10E9BFD7014ABEE502BFEE5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q..U...._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/engagement-window/window-confs/2498374730?cb=lpCb47203x54892 .https:/ /godaddy.com/...../.....R.....?x.wV...p.....3..U.<...M.M...A..Eo.....#.S.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\08b95bf8e6dd7b84_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.3850181538767306
Encrypted:	false
SSDEEP:	6:m2yYEpEFXwKVZqZf+1l/gf/G+Zux9hnK6t:BOpEFgKVAGHuODp
MD5:	F8B6968C3F83936A0F8922803F96775C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\08b95bf8e6dd7b84_0	
SHA1:	225BC0DEFAB8DFE04F3F4D4293D66A85F1E34950
SHA-256:	4DFDCBAEBF142E0086B2A3A5FFB20C1543DA34AD4038B94842C198FFA92A6543
SHA-512:	1884A3289767C1DA718151CD3D00890332746350CF1472CB0106FB8EA8F40CE5D48753A891CA1226B9843F504B66082BBFFFD49376E09920D6822C4FE8793418
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F....._keyhttps://cdn.trackjs.com/agent/v3/latest/t.js .https://godaddy.com/N...../.....j_:...hO.+.Oh..XbL^.g7..$....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\094e2d6bf2abec98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.912747592888139
Encrypted:	false
SSDEEP:	6:m3VYyK08fNH1DbgufyL6xK6tNr81WJvCyL6:aKjfNH1Dbffyqf8wT
MD5:	7FAD9BE66667D9BB9E92CA13D6A3B8D1
SHA1:	7A3CF2B9D977C96019974F1A8785CF9ABEA3DFF0
SHA-256:	2682A19C7E4EC7906BB3701115B91EAC134A8DBE609C9D9F95153675ED1BB238
SHA-512:	49868FF23A1E8B50AA0884B90B321FAD11E6D8DE84783A074D399DAA902F76D1E639424523E5525CF570856706228A01D65BFDD60319AC6026672525196FFEBB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js .https://microsoft.com/m...../.....=.z-.7.K]..~..=..9.....8...A..Eo.....n..... ....A..Eo.....m...../.`...B8979D834762C8C9E520D553EE7C0514437D7937B56D7BCF4A63DCB620DA7901...=.z-.7.K]..~..=..9.....8...A..Eo.....j..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0995e489bf59c488_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.880867250500899
Encrypted:	false
SSDEEP:	6:me4YvP/grLa/MNrNqZwLXgYHkYcP3OjvAioZK6txpHmVQOrWotlUnCcP3OjvAhGt:ZP4C/MNgwrBs3OuTRytl63O
MD5:	6C34687C8A3D10F094E03BD2AD432416
SHA1:	9981D56AB5933EFD4ED442570BFC10638BEEA930
SHA-256:	723F2D9B27BEE098C9875E22B12BAD2B8187D53DC9C63914B81E918C2E59E4D7
SHA-512:	4B7530AB43BA36D94A707A9E26543FA43C872BD298273748810F02DD34EFE91CAA621B863243206B304A2915A5332FD9B4FA7479C7BD3A2D5A0195BF26F3A6C6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://img1.wsimg.com/liveengage/v2/tag/3.2.2/liveengage.js .https://godaddy.com/s.^.../.....y....>;...t.t...|.Z.W.s%..Y.!..A..Eo.....Jm..... .A..Eo.....s.^.../.P...3E6C8EFD78826B30C5613D1F230C159A9CD6F42578ECDB3C9369F251C9A32C68.y....>;...t.t...|.Z.W.s%..Y.!..A..Eo...../...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0ad5e255cfc99a9c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	104456
Entropy (8bit):	5.793943614662255
Encrypted:	false
SSDEEP:	1536:m6Q61RdpFraD31VWxwU5sJPImcmbEunVXNP8zNKLoBOOSj+qkq8:CS+VIwDJPIr0nrP8JeokLj+D1
MD5:	AD9F00C36B5820974A4CBFB43C3D17F2
SHA1:	990B60FF8CA774A5B167445438494CE34D3853E0
SHA-256:	4ED40F1CBB712AC645A8324DACE0543C5E1FB5F690B6DC7702E72C8F9E3A589E
SHA-512:	864417B1234FA0869117CDFC9E8193B2004B63623C2BD4031C5DBD5CEDB175BA1A5B172BE12D189C43FAF31EC5C4E42D9AACB399EFE4B3FC1219EF2F3501B6 AD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...}}.....B8979D834762C8C9E520D553EE7C0514437D7937B56D7BCF4A63DCB620DA7901.....'..v....O#.....E.Ni.....d....&.....`..... .....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....N.....Q.@F.&.....module....Qc2.N.....exports...Q c.%G.....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa....!...I.....@.-....HP.....;...https://ajax.aspnetcdn.com/ajax/jQuery/jquery- 1.11.2.min.js.a.....D`....D`....D`.....]....`....&...&..!.&....&.(S....&..`8M.....L`@.....Rc.....8.....M...Qb.....c.....Qbf.7K....d.....Qb..;....e.....QbBi".....f.....Qb>N.n....h.....S. ..Qb.%L.....j.....QbJ.%.....k.....Qb...D....m.....Qb.k~.....n.....Qb.....o.....Qb.N.n....p.....Qb:B.h....q.....Qb*. #....r.....Qb.....t.....R....Qb...K....v.....QbBg*.....w.....QbJ.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1056dc81b557cff9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1056dc81b557cff9_0	
File Type:	data
Category:	dropped
Size (bytes):	184184
Entropy (8bit):	5.882662836070553
Encrypted:	false
SSDEEP:	3072:ozbBXxNFlTqktd+NfVN9DOXxu4PkWtVqINBpS4k:oBXJ36fVUL3Pfk
MD5:	EC9BC35A7E804BEEA087087B328E8532
SHA1:	C83DEAB047DD219B96E0513A786A96F529073D6C
SHA-256:	FE95B356968A209AD2BD7F1A287F555BF737ECC2E3691D5F171063CB349F9391
SHA-512:	C9D28D97CFC0A5F29BCE46F75F02C8564A8FAA07F9F6B8F07B5CCDBCD570928CF37C31EBA33A3774CD6330878AD3D940B5701693E2430069F509BC6E91903D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....j.W....581A25197F6D2EAD7CA81ED93ACB886D8CA4DB364646596AA97432AA14C60E1E.....'.L.....O9.....y`.T.....(..... .....|.....(...|.....$)..@.....(S.<..`4.....L`.....(S...`.....L`.....Q.@>..f....exports.. .Q.@...2....module....Q.@.....define....Qb...o....amd...QbZ.S.....tcc...K`....D. .....s.....s.....&.\..&.-...%..O...s..$...&.(.....&...&.|.&.'..[.....&...s.....&.\..&.-...%...\..&.- ...%.....(Rc.....Qb.6."....e...`....Da..... ..f.....`...p...0.....@.-....TP.A.....G...https://img6.wsimg.com/wrhs/e099922f63ddb7a5d4027821f53ee78f/tcc.min.js.a. .....D`....D`....D`.....`....&...&....&.(S...-..`.....}.L`.....@Rc.....Qb.....r.....Qb.B.....n.....Qb...o....o...b.....I`....Da....L\...(S...`.....L`.....A.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1532d62772683cf2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	364
Entropy (8bit):	5.8394204896527455
Encrypted:	false
SSDEEP:	6:m886EYcrJXjdEGGWUPPEWqZxugkkIuWUQ+9K6tW2pAdNTJgEYBGiluWUQ+0:LrsrZ/O8lU7kIuWUQyo2pAbujuWUQ
MD5:	EB781874F9AB68320FCD379AAFE2AF87
SHA1:	79AF0EEA45BB3615530B68DF08461371761409B2
SHA-256:	D3E88925C9C319CD6C04E81338A588D7B64E6D673B4CB649EB9716EABBB76FFE
SHA-512:	DD3B887D345774E6876344D2B7EE86C4744514469FB5EEB905872240949F60561262276C852D1D95DCB607F83264F735513EFDA4097660D55180F5BCB6700939
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....2....._keyhttps://img6.wsimg.com/wrhs/bb838831e66ecc31c8d4d38593364457/vendor.min.js .https://godaddy.com/.HR.../.....`.....R.S<....$.. .6: 8dv.....A..Eo.....x.....A..Eo.....HR.../.x...74F8F1B50BB817AA990DB0FF617AEE54C8FEB6E9C0E897EA85B1BDDF147ACCFE...R.S<....$.. .6:8dv... .....A..Eo.....b.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\183955bae54e77e3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1350
Entropy (8bit):	5.653184720864661
Encrypted:	false
SSDEEP:	24:puHISYkPruHISWX2rjruHISSYbruHISGTruHIS9GH:i3YkPo3WX2no3Tbo3GTo3EH
MD5:	6B9C884C519C0510C57A71B93953DCBC
SHA1:	D3915FD5BEA492D6E4B967F86B927BD5401268B0
SHA-256:	F7A789FDEB88A9C40D5EF1E7F8617E52485E40A3BCBAEF49942BE5F7454CDDFB
SHA-512:	833A5159BE6B95D2C6D5DDEF24E3A354CD1EFEC46DE3CCA3B24ECB4F5F9384C37CCB7735CCE31F720941032C6912690BE4C4F66577BFE84AF861555CEF9335 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....2r....._keyhttps://lptag.liveperson.net/lptag/api/account/30187337/configuration/applications/taglets/.jsonp?v=2.0&df=0&b=1 .https://godaddy.com/..\.../..... .....c/J.....|..A...5&.....A..Eo.....,w.....A..Eo.....0\r..m.....2r....._keyhttps://lptag.liveperson.net/lptag/api/account/30187337/configuration/applications/tagl ets/.jsonp?v=2.0&df=0&b=1 .https://godaddy.com/...../.....c/J.....|..A...5&.....A..Eo.....:.....A..Eo.....0\r..m.....2r....._keyhttps://lptag.livepers on.net/lptag/api/account/30187337/configuration/applications/taglets/.jsonp?v=2.0&df=0&b=1 .https://godaddy.com/...../.....c/J.....|..A...5&.....A..Eo..... ....A..Eo.....0\r..m.....2r....._keyhttps://lptag.liveperson.net/lptag/api/account/30187337/configuration/applications/taglets/.jsonp?v=2.0&df=0&b=1 .https://godad dy.com/.4..../.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1cb141e79f5601dc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.613258549101889
Encrypted:	false
SSDEEP:	6:m6PYcBB8LjFkevPXQICW0ZSVCaQqNpqZSbl/getP8IMLrZ0K6t:vqnNHXxCxqCahuEhP3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1cb141e79f5601dc_0	
MD5:	4AA459BBB108D7824844E1935A1BC60D
SHA1:	39EC2BB689F1FA7987ECD4E44AA9675A6410BC03
SHA-256:	5B8F559F0A0628BD1F4685A4098C8FB918B0109762161C2BA2E1A84287401535
SHA-512:	B271FC4FE1C58E07D996321FEC8EBDB755003CD5165A5EA9ED7004BF7682F3B56A068C9EEB698F041ED8FD23FD80F5512785372DCBCD29D001BC095679DE40A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.t...._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/setting/accountproperties/?cb=lpCb50778x35525 .https://godaddy.com/...../..... ....."".....2-...D.W.g...`..x..\<\.A..Eo.....X.T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1dcc732920861c78_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25385
Entropy (8bit):	5.597449426204349
Encrypted:	false
SSDEEP:	384:CWK5TvvnbqVMDUNNLOcwGWx/j4frBWqtY4GhP/Enqt5/wOdcnkLBBnRZVHc7JLeE:CW0rn+V5XOczW8ZGhFztFPyLUw
MD5:	18D5C2C7D16F4B62CE20A607DE80B018
SHA1:	7129F1F3C8C7F3BFCDAE9238F2DF7AEBE91AC18F
SHA-256:	891E3278678B7667DC25129647A06E9A5416E3BC6C43DFF66057F1BF602105B9
SHA-512:	4C8F0EA482C56A02DA77E2EE6FE3311335290F6A75380A1674B952F5936E1FA219707A64E3EEC86D8C58B06DFEA3C2D8039762AC29683E8DC3056898CF0BBBD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a...c..]...._keyhttps://img6.wsimg.com/wrhs/19613ac22420404c34b7162ef50370cf/tti.min.js .https://godaddy.com/>.].../.....4=.G..=f..k.U.=h...sT...w..T. .A..Eo.....A..Eo.....'..[....O.....a...p5.....(S.<..`4.....L`.....(S...`.....L`.....Q.@>..f....exports...Q.@...2....module....Q.@.....define....Qb...o....amd...QbF..c....tti...K`....D. .....s.....s.....s.....&.\..&.-...%..O...s..$...&.(.....&...&.|.&.'..[.....&...s.....&.\..&.-...%...\..&.-...%.....(Rc..... .....Qbr._....t...`....Da..... ..f.....`...p...0.....@.-....TP.A.....G...https://img6.wsimg.com/wrhs/19613ac22420404c34b7162ef50370cf/tti.min.js.a.....D`....D`8...D`..... ....`....&...&....&.(S.]..`p.....L`B....@Rc.....S...Qb.B.....n.....Qb.....r...b.....I`....Da.....(S...`.....L`.....A..$..a.....C..QbB(X.....I...H....a.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e3d5cdfef0b6238_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.3855446275476595
Encrypted:	false
SSDEEP:	6:mlmXYAykwLWyEWqEXLXgKmyP7rufnK6t:2uip/XLX+yPIp
MD5:	A11FCD3D5CB12DDFE8EBA192CA293E7D
SHA1:	C600F190C2758685BF0DC03A5AADB2FEEE7FD8E9
SHA-256:	B6A4B13AE5BBB85FAC7E4105DDF8F4EF0047FCE8B6CD0887D0E458D621F3E7B8
SHA-512:	E6D3E509DBDB69C00B9542EDB8DA8537D2ECEE4ADE05754F534A3EC46FD9E49D675CE08F6440F2E4F3EBB8244E0A495EDF6138C7263DB61DB8294A56FEBEE26B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....:sc...._keyhttps://faxfax.zizera.com/lite/assets/js/app.e1f1e969.js .https://zizera.com/f.f.../.....W.....R.M.|.@v...E.....v..K.5\.A..Eo.....ZV.:..... A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\308b6aa73c0feee0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.545792738540494
Encrypted:	false
SSDEEP:	6:mgqEYvPNr/bKX8QQVrqZhxz/gjvM11LQ/K40h/ZK6t:4fPNzbGQVKhxr+U11EYhr
MD5:	FDE6B5B0D11AFDD1CEDA0A7CB8A7A13F
SHA1:	2B77EE62A6D732DE5F258B7142B2DDDDAFC25696
SHA-256:	B427DC74B91D71752307A605392389DEE1604CF147249999BAF5134F1B7941CE
SHA-512:	D4DB2DD05CD24D6C5974966D8569055086C22826585EEC1C24BA6EC4DCA93A1AB7313D5A52A2F3F84986827BC5B5927C73D49ACC0786D7D9CF94FE7C758910A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\308b6aa73c0feee0_0	
Preview:	0\r..m.....c...:.AB...._keyhttps://img1.wsimg.com/dc-assets/help/2.379.18-d325e66/js/flamingo.min.js .https://godaddy.com/.Z..../.....x.....0\Xw.Ns....._l`./e..A ..Eo.....RQ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\31754e45cfd28c3a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.568946246220943
Encrypted:	false
SSDEEP:	6:mfgVYGLKdXNQKwkE7ENCugBa/ikR7sa6Gs4rw7DK6t:EhNQKwkEAVEa/7sa6Gsv
MD5:	FFA099E8864ADDEEF4F98F96ECB3A97C
SHA1:	BCAE63CF05DA442087EABD3DA0DB2CFB4AFEC6A2
SHA-256:	2527F52982EE9D55018B27DCB86FE4FFF0B424F94373C931C7123A08DD2955A1
SHA-512:	7040DBA45B3CEA8B04F74B9E950163A2A9C88ADD7F97953A1074244739A45D45F9D76EAE5C888B5F1FB3FF35798B778007AC1AD3CD70648B00D1426D4F92226
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....._keyhttps://www.gstatic.com/recaptcha/releases/UFwvoDBMjc8LiYc1DKXiAomK/recaptcha__en.js .https://zizera.com/T.j.../.....$.....h.j..YN `.pd/`..I....2|-.....A..Eo.....N.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3332cf6ef51dd1a9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2344
Entropy (8bit):	5.941195127893168
Encrypted:	false
SSDEEP:	48:xaM1EW+MFF4h4e0rEkH83olGZMUHiOHrnzSnCKVNH8:x3Eiq4eAEkH8YkZMUCAax8
MD5:	38241E2B18DE3A5293052FEA2AAB4C07
SHA1:	97DAEA082A852E4EBEF83A0251B18B0166BA1237
SHA-256:	1A641768E7708364226ADA604C5E5C3BF6FFDA5F877944FB43FD054F4ED2B290
SHA-512:	5BBED80CBCDC80E38DBD389EF4E906C748B2BA504A9B57D64CFBC0FC26695144EA2333F7FC42AF0F225DDD530D55231920B5846385F2D925DC1ED4E08D20A C1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p...S..J...._keyhttps://tags.tiqcdn.com/utag/godaddy/godaddy/prod/utag.1355.js?utv=ut4.42.202011101205 .https://godaddy.com/c.].../.....,.....gB..z.G .9....W.....A..Eo...../fu.....A..Eo.....c.].../.....'.....O.....p.....(S.d..`..... L`.....(S...`.....DL`.....0Rc.....R..`....I`....Da.....Qb..%%.. ..utag..Qb...o....o.....Qc:.le....sender....Qbnj.....ut....Qc.....loader...(S.....Pc.....u.loadera....e.... ..f.....%P...I..A..@.-....dP.....V...https://tags.tiqcdn.com/ut ag/godaddy/godaddy/prod/utag.1355.js?utv=ut4.42.202011101205..a.....D`....D`:...D`..... ...`....&...&....&..a..D&.(S.-...`.....LL`'".....Qb.J.0....ev.....:.....a.....Qc.....base_ur l.DQ...j...6...//img1.wsimg.com/liveengage/v2/tag/3.2.2/liveengage.js....Qb:m.....data.....Qb.ZG.....GV....QbV.X.....map.I..Qc>.[(....split.....r...M..4.a.....9...Qb.....src. C..Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\406a0f0498fb7a87_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1290
Entropy (8bit):	5.48977877271737
Encrypted:	false
SSDEEP:	24:Bs6Qtc0bfLs6s0bZrLs6U0bI/NLs6tU0b1Ls6BI0bjLs6ahYc0bc:BsnDLsE9LsIU1Ls+jJLsWfLsRio
MD5:	AF080B044CFD1149D2E1C6C8D3B37433
SHA1:	309FA9C0CB6E82B9D08575071A3DE371DCC8B167
SHA-256:	BA8FC6262064C2F16CD2789EED6BF2DDB9E3918EC0212724C4467FE69822F827
SHA-512:	651726279793361E039FD5441FC58B7CED5B16A4CAEA2E90BE2C7A35C00B6603EACF85EE46D7E665F0E546D7BB87ACEA86A4CA5586CAE0D007261A6C6A5D7A 09
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....aV...._keyhttps://tags.tiqcdn.com/utag/godaddy/godaddy/prod/utag.js .https://godaddy.com/d.Z.../.....H...N...[..]..<....|...1.G5Q.A..Eo.....1.m.....A.. Eo.....0\r..m.....S....aV...._keyhttps://tags.tiqcdn.com/utag/godaddy/godaddy/prod/utag.js .https://godaddy.com/..I.../.....H...N...[..]..<....|...1.G5Q.A..Eo. .....Nc.8.....A..Eo.....0\r..m.....S....aV...._keyhttps://tags.tiqcdn.com/utag/godaddy/godaddy/prod/utag.js .https://godaddy.com/...../.....N.....H...N...[..].. <....|...1.G5Q.A..Eo.....QC.....A..Eo.....0\r..m.....S....aV...._keyhttps://tags.tiqcdn.com/utag/godaddy/godaddy/prod/utag.js .https://godaddy.com/...../..... .....H...N...[..]..<....|...1.G5Q.A..Eo.....n.....A..Eo.....0\r..m.....S....aV...._keyhttps://tags.tiqcdn.com/utag/godaddy/godaddy/prod/utag.js .https://godaddy.com/. ...../.....H..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41735a75d71fff99_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41735a75d71fff99_0	
File Type:	data
Category:	dropped
Size (bytes):	508
Entropy (8bit):	5.634810983574212
Encrypted:	false
SSDEEP:	6:mnYbLjFCsWLqLUqxYy6cUqUqZwugAloFYWIrNhK6tWnYbLjFCsWLqLUqxYy6cUqr:ln3WOxNjloAjn3WOxqJ+Hvloo
MD5:	795CA504DE9F9B381835B2F46654327A
SHA1:	6B5717C548FD8C68781D44F861910D361B604711
SHA-256:	7B27EE55B33B3B38D37A50FB4E439F6C2428AF27211A253DA12FEADE6E37392C
SHA-512:	E3E0705512DE758FFB10A62B37157D2DAAF98FF1FEE251739CF3C6D38EE210743EBAEEFABAE4A9D6BD8B89A9EE67941032FB17080D9FFD806CB6BE0BF754FE77
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z....[oG...._keyhttps://lpcdn.lpsnmedia.net/le_re/3.43.0.1-release_5028/jsv2/overlay.js?_v=3.43.0.1-release_5028 .https://godaddy.com/...../.....-.....O...c...y..v.....x....].[t.9...A..Eo.....;.....A..Eo.....0\r..m.....z....[oG...._keyhttps://lpcdn.lpsnmedia.net/le_re/3.43.0.1-release_5028/jsv2/overlay.js?_v=3.43.0.1-release_5028 .https://godaddy.com/.K..../.....`/.....O...c...y..v.....x....].[t.9...A..Eo.....~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41c17cabcb7066a9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	361
Entropy (8bit):	5.8225168451961355
Encrypted:	false
SSDEEP:	6:mROYET08NuILZPMQWqZkXgTlISJbcGthK6tzRHURu00RFE/SJbcGR:mig8Nu2pMQlW+F7fHuroFEip
MD5:	7D9072DBF39FED1676F0A14A279336F7
SHA1:	E5BB600BDDA53B2E55ADC383ED2C3CE0E92968CE
SHA-256:	A1CDFABECD48083FF938BC592291F8AEA623D654A93E1A717B03F6BBBCBB3EE8
SHA-512:	BA76813868D5C39877ED0A12FABCD4457EBAEDD6FA79E45403D05B0C05583C28639991FB305247C83EDA389F7FC904EEEF09644730513F71438D80FDE6FC9A8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a...G.'....._keyhttps://cdnjs.cloudflare.com/ajax/libs/babel-core/5.8.23/browser.min.js .https://godaddy.com/.%Q.../.....a.S'a^^3.. ....`.'..H.1U.Xc....A..Eo.....^.....A..Eo.....%Q.../.....42236B44E112E764AF7E535F4FED12B2F182B78050A8D73EE34CADF128F75423a.S'a^^3.. ....`.'..H.1U.Xc....A..Eo.....eb..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\47ccc19b4da77a8d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	273
Entropy (8bit):	5.676999400708114
Encrypted:	false
SSDEEP:	6:mFYcrJXj1goUT/jWxkhBYYqZq//gil4xtK4ubK6t:orZioUJoXY5iKHN
MD5:	CC252EDB370819E858962A1B2F353321
SHA1:	4D4D9330996937BE12912C8F85C27DCAD3227DFE
SHA-256:	E04579EE68423F06AA44E7C4F590B9CDDA1339D2403DB82236C7119596B2196C
SHA-512:	305B4C54076AADD1262BC4C3F14CA2DABCE38BC6EEEBBDA5B21DE6BE02D6A6952ED4B917B6B5D0C107F22B66069FD803579044CC8B325974C96DB9542B1933B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....4..t...._keyhttps://img6.wsimg.com/wrhs/3fab94f367d4871640366242ebfff587/vendors~browser-deprecation-banner.header-chunk.min.js .https://godaddy.com/u...../.....U.....$cl0.....)\!}.....W.W....p..%.A..Eo.....m-;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d6125cbda70b6f0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.637455831773555
Encrypted:	false
SSDEEP:	6:mkYcBB8LjFkevPXQICW0ZSVCzqZ0rl/gQnlof16iJn7K6t:YnNHXxCxqCSctznc6iX
MD5:	0ACBAD443D3D603C895E67B12D1B431A
SHA1:	8EFE9D906D796BCE63767A51E01A83EEA216D62E
SHA-256:	BA45F66B18DD91FDD752A4E8E45B185AD00FB2424983DBFA53F96FB822985344

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d6125cbda70b6f0_0	
SHA-512:	19F97B62FEFBC6D7888DD3CAF5D70BA5DAAE036AE0ECB8E182AB760899724B1C2B44F258FE985E13D7994178D690937A6E6C594C752728CBF6C6AE736FB9CA D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....'....._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/setting/accountproperties/?cb=lpCb49098x80101 .https://godaddy.com/V...../..... .....f....kY.....2...`...P.....s...A..Eo.....F.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4e7ced3c9971ec86_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.873498736692149
Encrypted:	false
SSDEEP:	6:mUMIEYcrJXjaVNdNGlIQcuIQWqZEHugvlS+oFcI1hEnK6tpCo1G6PRihUrGRUn++:pMBrZuV7HulEOgsF51Weo1VihUfF51t
MD5:	780F55A750552581E27FE0F2BB976F0C
SHA1:	491AC25611871E07988D87ECAACED98106E54619
SHA-256:	5D3F8CBD894D8E58D75BAFB045943402A652CA46E8A6B02D6C78A27F83E11CF8
SHA-512:	FEE90E10AFEC3773BE88F4016E9D896B6AE7C4673CA3EAC1A636DB0700859B264FFB0A6B1863A9DA0F502F626D8AD39A77C9C7B2FD698C8CC2441A4E0AEAD F2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...Q....._keyhttps://img6.wsimg.com/wrhs/2a8723002f286c722aab4069a3c0bc9c/utilityheader.min.js .https://godaddy.com/JIR.../.....Zy...O..G.... .e..T...r.!..C..mZ.A..Eo.....9^.X.....A..Eo.....JIR.../..`..24392BC5F34EDB802D4C2D65221530B19ACCFF47BC1064C2AA8DB9E2C93CB1B4Zy...O..G.....e..T ...r.!..C..mZ.A..Eo.....6...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f0802021d44bc50_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.953077041471363
Encrypted:	false
SSDEEP:	6:moYGLUxGBzQ2c7MNXqZkyx/gtcZSJjKY1K5tlhK6tRfhEUCoBFaCMEZSJjKYe:qGBQ2cIokKOdhKNJ7Hfn6CyhKn
MD5:	E5317F28EE91FF19F27678BC285FE99C
SHA1:	B418C4EA56EABF5B52393AA1411731CB658E67EB
SHA-256:	F697A8FFAD614703E6B8BC9E87F07715BFF46C2EB9F54CD647A4BD41765A7C48
SHA-512:	4D3994E2905B054327E07718736EB4AFEB7C3BE301D8A7CEBD77FF77DE5593CDBFF765B7C40E715FF8B2A0F65B36025417795E8C8B98808E6587542099D3D543
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i...../...._keyhttps://www.youtube.com/s/player/8b85eac2/www-widgetapi.vflset/www-widgetapi.js .https://godaddy.com/1...../.....(..)....L.l.9Y..~..n6x?7 .V.5.K...A..Eo.....#../.....A..Eo.....1...../.8'..CB915ADED5410A148D1F11EB69CBFBE0151BF2F4E4CE4C633D73CA26FAB6C9E1(..)....L.l.9Y..~..n6x?7.V.5 .K...A..Eo.....\...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5100317373070f9f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	280
Entropy (8bit):	5.713196422981179
Encrypted:	false
SSDEEP:	6:m4YcBB8LjFkevPXQICACJePRiNEPBFWqZi8g8n/lT9SQ9+4zRK6t:InNHXxCACkpiNEP1i8jtIQ9+Ur
MD5:	B72E6AFA4513975D25DD78B1D2EE7AA2
SHA1:	C0F6638C88C9D281610A9717D379F787279F4A6A
SHA-256:	7973855E7297A59F6401176E5ADBDDBA1CDDD04F9062F6961CDFF412B2CB13F6
SHA-512:	CE9F30404F08B7BBEB74712081F2BA9933827294E55A865E6F2838BA8C4F6894C16C822AB36DD2B9C1FCAA67304F77F8483FF31211EF9B0B6F2E65EEAB436D77
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k.Y...._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/engagement-window/window-confs/2498374730?cb=lpCb1326x77678 .https:// godaddy.com/^...../.....!0.....k. ..I<{o.zX..w.].h..|k.....A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6745a26ff250e255_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\6745a26ff250e255_0	
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.748737573243358
Encrypted:	false
SSDEEP:	12:SnNHXxC8mTieu3TPOQchvVAdXOhknNHXxC8mTieu3TPOQchvVAhLKh71:qNHIUNGQRe4NHIUNGQM91
MD5:	6A3E5879356BF637EB06CC0A247233EA
SHA1:	4F2FB9E6C0B68BA19DCB017B7E64A149A0DF6CE1
SHA-256:	F013DE021C17DD23FBCA71F12D35AEFE5422073F859566BB315398B4B1A401DD
SHA-512:	7137BF725F7331D6C81E21D77B4528A9CA58E7C7D3C5E464C1168954C6F4B7AEA7C7E7BBAA1D106D4D9B306D62FA4F6D8B80A7491CCE090A0053435188E5186
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m.f...._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/le-campaigns/campaigns/1741658530/engagements/2498565930/revision/12748?v=3.0&cb=lp2498565930&flavor=dependency .https://godaddy.com/^...../.....RP."Qd;..o...`L.....(...v.....A..Eo.....u.....A..Eo.....0\r..m.....m.f....._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/le-campaigns/campaigns/1741658530/engagements/2498565930/revision/12748?v=3.0&cb=lp2498565930&flavor=dependency .https://godaddy.com/...../.....~/.....RP."Qd;..o...`L.....(...v.....A..Eo.....9I|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6dc6a15fa209a9ca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	75744
Entropy (8bit):	5.690974092522406
Encrypted:	false
SSDEEP:	1536:rMouQCd0v/IPFkQB7KCn88wLh4qu4u/pvj+qk1:rMos0YVeC4wpvjU
MD5:	76952B33FA130BA2DFF00AF6A073C485
SHA1:	68B48D0CFCCF61C540AE02A9B4F540FE4252505F
SHA-256:	15795716BC9286371341BBD1DA74E048453B9655A152CB0D89139DBB9BA6D94E
SHA-512:	6B63A2BFEDE7BD07CC0E053CD752FB3A7D0C07085CE8AF1D4180A4165AEECBEA361BDF350F92D02AEB3642E458F77C5BA27CE28983CFBD57048DEA4446C8A145
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....CB915ADED5410A148D1F11EB69CBFBE0151BF2F4E4CE4C633D73CA26FAB6C9E1.....'.....O.....&..J.SA.....-.....(S.<..`2.....L`.....(S....-.`.[.....L`.....m.Rc.....Qb...L....aa....Qbj.i\....ba....Qb..8[....da....Qb...r....ea....R....Qb..d.....ia....Qb.0....ja....Qb.....pa....Qb..o.....qa....QbRJ.....ra....Qb...3....sa....Qb.=.....z.....Qb.(.....va....Qb..Z....wa....QbzT.....xa....Qb.....ya....Qb...@....Aa....Qbn.Yg....Ba....Qb..6....Ca....Qbn..X....Da....Qb..]....A.....QbJUt.....Ea....Qb.'.....Ia....Qb..*.....Ja....Qb.C.....B.....Qb.).....C.....Qb.c#.....Ka....Qb...a....La....Qb.....D.....Qb.G.....Ma....Qb.dD^...Na....Qbf.....Oa....Qb..6.....Pa....Qb..b.....Qa....Qb.....Ra....Qb.m*j....Sa....Qb.s.r....Ta....QbZ..|....Ua....Qb..8.....Ya....QbZ.%.....G.....Qb._w.....Za....Qbz&.2....$a....Qbnp.....ab....Qb..l....bb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\702495c6e2e78b0c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.567188857539359
Encrypted:	false
SSDEEP:	6:myPYcBB8LjFkevPXQICW0ZSVCQbqZZHg8m5aXHH4mK6t:7qnNHXxCxqCQ65jf/
MD5:	5480A44A766006594E4F98C678BA06A9
SHA1:	ED7455C080A7627EFFB05F05C0C681801393F4BB
SHA-256:	DBFDD8A6B69A367908C73194E32BCD66EDAAA4767792D7FE9BB68CD6E9686618
SHA-512:	EE213A18FA7CD0AB81D05A60399D4377CCED3FA8AE8328FF5622E8D67358030CA0EF74A874E09EA17480CD8C7DEDB9962E39B163F89695E7232D2563F41D7BCF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/setting/accountproperties/?cb=lpCb44690x57785 .https://godaddy.com/kJ..../.....d/.....rs.NauU...W.ELCk.~6...?.;...8V..A..Eo.....?z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75f1105a42981b97_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4711
Entropy (8bit):	5.570404169118136
Encrypted:	false
SSDEEP:	96:JxQ83x6rzdCbApWuXtLa6lQvD28mguVX0N7Zmrp4:U8IYqWWRh8mXVX0ZM4
MD5:	0B24EB8B3A08176D0631C4C772A82532

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75f1105a42981b97_0	
SHA1:	437EDB6C32352896ABC0EC7D83D8C75D03282755
SHA-256:	C842938DF904ECE53CB60748DA7D2C5475719C57AEC0D81FED5B3410BDF81497
SHA-512:	E22166261ECD040B71291B35B71483D28C5536FEF16F3E2D595E352BEFC0AB8391EA2BD12D87A541D1BF33F6E339C9620645960DCEB65E44D4E7284EBF46EC8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...^29...._keyhttps://img6.wsimg.com/wrhs/d6c7b1acb132140b70d61ad9ce6bc527/heartbeat.min.js .https://godaddy.com/..V.../..... .....0C4.?{^...-.S....d.5)..A..Eo.....[4g!.....A..Eo.....'.....O.....s.....(S.<..`4.....L`.....(S...`.....L`.....Q.@>..f....exports...Q.@...2....module....Q.@.....define....Qb...o....amd...Q.PF.M.....heartbeat.....K`....D. .....s.....s.....&.\..&.-...%..O...s..$...&.(.....&...&.|.&.'..[.....&...s.....&.\..&.-...%...\..&.-...%.....(Rc.....Qbr._....t..`....Da..... ..f.....`...p...0.....@.-....\P.a.....M...https://img6.wsimg.com/wrhs/d6c7b1acb132140b70d61ad9ce6bc527/heartbeat.min.js...a.....D`....D`....D`.....x..`8...&...&....&.(S...`.....LL`"....@Rc.....Qb...o....o.....Qb.6."....e.....Qb.....r...b.....l`....Da.....(S...`.....L`.....A..$..a.....S.C..QbB(X.....l...H....a

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\762ca5cdd3b40fce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.8582972076242825
Encrypted:	false
SSDEEP:	6:mpEgEYET08NWQA82qZYUXgTPM/gGXUm4B7K6tqKLU820bdZZiWgHM/gGXUm43:ng8NWQ9FYUXgPMoGMAUEMoG
MD5:	5FCDC98323170CC5D1BDDF30070E0B1E
SHA1:	AB160D153DF7B9D7C8EA7627E71EA751BEC8B7FC
SHA-256:	EEE89826FDBBB0F29A43CD486806DC41E2AE60300C738738E16376F48625BD16
SHA-512:	0F9508018A2D4838F87DC8179AB115754C18B2AAE83290E66D628F6DEF7C5B094828AE3ED3E0DBC62648298F9372834AB8B38E603182B32C0AEDD35DFC7E594
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[....b...._keyhttps://cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js .https://godaddy.com/..Q.../.....S.....E.b.....{q...)..AE3qL.".2_.A..Eo.....j.....A..Eo.....Q.../..x..AE8CA336DD3BB037CCAE2DE0844B15BB3405AF03760159AA8A2B8773C21270E2.E.b.....{q...)..AE3qL.".2_.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7f58cad8484a3ffb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.633693075627269
Encrypted:	false
SSDEEP:	6:mqPYbLjFCMuqlTWlN7dJMzQLncZUdOO4XO7TqZk99/gSxLQkMEok9Km4lXK6t:XynfjlkPSc4RkWknDrrlA
MD5:	2772A2690318D95EA1F1972587FD0058
SHA1:	8E14A2F8C8EA5F7856F6352445EDB6EA011C2F63
SHA-256:	7F72C14B5F4AFBCA3FAF9D7B6F1856E2B7F0C7893984A88BB296FD66BB4964E9
SHA-512:	C12F7EC29FEF48377AB44F31645508F46462CAF8B72DAFFA62AFB7EE271983665A3301482660EAEFC55EAA695A0FEF896382EAB4DB25E4BEE65B9A9AEF87734 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w....._keyhttps://lpcdn.lpsnmedia.net/le_secure_storage/3.11.0.2-release_5036/storage.secure.min.js?loc=https%3A%2F%2Fshortener.godaddy.com&site=30187337&force=1&env=prod .https://godaddy.com/1...../.....z.....w..Lhrn..q.nv.+r.'<...E.6J8ba.A..Eo....._.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\80e4f13fb63695ca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1425
Entropy (8bit):	5.654362369493448
Encrypted:	false
SSDEEP:	24:sNHIxlGNHIh6SGNHIBVGNHIV9zGNHIPgp:sRmGR8jGR2GReGRoy
MD5:	02C6137091BD29A9A273DB4230614A1B
SHA1:	D48D7F32352054DF4E1945C9DB2154B9FA3CEF59
SHA-256:	F7F3D319D50CFBA006043B3DAC60462FE5119E448622928A4787AB4DA788F96D
SHA-512:	A510C47AD9FD02C6B683193C5ED1213A201A861EC8C6E81671BEC82A911CF6DE92490BB6F3A0AC15ECFB871BAF209C643E78C8C677B5E90F9AF4C95EBF9C6 D3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\80e4f13fb63695ca_0	
Preview:	0\r..m.....L....._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/le-campaigns/zones?fields=id&fields=zoneValue&cb=lpZonesStaticCB .htt ps://godaddy.com/.a.../.....6t..@.6.6....D.....t.A..Eo.....BUt.....A..Eo.....0\r..m.....L....._keyhttps://accdn.lpsnmedia.net/api/account/301 87337/configuration/le-campaigns/zones?fields=id&fields=zoneValue&cb=lpZonesStaticCB .https://godaddy.com/8..../.....,.....6t..@.6.6....D.....t.A..Eo..... .....A..Eo.....0\r..m.....L....._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/le-campaigns/zones?fields=id&fields=zoneValue&cb=lp ZonesStaticCB .https://godaddy.com/...../.....2.....6t..@.6.6....D.....t.A..Eo.....J.#D.....A..Eo.....0\r..m.....L....._keyhttps://accdn.lpsnmedia.net/api/a ccount/30187337/configuration/le-campaigns/zones?fields=id&fields=zoneValue&cb=lpZon

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8c4ebfa60d7b4172_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	342064
Entropy (8bit):	5.688334961201765
Encrypted:	false
SSDEEP:	3072:1VebTPNHkhKd48OkEse8moNPlnAr97qyKTzRNwlXE:SkUd48Okuto/U7qyKTzca
MD5:	0EC37A38005566C7BAE8497FD0F2748F
SHA1:	B2295907EF12D110E8D650EDECCE5AB9BE1FCC60
SHA-256:	F2D394E2582D72D8705C1D0669257694985994C07D6ED71E4B436F7768EF11CB
SHA-512:	AB83B5D7000FA8478E0458699CE5D815A639CA9ABA0E75F085AF04E65629CD325FC5E4C1BF1F746696D3B11775182ADBB7157C6821BB6705C5CFC8C236F5DC0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....#....BC1B85D43568E43D3631AF3AA30C77D3D098F01B4FEA04EB67E4B78EA6C5DE98.....'.$A....O^....5..y4.....\|..... .....2.....4.....D.....<..... .t...t.....(S.<..`4.....L`.....(S.]..`n....HL` .....Q.@>..f....exports...Q.@...2....module....Q.@&.....require...Qd.e.P....prop-types....Qc.Rf.....react....$ Qg..%1....react-transition-group...a...Qd.....react-dom.....Q.@.....define....Qb...o....amd.....`.....M`.....a.....A...Q.P&s.....PropTypes.....Q.@.1.>....React.....Qb.._.....u x... Q.p.....ReactTransitionGroup..Q.@J..h....ReactDOM..K`....D.!.P.....s..[...s..T...&....&...&.]...&....&...&.]...&....&...&.]...&.(...&....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9064f3a5056d6bb1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1055
Entropy (8bit):	5.585766300613777
Encrypted:	false
SSDEEP:	12:FEynt7sefMNRHEyn5HdfMN/u7HEyn2fMNXHEytbIfMNTHEywPlufMNr:FAekNRHT9kNOHQkNXH8kNTH+IkNr
MD5:	52F3AFD76A961CFEB82772D652214F0E
SHA1:	34444608117EEAC69A7ADD214600A3197E43FDB8
SHA-256:	C27A5D4FC6AE023E5673EF16E2BE1574625A6C179C9B0E2DCDA8CE0E2974B509
SHA-512:	621501D8E34E511371F9C2A3635FA891018A844F81D2B8EB6189EE4B9E66107F834D022EEE527D342BD9AA796E0E31525EE49D99FC112D756D861217027C0D51
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....D.T...._keyhttps://lptag.liveperson.net/tag/tag.js?site=30187337 .https://godaddy.com/.3[.../.....'.....*aI...R=.X."mIn?).-7%...:....A..Eo.....A..Eo .....0\r..m.....O....D.T...._keyhttps://lptag.liveperson.net/tag/tag.js?site=30187337 .https://godaddy.com/.9..../.....*aI...R=.X."mIn?).-7%...:....A..Eo..... ...!.....A..Eo.....0\r..m.....O....D.T...._keyhttps://lptag.liveperson.net/tag/tag.js?site=30187337 .https://godaddy.com/...../.....'.....*aI...R=.X."mIn?).-7%. ..:....A..Eo.....i..G.....A..Eo.....0\r..m.....O....D.T...._keyhttps://lptag.liveperson.net/tag/tag.js?site=30187337 .https://godaddy.com/...../.....g.....*aI. ..R=.X."mIn?).-7%...:....A..Eo.....>.....A..Eo.....0\r..m.....O....D.T...._keyhttps://lptag.liveperson.net/tag/tag.js?site=30187337 .https://godaddy.com/4...../..... .....$.....*aI...R=.X."mIn?).-7%.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\921a520646898d46_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5992
Entropy (8bit):	5.809363247850794
Encrypted:	false
SSDEEP:	96:tu4BB01Rf2YQ7MiEJPGfyb6oCBnahMmg/m0+46fU281u0NeA8dPnSzfAtvMYH:IRejCPhiNmg/x6U2yuQeA8dPnmfc
MD5:	7952CF9377D8CF8F0F6325F064458359
SHA1:	8ED9E1C569E37E6AA0D3AE529BFE5EC68B04B970
SHA-256:	7FA17F72595EC199EC4BBF017C87072165CC042438A5C2FE1736F42A8F7438CA
SHA-512:	99FF0743AD8283208C2BC3016A258D13822D7DF7A4D216C85299FE277159CB8A5F371104820A3448329DDD96CD05DD5112F312828A1D90C57BDCBB2488776A79
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\921a520646898d46_0	
Preview:	0\r..m.....x....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=42ce545a-d075-ac8e-38d1-8d9b4eaa1c7e .https://microsoft.com/.p..../..... .A.o.,.M#4.Y..<.iZ..m..M.`.Q..k'.A..Eo.....3.`].....A..Eo.....'..u....O.....MB.....(S.y...`.....L`\.....L`.....(S.....Ia&...m....,Qi2.$H... .ShowSelectedComponentKeyPress...E.@.-....hP.....\...https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=42ce545a-d075-ac8e-38d1-8d9b4eaa1c7ea.....D`.. ..D`....D`.....Q....`....&...&....&.(S...Ia.....,Qi.t.. ...SetRightSideNavigationMenuHeightE..q.d....).....&.(S...Ia.....$Qg..w.....ShowSelectedComponent...E.d..... .....&.(S.....Ia.....(..f.....-.....d.....4.....d.....-.....d.....!.!.....Qd..3=....ShowToolTip.E.d.....D&.(S...Ia....>.....e.....-.-..... QfJ U?:....AssignToolTipToHref.E.d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9812c157ee66a51a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.594744294919491
Encrypted:	false
SSDEEP:	6:mL/VYcrJXjE8Aj5RWG4DVeQWqZw9/gF8CcSv4rcJ/prbK6t:krZ48K7WGqrlwFUScJRx
MD5:	D5A69C11258CA47EDAFAC45B2C3A6790
SHA1:	BF2838CB96B60A836A40B7B62917DB7204F41C94
SHA-256:	6BEB9C5DC2F1672634C0B2409EE42F3CCA3485BEDFFADC8061D844774E6BE8C3
SHA-512:	9B3241FFBF9E1DA6A106A4C7046310BCB6F9B5556D76048A66A976FAD1ADF470FF17DDF87AD560700C8D6EF96D3FE8F5ADDC8741025F5FB24057E541103D5C1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...0O....._keyhttps://img6.wsimg.com/wrhs/a41f55bee6aa8d6c09469d7143ca4f41/helpHeader.min.js .https://godaddy.com/...../.....h0..z....o-.E.w.....] ..q.>..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a1898ca8587555c5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.578400994367433
Encrypted:	false
SSDEEP:	3:m+lJMQ+s8RzYAykKIC9/xWyWaWLnWRIEt9P/lHCRvIG3Zqqb9TdZmY1pK5kt:m7YAykwLWypGEfgRvIGpq1YDK6t
MD5:	82E6656BB695B039EE62765FF46C2C00
SHA1:	7F74016373B24D40CAA34181AF26D35B4463FCC8
SHA-256:	4F5ED65896F706C0E84122D669E4C3C1FDA4B5A04D4CDDC9FC6FB2503F39B792
SHA-512:	DC822D218AD0AC82319537393B5F466862D8FF5153EC87EFC4A2C584F8EF7E0D9B00570EE8A43B8A1C7CA7D14A56C7D72CC6D5716B78807A1A0143D56E856AI F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[...".....,_keyhttps://faxfax.zizera.com/lite/assets/js/chunk-vendors.753f9ae2.js .https://zizera.com/..f.../.....b~.4..,_.DR.<..6.0.1.w).T.X....A..Eo.....^.. .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aa261b7c4be61a46_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	508
Entropy (8bit):	5.664232406720629
Encrypted:	false
SSDEEP:	6:mQnIEYbLjFCsWLqLUqxzZUqUqZ3+XHgCQViehn/ZK6tWQnIEYbLjFCsWLqLUqxza:rnILn3WOzMuf/TFnILn3WOzz8/lfE1
MD5:	2409043CDC437EEA37A5794CF805535F
SHA1:	6C600B63F24C527947BDC17918AF0C79E215BC9E
SHA-256:	0B31F4930F99ECE3F8125C4C6EAC03EE0A510F0A487CD8D84675456D2978F9E2
SHA-512:	39EFBF1753A88EBA5F80C4149BC9666548316EBABB9AAD093EE7B67BEF13627E836EE00EEBC82322E3BB1A4C0AD92CF89A43ABF0305ECB46D57C2A395F2C3 E88
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z..../.8...._keyhttps://lpcdn.lpsnmedia.net/le_re/3.43.0.1-release_5028/jsv2/UISuite.js?_v=3.43.0.1-release_5028 .https://godaddy.com/...../.....Qlf.x M.p..+p.....6.~8,....A..Eo.....@.....A..Eo.....0\r..m.....z..../.8...._keyhttps://lpcdn.lpsnmedia.net/le_re/3.43.0.1-release_5028/jsv2/UISuite.js?_v=3.43.0.1-releas e_5028 .https://godaddy.com/i..../.....50.....Qlf.xM.p..+p.....6.~8,....A..Eo.....Z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b1e45d6786b73622_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b1e45d6786b73622_0	
Size (bytes):	361
Entropy (8bit):	5.9347035068528085
Encrypted:	false
SSDEEP:	6:mRDYcrJXjAgJojdwMqZw2+gzYKypjLK4zbK6tqL2UUfCnu1Tc1WkVuCKypjLK4V:m/rZ8gijdGw5CKplIL2NfkMTc8kcwp
MD5:	8936349C4D0CB89BA7DF247083F16CD6
SHA1:	F2ACC28097774EC62596F3549773C6353469071F
SHA-256:	86446FCDCD45592825810216CEDE9F65E5605B09D21A80E624C3A456C6B126E8
SHA-512:	F1208B262343BF2C4D87E8F4B39FF53A64785C2CD18CFA0DDB8A74F5A3DE7CFDA3690489FA8E58C11B435338EC3DAE916BCB7BF8F4DB5B1619D246E042252DC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a...G....._keyhttps://img6.wsimg.com/wrhs/e099922f63ddb7a5d4027821f53ee78f/tcc.min.js .https://godaddy.com/..S.../.....J.B. ..g...$RW.w..~Q.;$.-..._<Z..A..Eo.....gV.,.....A..Eo.....S.../.....581A25197F6D2EAD7CA81ED93ACB886D8CA4DB364646596AA97432AA14C60E1E.J.B. ..g...$RW.w..~Q.;$.-..._<Z..A..Eo..... L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b8df2d1d558aabf6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19394
Entropy (8bit):	6.000229779466519
Encrypted:	false
SSDEEP:	192:dMqrvMfMldsgVefH6JM2roacbJvie80nZ4ODzFyfR8WQL3l5LWFRAUZo6iJOe/In:dM4Mfk+H6HVcbJvL8KlUZJDliGqKvak
MD5:	7F9D514A89FF1F88F32E2D3DBA3CBEB4
SHA1:	1324572EBA510F2CCA21D737EF90B3BEABC323CF
SHA-256:	A8E366157B0803F29B128B5C88E4ACF993E0D6937E3FCDCC376E9F00A432F9F1
SHA-512:	D259DCA56E38208D51E42DD285AD7EAB13D7A0A6D622F2E6DEB16D7A78F851BFDA61C8E3384840ACF8DCE54BA38F799CEF5AAC46CA108ED31E97FD88AF7BD59
Malicious:	false
Reputation:	low
Preview:	0\r..m.....wg.Z...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/b2-7087f0/ea-1a640b/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/50-f1e180?ver=2.0&iife=1 .https://microsoft.com/...../.....E..t1O...]"#.,a..;.....A..Eo.....u.v.....A..Eo.....'.R.....O.....H....H.....(.....(S.0..`.....L`.....(S....`.....L`.....LRc".....Qd.}.....requirejs.....Qcb.....require...Q.@..9S....define....Q.P.q.....__extends...d.....I`....Da.....(S..`.....L`>.....Rcf.....*.....Qb.k~.....n.....Qb*. #....r.....Qb.9.....s..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bb2286b571c6fc01_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.634302671843968
Encrypted:	false
SSDEEP:	6:my/PYcBB8LjFkevPXQICW0ZSVCYqZ02ugVLb72wozK4TK6t:jqnNHXxCxqCX02uQLO
MD5:	7BA09E2C9FD1E67B78B2D4368D644AB1
SHA1:	2EDD0B2B2C0FBA8441FF5DE4A59155D1A8EA2DD7
SHA-256:	ED628D0B8252A907EAED5D51E58148FFB533F4EDB6D03FD248CB3F0C4DE6D6D4
SHA-512:	26F186039A8EDD599728BD0FE3AC18EC7C9F4CB53A1FE8DE68CD5DA7710F81C9D2EEDCD7D01D4992553726B7AEF4CA6B9DD806F5745F318E4BFFC2C37C728C2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....&d.H...._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/setting/accountproperties/?cb=lpCb21250x95577 .https://godaddy.com/.R..../.....0.....>...'q.y..[GI..a.<.....!..A..Eo.....h.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c3de3858c26638d5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1248
Entropy (8bit):	5.71745280737017
Encrypted:	false
SSDEEP:	12:vLnfjlkPSF4RkW8jNuMtdBNWFLnfjlkPSF4RkWj2uuLuMtdBFFLnfjlkPSF4RkWI:vbeMVDWFbeMYujFbeMIDFbeM1U
MD5:	EA5EF979016EAAAACE25BB6C5D4F326C
SHA1:	69FC7428A95D2E3C3B8A6FA4AE2E3D0E716867C8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c3de3858c26638d5_0	
SHA-256:	4AF1A627DB37BEC25644A90A1CEE602A170A5ACA8F76CBE4B3FB994D0F483C1F
SHA-512:	09355C7738FEB0BA23B40DEED835D0B173F7624C6ECC832947E10BC0F8C03843D1706B8557EC249FAD5619A8B1B17DD06C746AA2F3FA4AE745DCD5B7DC74B6DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....0...._keyhttps://lpcdn.lpsnmedia.net/le_secure_storage/3.11.0.2-release_5036/storage.secure.min.js?loc=https%3A%2F%2Fwww.godaddy.com&site=30187337&force=1&env=prod .https://godaddy.com/)...../.....%.....n<`....^?!.)..p.J$.y.X....@..A..Eo.....).g.....A..Eo.....0\r..m.....0...._keyhttps://lpcdn.lpsnmedia.net/le_secure_storage/3.11.0.2-release_5036/storage.secure.min.js?loc=https%3A%2F%2Fwww.godaddy.com&site=30187337&force=1&env=prod .https://godaddy.com/...../.....+.....n<`....^?!.)..p.J$.y.X....@..A..Eo.....Y.....A..Eo.....0\r..m.....0...._keyhttps://lpcdn.lpsnmedia.net/le_secure_storage/3.11.0.2-release_5036/storage.secure.min.js?loc=https%3A%2F%2Fwww.godaddy.com&site=30187337&force=1&env=prod .https://godaddy.com/...../.....-.....n<`....^?!.)..p.J$.y.X....@..A..Eo.....h_.\.....A..Eo.....0\r..m.....0...._keyhttps://lpcdn.lpsnmedia.net/le_secur

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c487f9ceefa38302_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.6654748670429
Encrypted:	false
SSDEEP:	3:m+lszOK8RzYcrKSXNNWgIlYBOc7WFvDASqZD+v//lHCkn/240Vw3OhCIbn2oMmQB:mWnYcrJXjcYBOkOqZiv/gke9CYqK6t
MD5:	5AA13106E316D5E4016E9C08214DCDF9
SHA1:	CBF2F84F2E2868AD71A935DFCD3F94436B2E45D2
SHA-256:	FD8A57F888C58FD5997E64F0821AC66B44BA1F20BAFD85270D628D9459AECC10
SHA-512:	5755D1B8285395EAF312E424CB2E0BCA0508472CDE5237FA0F188B34A678F4053F6BF83D81EFB20E8B6F774BC2652F7D3F432306AE36693BFF8B13071C2E6F4D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l....._keyhttps://img6.wsimg.com/wrhs/5f1d295b85aaaba74af4ee02bdc62854/vendor~uxcore2.min.js .https://godaddy.com/m(..../.....0.].[0...+D..;.+...P.L.j.y.c.A..Eo.....$..h.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ca9e60488bdc5258_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	155816
Entropy (8bit):	5.977606134965258
Encrypted:	false
SSDEEP:	1536:U0CjM7SNeqJq2tEzOaZIDBml+pMXGN28iOwrp8EyX8IQrCRezHGgnNdK:z4US/Jq2CyY3WYVOK8userHjnNdK
MD5:	C8A215BD241D69CD59B6D1AE5B9D4085
SHA1:	C68582BA57C696B07197EA193A546A47A1C1FDAE
SHA-256:	3ED29B263B675EE61CA75DEFC6BC79C9AEB9B2A3432C1DBC077F2F9A3DC36CAE
SHA-512:	1084320F093C2AC74FAA5367E0B5741283F680CC4F9E71F47F8EF1F1688A71995630DA5DC0D9295E3E39CC817384D868BFC57EFC4DABD49C9FF65791727EDF5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....24392BC5F34EDB802D4C2D65221530B19ACCFF47BC1064C2AA8DB9E2C93CB1B4.....'.^.....O0...._.....H.....x...PJ.....H.....(S.<..`4....L`.....(S....`&.....L`B.....Q.@>..f....exports...Q.@...2....module....Q.@&.....require...Qd2k.....@ux/button...a...Qe.P.t....@ux/component.....Qdrl^.....@ux/modal....$Qg...$....@ux/namespace-component...Qd.....@ux/spinner...Qc^$;....@ux/util..Qd.e.P....prop-types....Qc.Rf.....react.....Qd.....react-dom.....Qd.XtR....react-intl....QdN.....react-trfq....Q.@.....define....Qb...o....amd...Q.`2.....UtilityHeader.....`.....4M`.....Q.....A.....Q.....a...Qb.._.....ux....Qc.....Button....Qd~..P....Component.....Qc..R.....Modal.... Qf..i#....NamespaceComponent....Qc.}.K....Spinner...Qc.....utils.....Q.P&s.....PropTypes

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d3eaba701bf0be20_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.592869736766436
Encrypted:	false
SSDEEP:	6:mF3YxwSEBW2PYuVrI8cwTqZN/gHYJEsOhJF0b4CxZK6t:ldoDQT8c9V6h4bxxT
MD5:	6052ABA9442DBE9F95F7F4AFD9567D28
SHA1:	997165453FAB21AD8EA13B4EC61601C8C4C8E65B
SHA-256:	E2D1E6598509EE9DC1447D8A21E20CFE2855EC2A8D477CDB1A0533CC64485A70
SHA-512:	2FCBE6220683AA2FFE877457DBE25652C83EC4C1CA42D5FF9A0229E584FEAB6490B6D4E1428DDC434818B882D4967FDF3FA71EF81E368A3B162CA7875EC9092 1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d3eaba701bf0be20_0	
Preview:	0\r..m.....g...5X.F...._keyhttps://securepubads.g.doubleclick.net/gpt/pubads_impl_2020111801.js?21068793 .https://godaddy.com/m...../.....".....uWwAvkOf4{ea.... ..q..,...}.8#.A..Eo.....R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d6862ab8bd2f679c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	365
Entropy (8bit):	5.934438679276246
Encrypted:	false
SSDEEP:	6:mm3YcrJXj1GDAXdZNkOqZylHg1h/vO6eblLrAK6t+Ltlx53V6agwHZNfkO6eblLr:7rZRGCHW92HwJvO6/Urvaw5lkO6
MD5:	D3C8A4B6EA10107DFD7C6C9BF5D8F516
SHA1:	E2C0C5B8EDE2383EA70C07CC3EFD78C1AE75BAE5
SHA-256:	2154E7FD63688883BF9B570D47141924450BD5D17248736B00007DBC0AF8D9A2
SHA-512:	BF538584FCCD78AC29809E97A45779F17A6A53E8BC149EC954CC0C4DC2CDD167ADA1045B1080328E8BAA2CC27B9938B3AD10CF008982656307D2A05C3EDA01 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e.....C...._keyhttps://img6.wsimg.com/wrhs/b0de8fce1ace6e77cf5891d58d0aafc2/uxcore2.min.js .https://godaddy.com/N>R.../.....IT....*...~....*Kw. ..O8X.1'>d.A..Eo.....\.YI.....A..Eo.....N>R.../..7..BC1B85D43568E43D3631AF3AA30C77D3D098F01B4FEA04EB67E4B78EA6C5DE98IT....*...~....*Kw...O8X.1 '>d.A..Eo.....k.iL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d8fbe577ab80525e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.6170244260848845
Encrypted:	false
SSDEEP:	6:mm0ZIEYcrJXjfZULVIUwLOqZuCKvl/gpYJ4JsvDR/ZK6t:0ZBrZbZ3D9ivtsYrh
MD5:	7538E0294263C1B2C4F120C09F772BA1
SHA1:	4F9B012A942CC2EF4F445F753AA56F3E7CF66A91
SHA-256:	8C534F3D436D781554047426E101A95E272312380064F482AFFDA313394565E8
SHA-512:	2DF7C5E783360D0E3DEECF16E24DBBEA0B01FFDA1AA7D68E71361D827062CD0FD35716896585C38205A15757D4B54367527B7975A362C3216E9D8F50F03C41F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e....u.F...._keyhttps://img6.wsimg.com/wrhs/1cdb971aba0e6f81bcd65741b66a16ea/uxcore2.min.js .https://godaddy.com/...../.....Q...N...M<qx5.). GtD.R.....A..Eo.....#sf.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e8081f3cea3392c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	61075
Entropy (8bit):	5.550092293831279
Encrypted:	false
SSDEEP:	768:yEKb8J5WWWrsVlfTZLF4+kE93WtLpEPnB0tp0ttzPkEZwQ4AZweLFqD:yEyIUQVlfTZLF44X/ytpAk8ZweLFO
MD5:	7549B686428B93DA7F56226281399A24
SHA1:	07F3DAB44E7230F30C877DA271B59A65C6C2B64B
SHA-256:	4F720591354D0E44D1CEBDE5F38D7FC696CE7FD930010BF112D1CC1E9F04AB66
SHA-512:	8BB3964F9F1C33937FC57ACA1E70EF089D0B69F4EFBC42E73E56CD1920B24D892924B828FC8FBC08B51EDC485F55F940F435E4EE1B5A42112BC14887706AE15
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{....._....._keyhttps://img1.wsimg.com/cms/sales/js/sales-cms-m5dfhHAYxYelydH0TOQilVeHUgw_6MEeM366phtlfb01.min.js .https://godaddy.com/..../..... .....>...J)B.g..t..A..B.....R.A..Eo.....>.....A..Eo.....'.|.....O.....v.....$.....\.....(S.-...`.....L`t....L`..... (QhV.S.....merchandisingPackageTagging..(S.|.`.....L`.....(S.H.`L.... L`.....8Rc.....Qb>..B....t.....S.a.....I`....Da4.....(S.....Ia'.....d.....Qb..1.....n..... !..@.-....pP.....a...https://img1.wsimg.com/cms/sales/js/sales-cms-m5dfhHAYxYelydH0TOQilVeHUgw_6MEeM366phtlfb01.min.js...a.....D`....D`....D`.....a...`....&...&.. ..&....&..A.D&.(S....Ia.....!.....d.....&.(S...Ia....1.....S...d.....&.(S.|..`.....L`.....(S.....` ....i.L`0....U.Rc&.....Qb.Y.....ee....Qb.....gu

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\eec5c79e2dbb46ae_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	134688

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\eec5c79e2dbb46ae_0	
Entropy (8bit):	5.943306648070785
Encrypted:	false
SSDEEP:	3072:Uz1MX10kqn23aDMcYXjkXyF607Y535J3Vu:DOnbXYXjFkcGi
MD5:	8CBD4C37F09F199211F98277257A04D8
SHA1:	153DBD8165BA392318C6C2A84C3A5B2707BAEAB2
SHA-256:	6D9F7F3EE20FE49A23F35B817C70998E49DAE33628A6FAAC3C4FFFCB9E746083
SHA-512:	D293C849408B2EDB362B2883656635F926FDABCC125945E1239417D648CD161AE07C931AAADD5B0A5CCA75CB5BE5A3E94C5BBD04D9F4867D53AB45B5B44613C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...8.q.....74F8F1B50BB817AA990DB0FF617AEE54C8FEB6E9C0E897EA85B1BDDF147ACCFE.....'..o....O-.....f$.....$.....T...T.....(S....`.....L`B....(S...`.....LL`"....@Rc.....Qb.B.....n.....Qb.....r.....Qb...o....o...b $.....I`....Da.....(S...`.....L`.....Q.@>..f....exports..$..a.....S.C..QbB(X....I...H.....a.....Qb..@Y....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%. 0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....a.`....Da@...8.....e..... P.....@....@.-....XP.Q.....J...https://img6.wsimg.com/wrhs/bb838831e66ecc31c8d4d38593364457/vendor.min.js..a.....D`....D`....D`.....`....&...&....&....&...(S.X..`l.....L`.....a.....e.....a.....G...C...K`....Dp(... .....&.(.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ef34c246df0e42bc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.6473659842518185
Encrypted:	false
SSDEEP:	6:m9tXYcBB8LjFkevPXQICW0ZSVCHTqZB/g1NuZCY9prljK6t:uCnNHXxCxqCSpwYCY9p0V
MD5:	C97AE38DD4BD10FA777934CA28A8814C
SHA1:	E6E63835712C98307416D72BCE1715F3069A3C35
SHA-256:	A3F5A1E4BC11355FA30270A98203354884EADD40551DE30AE7538F3E4E6F8D46
SHA-512:	719E7C017F613FB64608C327E5BBD578372A98A282181FA7E080648D71CB77E296F4711134E849E7B966553CF3CBD88A6332DBC19A5639E24A7590D28999FDF2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....*....._keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/setting/accountproperties/?cb=lpCb41535x45434 .https://godaddy.com/.Sa.../.....m6....cF...K....".. .(M;....Z.A..Eo.....^.^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f562afac76b4b973_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.564827461777375
Encrypted:	false
SSDEEP:	6:mvEYcBB8LjFkevPXQICW0ZSVCHuvqZBC+/goIdcm4rK6t:gjnNHXxCxqCHjUuL4C
MD5:	9AC9CAFD7967FFF73E865FDB8B00580F
SHA1:	B0D340224AD4F7D52E0DE0FEDBD6869121E61478
SHA-256:	F47083A75B68C499EEE3CE4B572FF771B55DAF4DD6B3BA60BB2EE7DE2D0DFF8B
SHA-512:	1F5DBACDD5D6C42513E2DF1E8ED147B35C98B7C4F42076AF03B829F60F521D056C4A62BA2168688D08CF9134CBFA72CC0640C8220B7A008B8B982FAD1F7682E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n".....keyhttps://accdn.lpsnmedia.net/api/account/30187337/configuration/setting/accountproperties/?cb=lpCb27407x40474 .https://godaddy.com/A...../.....z%.....Re....8..e.[.J..FM.F..v.e"z..o...A..Eo.....#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fce188cfb0287bd8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.388644163974561
Encrypted:	false
SSDEEP:	6:m0YGLSqfJPnZqZEBll/gHv/grQLu0SYHLK6t:hxvAE9mbj9
MD5:	617FEA6EC25A462071DC9583FBCAAD91
SHA1:	91BBCA5F60A2A5A149BD51A844DE77A701B4F9CC
SHA-256:	C8E297B873F5BB188BA6E0E729CF87C3EAC600C0164A4A443EB64F5762D6041C
SHA-512:	79B847213397B9359D11723B728DA217A43A33A8E144863D4835A8422352AB8198700346366730BE0FF4B6231E108FE72A6F20D6BD4D59DE4DAB94A3E3EF8E2E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fce188cfb0287bd8_0	
Reputation:	low
Preview:	0\r..m.....I.....<....._keyhttps://www.googletagservices.com/tag/js/gpt.js .https://godaddy.com/...../....."....*.V.....E##.....}.....A..Eo.....~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ff6d0be77341b55e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29125
Entropy (8bit):	5.766165040953499
Encrypted:	false
SSDEEP:	768:UVvsv7N/BUkcEu7LtUqJ7d/+pDvydV12xbdNRJ9DA:UVvspgEu7xUIV+dydsJK
MD5:	E9CD8F2193B4801DEAAF407F841054C6
SHA1:	99F5A4BD3C454E13D321319CC71DA4C3579CA146
SHA-256:	9CD23BC1F696FB9F6F1479B4D03FBD333D070B80883B45B17A5872E35FAFE9A8
SHA-512:	8B3ADCB02C36764CD8DC6A2B5CE57510E7E2CB1251C255B4025C63C21D41BA63C611AC80FCED63DA80709DA648285541450FF1F9C8A1CC34CC094125305A49 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<..5...._keyhttps://img6.wsimg.com/wrhs/dffbab4b36fb049029b7ac907a90f8c7/vendors~browser-deprecation-banner.header-chunk.min.js .https://godaddy.com/.aX.../.....a.....:it+..rO!.>(..2...m.A..Eo.....A..Eo.....'."i....O.....o....v.....h.....p.....(S.I..`.....$L`.....QcrE.....window...(Q...#3(....webpackJsonpUtilityHeader.....Qb.N.....push.....`.....L`.....`.....M`.....0Qj.y.."...vendors~browser-deprecation-banner..`.....a.....HQp.:6.:..../node_modules/@ux/browser-deprecation-banner/src/index.js..C.(S...i..`.2.....L`f.....Rct.....2.....S...Qb...o....o.....QbB(X.....l.....R....Qb.....h.....Qb:fR:....p.....Qb.....m.....O...Qb.L.-....w.....Qb..|.....f.....Qb.z.D....M.....Qb.....v.....Qb^h{.....y.....Qb...{....B.....Qb*^?.....F.....Qb.....S.....Qb...U....k.....Qb.....O.....Qb..4j....x.....Qb.....A.....Qb.....N.....Qb..}.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ffae120ac1988083_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	255736
Entropy (8bit):	5.736642358741171
Encrypted:	false
SSDEEP:	3072:WJMXBUixMAqke65jgL/Ghja7ViZ2602esos/AILYwwQUaF1x8:WJiBTxDXskoAw7cx8
MD5:	67BACF5B766C08A9DDB1A923654A2998
SHA1:	1942DBABF46B60B34E7092488E75703BC6CF080A
SHA-256:	9BE3D36468912E8FBDC897A67DDD3E5DE4EF0DCDB3128BF770854CCDF938710B
SHA-512:	BE885EE5CCFF1CAD038DC2E6478C9B44FB68E8D5F4CA1C5960DB0620C11575A993C996F19C3F61F3673F2054F09A995F18080DAE892E785C7114BAA1AF676F8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...W.....3E6C8EFD78826B30C5613D1F230C159A9CD6F42578ECDB3C9369F251C9A32C68.....'._....OO.....6n.....(...$.....l...`.....4#..|.....T.....t.....D.....d.....(S...%...`.+.....).L`.....(S...`.....LL`"....@Rc.....Qbr.._....t....Qb.6."....e....Qb.B.....n...b$.....I`....Da.... ....(S...`.....L`.....Q.@>..f....exports..$..a.....S.C..QbB(X.....I...H..."...a.....Qb..@Y....call..."..K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0..'....&.%.*..&.(...&.(...&.(...&..&..'..W.....-...(.....,Rc.....`....Da@...8.....e..... P.....@....@.-....HP.....<...https://img1.wsimg.com/liveengage/v2/tag/3.2.2/liveengage.jsa.....D`...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.3066939857505875
Encrypted:	false
SSDEEP:	192:dubJYwbd7pEnVORuwWUlTvwEsO7YnVOQ4d:UYwbdwMpWUlLwEsOSMX
MD5:	2142F7982A5EF577D35E760625EDCAAD
SHA1:	754E37F4F05D8F7BEB3AF9A14519B421B66B1532
SHA-256:	12487E0E679A7EAE9CF0C8740C3293D38A8D9AAA16026E45EC6A208A182BB6AB
SHA-512:	623A6AA4BF5B55757AB6E15776D6A80DF12F4A2C5777F5EE6FB77EF8FEEA1D6D94AB816FB481F3DCD6A6B5674CE265BFCC18D2911E2A474B38EF5DD44EB6D 02
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.873740670444313
Encrypted:	false
SSDEEP:	96:COPcNw0bCBJYw7BdON8oupEnLJOJEMNwn:COPcufJYwbd7pEnVOJEMun
MD5:	34B8F511DED4B7891AB13876290B76DC
SHA1:	EB7EECA1EB94C7A47FDD7EA06E108A7FEE70D3C3
SHA-256:	3F0E13755ABC3FCA96FA426A35A17157C315252C92BE2E23C1B197EF16BCB532
SHA-512:	6D6E3B02ACD9943172541F94DC4D9352D6B659410D213C7AFABF8965A0B89EA2A763CC98C785F7017660C0FDA1DD68B9835C06D4BF10B25FBD43945800FF192
Malicious:	false
Reputation:	low
Preview:	.....0.)..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	31205
Entropy (8bit):	3.3866644363923935
Encrypted:	false
SSDEEP:	192:3owKvQHM4N8Do+CLN4/7tV+FKr+lQ5/o+ZE+O5TrHOWfirW2E5/WeGFw4UCkcn7b:2QdFL+TtWJQhP/6a0e
MD5:	62FF9A87B854CECC0AB32C2DF9E9DD28
SHA1:	A3D795DEA6B13444DDCC05B068131E1209DBE008
SHA-256:	181306BBA546C8FFD850EDDC9BC78AFD903FA55B94BD9D22C4F9D610A9D5F06B
SHA-512:	09FE329FB12F47351458B3C61250FBBF948C881449A074A4EB45A8DD5FF84E32022C919080FD8E73724D39197ABEB8389EA326B7369F234CC48F837F2E81E0FB
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...cf68a14e_5639_46ad_97fb_8837784b980a..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....*...https://faxfax.zizera.com/remittanceadvice.....r.e.m.i.t.t.a.n.c.e.a.d.v.i.c.e. .-. .f.a.x.f.a.x.....h.....`.....my.....ny.....0.....\...*...h.t.t.p.s.:././.f.a.x.f.a.x...z.i.z.e.r.a...c.o.m./.r. e.m.i.t.t.a.n.c.e.a.d.v.i.c.e.....`.....X.....0.....H.....`.....p.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....N.o. .o.w.n.e.r.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.148645944794037
Encrypted:	false
SSDEEP:	6:s8ZAVq2PWXp+N23iKKdK8aPrqIFUtwVjAgZmwyVjAIkwOWXp+N23iKKdK8amLJ:d6va5KkL3FUtwv/y95f5KkQJ
MD5:	85164477CA20542895B2B2A94F331E82
SHA1:	6DD9E7A7B31C8942FB882D0C9FFD9EE2E5F4A56F
SHA-256:	88323A2B24F8E4849710210A5D785C0C308A82D779BA707981D3C56FC706F8C2
SHA-512:	27D44A4DF48CDD6F46BFDA4A196D8C1FAB4BEEFE5D83283DB3250259ADA43ED1162FB6FCF7D59CA8FDB6A9653C57CBEB4FDD13AB59A850370D2DC03CAB5 41A6
Malicious:	false
Reputation:	low
Preview:	2020/11/20-23:02:02.195 1440 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2020/11/20-23:02:02.196 1440 Recovering log #3.2020/11/20-23:02:02.196 1440 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.145503038992787
Encrypted:	false
SSDEEP:	6:V4AVq2PWXp+N23iKKdK8NIFUtwaOVNAgZmwySRvAIkwOWXp+N23iKKdK8+eLJ:Vnva5KkpFUtw7h/yi75f5KkqJ
MD5:	B478157CBD41FFE7FAA711B436EAECBB
SHA1:	28673BEF35E5B15067768669621E2760D35FF06C
SHA-256:	D68A6A86BA2942A3F2EF3A7AC8FCB33DC6D58CAECB51D89EDBD4495354EA4C3D
SHA-512:	101F36D620E4C35C82F56E3FB76FA1FA1BFD5B54576F44BE5BEA7A4C023EB1DEBF3554571388C36E9BA8F9111ADD22250AF3F698AD9A45062951AD5CE40E8F E
Malicious:	false
Reputation:	low
Preview:	2020/11/20-23:02:04.154 1440 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2020/11/20-23:02:04.156 1440 Recovering log #3.2020/11/20-23:02:04.157 1440 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49C
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytl8i5cYLqNLbSnc45XXd/jEluKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2l/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9l/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	2.4945244875261876
Encrypted:	false
SSDEEP:	192:mTlC1FK2ws2Oka1GhssK2ws2OkaU4X37kDLI4OK2ws2Okah9sf8l/jfTOGf1fffl:4lWYHOHHOJ7YLFdHOsw3NHcokCM6
MD5:	51EFCC54A50A22C16C8818AC3B61C8CA
SHA1:	B07F9FE2ABA97F0DB8A6106CEEAFCFDB6C1163F7
SHA-256:	892A114BB75E001321470CCF23F3341439407F5601B10BF316026035C1E66B08
SHA-512:	3B77A2AC81FA335818D9933F19D6120ED576FFE6A788974939CB7057BCCD1CA4215E0AD49F76584AB4CF29AFF1AE185621100657AF58AFDFA75F9264E6A5AB1
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	68412
Entropy (8bit):	1.4521398585922638
Encrypted:	false
SSDEEP:	192:ALYegK2ws2Oka4StAcw4tfwOUJ2jfTO89sf8lh:ApXHO4SftfRGC
MD5:	AF676B1531BE9F2B5AA7C4837A0A364A
SHA1:	8994D330CAC3185346B289BBDB6E37D7CE83CBD3
SHA-256:	D71DEB2E76F55F28D9E39F4E43C50FD1DAA4D48F4A8672E7D7345138259E48C1
SHA-512:	C778BF39D30AE295906C3C993936DE59431E678DDA87AE9E4717E7C301E543FE43C234884CC7E56D891A8E65979B47B0D7A2309C779B830F52A69BD05657DB4
Malicious:	false
Reputation:	low
Preview:	.....>.I..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.175511748083018
Encrypted:	false
SSDEEP:	6:0Uh9+q2PWXp+N23iKKdK25+Xqx8chI+IFUtwHUuUqN2WZmwyHUIh9VkwOWXp+N2k:th9+va5KkTXfchI3FUtw0bqNJ/y0Ih9s
MD5:	CDF0C28D9E519318DC9E401A344F4389
SHA1:	F767604C5186C906F39238402A1E676E2EC04622
SHA-256:	DD2F3316605ACC450A790D6DD55E678C6D61AC2EA8269C50813DE5F7A9AE0E02
SHA-512:	63AB706D3BF3A96D8E9C806D4018B051081F14DED3F2FCE7509DAEA3600897DF75807500C556B2D18855691806FE6244CCAEB721CE656C7FB1A9B6E83DBB994
Malicious:	false
Reputation:	low
Preview:	2020/11/20-23:02:07.102 140c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2020/11/20-23:02:07.105 140c Recovering log #3.2020/11/20-23:02:07.107 140c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.1728101121322325
Encrypted:	false
SSDEEP:	6:0DE9+q2PWXp+N23iKKdK25+XuoIFUtwH6E2WZmwyHC9VkwOWXp+N23iKKdK25+Xp:T9+va5KkTXYFUtwnJ/yi9V5f5KkTXHJ
MD5:	04BD046DDB601B08671C56FDFD0FF0BD
SHA1:	DA88F3D77830803F1872B985666E987980029DBE
SHA-256:	12194436EDA07F7396F24E05C61670AB5BCA798A7972FBF2D8031D3635C37207
SHA-512:	4473AE17ED3C45755E833BC192B98212732ADE6834CE650E99148D5EC17A438BDD77C49D6C724B48E01839859B7E85E0595FE7F4A06F00E1920E1039AB8B74DE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Malicious:	false
Reputation:	low
Preview:	2020/11/20-23:02:07.094 140c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2020/11/20-23:02:07.095 140c Recovering log #3.2020/11/20-23:02:07.096 140c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.220320820083964
Encrypted:	false
SSDEEP:	6:2L+L+q2PWXp+N23iKKdKWT5g1IdqIFUtwAKWZmwyWLVkwOWXp+N23iKKdKWT5g1L:PL+va5Kkg5gSRFUtwvW/yWLV5f5Kkg5i
MD5:	DC250BB9EA9CEC07CB1332DD5D42F729
SHA1:	2629C1D03F3D22A1E21E68C7AF5DCE883C493901
SHA-256:	82568F579B9C6AA98FEDDFA980C2B0DD4ACD45536504B1E8DD70093174122BF4
SHA-512:	123CEDCDF4C4171E4A70A8389CB49FDCB943A624D674FAA18A3BA1174D2BD049B59C88C021D83A5B8B8FFD87778A4A0BCAD9FF8B503CE2231D0F28C8A53CF4E
Malicious:	false
Reputation:	low
Preview:	2020/11/20-23:02:06.964 125c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2020/11/20-23:02:06.971 125c Recovering log #3.2020/11/20-23:02:06.971 125c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	184320
Entropy (8bit):	0.6410413826629122
Encrypted:	false
SSDEEP:	192:RBlHksuIHz4FphIHW4QswrkqhIHgA43jfTL7ahWKkwrkqhIHqtg04Pfsfafz9cTr:Td9syyygH+yqKvkCM/
MD5:	BCD3F8E8538439BC331CF837942156A7
SHA1:	C7B4A2C43A387204E47B6C1C10951BB960A547DA
SHA-256:	92975A2F0CDD934D6C0BF4B6853175CB1E8FEE534861A6F79DB119F060FFCC54
SHA-512:	4872A6CCB00BAF56E569B244F1A0B116067307DB46560A76DE8A9B632EAC5A0F94E45A96D6F674356F38EC9966FAEE6EE7B81A0CF100632D9FE81F947EC4C02A
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	476
Entropy (8bit):	5.165061248968647
Encrypted:	false
SSDEEP:	12:yRwrA+KOT0TIBUGdDVbm/7WVBBTrKBk778B//OA+s6C/UQ:yid4qtdDtmD+3TrIY78BHOA+wL
MD5:	1BFFDEB1CD90E94FF55EEF966CA5B617
SHA1:	8409846EDD7FA91885174F40662578DA8EEA118B
SHA-256:	FA944CA49025DECD9D68E5F031D69312B0066A40759E9AAE09EA8315B6154D3F
SHA-512:	7084A0721466DDF2398DDA7AED13A3A40DD46357087DFC99F34252655743919221AC384B7793E2B1B1210E14E7882D08A7E0757A8A3C04849D475702C7E5C4FF
Malicious:	false
Reputation:	low
Preview:	....."0....com..faxfax..https..remittanceadvice..zizera*D.....com.....faxfax.....https.....remittanceadvice.....zizera..2.....a.....c.....d.....e.....f.....h.....i.....m.....n.....o.....p.....r.....s.....t.....v.....x.....z...:/.....Bk...g..... .....**https://faxfax.zizera.com/remittanceadvice2.remittanceadvice - faxfax:.....J.....

Static File Info

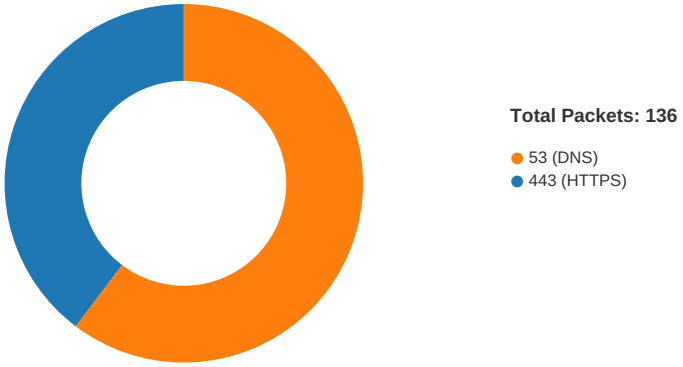
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-23:02:02.397765	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 23:02:04.875173092 CET	49724	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:04.876697063 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:04.914551020 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.914746046 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:04.915136099 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:04.916076899 CET	443	49724	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.916167974 CET	49724	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:04.916578054 CET	49724	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:04.953084946 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.954253912 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.954302073 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.954340935 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.954390049 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.954442978 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:04.954489946 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:04.956273079 CET	443	49724	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.957499981 CET	443	49724	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.957552910 CET	443	49724	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.957596064 CET	443	49724	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.957633018 CET	443	49724	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:04.957639933 CET	49724	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:04.957686901 CET	49724	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.123611927 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.124419928 CET	49724	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.124471903 CET	49724	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.124566078 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.124913931 CET	49725	443	192.168.2.3	34.255.187.247

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 23:02:05.161901951 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.161948919 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.162060976 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.162144899 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.162273884 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.164468050 CET	443	49724	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.164504051 CET	443	49724	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.164554119 CET	49724	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.164604902 CET	49724	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.168349981 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.168389082 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.168463945 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.168479919 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.168508053 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.168513060 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.168514013 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.168556929 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.168581963 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.168596029 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.168606043 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.168653011 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.168669939 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.168726921 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.200134039 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.200190067 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.200228930 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.200278044 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.200308084 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.200352907 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.200411081 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.206319094 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.245984077 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.258624077 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.258939981 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.259366035 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.259720087 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.296879053 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.297620058 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.298932076 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.298988104 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.299031973 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.299058914 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.299073935 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.299115896 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.299139977 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.299318075 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.299360991 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.299381018 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.299387932 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.299463987 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.300776005 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.300816059 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.300930977 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.300954103 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.300997972 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.301045895 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.301065922 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.301090956 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.301157951 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.301436901 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.301486969 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.301544905 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.301692009 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.301733971 CET	443	49725	34.255.187.247	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 23:02:05.301793098 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.301872015 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.301914930 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.301990032 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.302062988 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.302131891 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.302196026 CET	49725	443	192.168.2.3	34.255.187.247
Nov 20, 2020 23:02:05.302274942 CET	443	49725	34.255.187.247	192.168.2.3
Nov 20, 2020 23:02:05.302318096 CET	443	49725	34.255.187.247	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 23:01:59.626236916 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:01:59.653589010 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:00.600748062 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:01.612632990 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:02.396856070 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:02.397670984 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:04.811518908 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:04.816236019 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:04.818197966 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:04.821616888 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:04.847481012 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:04.852103949 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:04.853893995 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:04.872786045 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:05.131659985 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:05.175643921 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:05.239886999 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:05.257971048 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:05.261189938 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:05.284004927 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:05.296830893 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:05.303013086 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:05.471781015 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:05.515444040 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:06.699569941 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:06.743623018 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:07.515034914 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:07.559329033 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:07.660623074 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:07.687469006 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:08.677772999 CET	60633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:08.713674068 CET	53	60633	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:09.030395031 CET	61292	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:09.057585001 CET	53	61292	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:10.481120110 CET	64910	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:10.516997099 CET	53	64910	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:12.081247091 CET	52123	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:12.127651930 CET	53	52123	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:13.018837929 CET	59420	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:13.054430962 CET	53	59420	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:13.991240978 CET	58784	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:14.042282104 CET	53	58784	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:14.212506056 CET	63978	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:14.250552893 CET	53	63978	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:14.472903967 CET	62938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:14.500389099 CET	53	62938	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:15.209084988 CET	56803	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:15.245007038 CET	53	56803	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:15.477308035 CET	57145	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:15.492245913 CET	55359	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:15.525791883 CET	53	57145	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 23:02:15.538208961 CET	53	55359	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:15.654925108 CET	58306	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:15.780277014 CET	53	58306	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:15.917532921 CET	64124	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:15.944655895 CET	53	64124	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:16.477982998 CET	49361	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:16.513766050 CET	53	49361	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:16.517004967 CET	63150	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:16.519455910 CET	53279	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:16.552741051 CET	53	63150	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:16.554888010 CET	53	53279	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:18.708484888 CET	56881	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:18.746208906 CET	53	56881	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:19.674335957 CET	53642	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:19.712002039 CET	53	53642	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:20.132363081 CET	55667	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:20.182914019 CET	53	55667	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:20.634038925 CET	54833	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:20.637625933 CET	62476	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:20.664890051 CET	53	62476	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:20.671396017 CET	53	54833	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:21.231867075 CET	49705	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:21.259912014 CET	61477	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:21.270930052 CET	53	49705	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:21.299499989 CET	53	61477	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:21.515096903 CET	61633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:21.526010990 CET	55949	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:21.552350998 CET	53	61633	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:21.563364983 CET	57601	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:21.565555096 CET	53	55949	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:21.601658106 CET	53	57601	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:21.651432037 CET	49342	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:21.678590059 CET	53	49342	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:24.640398979 CET	56253	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:24.667464972 CET	53	56253	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:26.551603079 CET	49667	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:26.588876963 CET	53	49667	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:26.790709972 CET	55439	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:26.837583065 CET	53	55439	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:27.692682028 CET	57069	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:27.693087101 CET	57659	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:27.694202900 CET	54717	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:27.694736958 CET	63975	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:27.695708990 CET	56639	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:27.730460882 CET	53	57659	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:27.731218100 CET	53	54717	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:27.735008955 CET	53	56639	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:27.740935087 CET	53	63975	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:27.745466948 CET	53	57069	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:27.866313934 CET	51856	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:27.903773069 CET	53	51856	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:28.401073933 CET	56546	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:28.438565016 CET	53	56546	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:29.949254036 CET	62152	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:29.986363888 CET	53	62152	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:30.038875103 CET	53470	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:30.044054031 CET	56446	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:30.076328039 CET	53	53470	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:30.091243029 CET	53	56446	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:30.823672056 CET	59631	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:30.862816095 CET	53	59631	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:37.368416071 CET	55515	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:37.369070053 CET	64547	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:37.406402111 CET	53	64547	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 23:02:37.412615061 CET	53	55515	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:37.961721897 CET	51759	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:37.969146013 CET	59207	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:37.999579906 CET	53	51759	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:38.012711048 CET	53	59207	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:38.362312078 CET	54269	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:38.401644945 CET	53	54269	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:38.768889904 CET	54856	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:38.806492090 CET	53	54856	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:42.069474936 CET	64140	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:42.106996059 CET	53	64140	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:43.802468061 CET	62271	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:43.839690924 CET	53	62271	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:44.042614937 CET	57404	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:44.098819017 CET	53	57404	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:45.134246111 CET	57712	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:45.134287119 CET	60065	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:45.172214031 CET	53	57712	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:45.178139925 CET	53	60065	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:45.378071070 CET	55068	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:45.421837091 CET	53	55068	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:45.511512995 CET	64700	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:45.547097921 CET	53	64700	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:45.548281908 CET	64701	443	192.168.2.3	142.250.74.194
Nov 20, 2020 23:02:45.582381010 CET	443	64701	142.250.74.194	192.168.2.3
Nov 20, 2020 23:02:45.582437992 CET	443	64701	142.250.74.194	192.168.2.3
Nov 20, 2020 23:02:45.583687067 CET	64701	443	192.168.2.3	142.250.74.194
Nov 20, 2020 23:02:45.583936930 CET	64701	443	192.168.2.3	142.250.74.194
Nov 20, 2020 23:02:45.625178099 CET	443	64701	142.250.74.194	192.168.2.3
Nov 20, 2020 23:02:45.625653982 CET	64701	443	192.168.2.3	142.250.74.194
Nov 20, 2020 23:02:45.650085926 CET	443	64701	142.250.74.194	192.168.2.3
Nov 20, 2020 23:02:45.658289909 CET	443	64701	142.250.74.194	192.168.2.3
Nov 20, 2020 23:02:45.658328056 CET	443	64701	142.250.74.194	192.168.2.3
Nov 20, 2020 23:02:45.658617973 CET	64701	443	192.168.2.3	142.250.74.194
Nov 20, 2020 23:02:46.121664047 CET	61998	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:46.148727894 CET	53	61998	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:46.724931955 CET	53724	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:46.760507107 CET	53	53724	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:46.907229900 CET	53725	443	192.168.2.3	172.217.21.226
Nov 20, 2020 23:02:46.930706978 CET	443	53725	172.217.21.226	192.168.2.3
Nov 20, 2020 23:02:46.930756092 CET	443	53725	172.217.21.226	192.168.2.3
Nov 20, 2020 23:02:46.931992054 CET	53725	443	192.168.2.3	172.217.21.226
Nov 20, 2020 23:02:46.962299109 CET	443	53725	172.217.21.226	192.168.2.3
Nov 20, 2020 23:02:46.962757111 CET	53725	443	192.168.2.3	172.217.21.226
Nov 20, 2020 23:02:47.673109055 CET	52328	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:47.714104891 CET	53	52328	8.8.8.8	192.168.2.3
Nov 20, 2020 23:02:56.306561947 CET	58051	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:02:56.348040104 CET	53	58051	8.8.8.8	192.168.2.3
Nov 20, 2020 23:03:00.586973906 CET	64701	443	192.168.2.3	142.250.74.194
Nov 20, 2020 23:03:00.638885021 CET	443	64701	142.250.74.194	192.168.2.3
Nov 20, 2020 23:03:01.415607929 CET	64130	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:03:01.466334105 CET	53	64130	8.8.8.8	192.168.2.3
Nov 20, 2020 23:03:02.841819048 CET	50491	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:03:02.877124071 CET	53	50491	8.8.8.8	192.168.2.3
Nov 20, 2020 23:03:03.111206055 CET	52529	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:03:03.147032976 CET	53	52529	8.8.8.8	192.168.2.3
Nov 20, 2020 23:03:03.197010994 CET	53656	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:03:03.240935087 CET	53	53656	8.8.8.8	192.168.2.3
Nov 20, 2020 23:03:03.294064999 CET	62724	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:03:03.331861019 CET	53	62724	8.8.8.8	192.168.2.3
Nov 20, 2020 23:03:03.687882900 CET	56059	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:03:03.723603010 CET	53	56059	8.8.8.8	192.168.2.3
Nov 20, 2020 23:03:25.101712942 CET	63060	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:03:25.128994942 CET	53	63060	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 23:03:25.344134092 CET	51498	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:03:25.379944086 CET	53	51498	8.8.8.8	192.168.2.3
Nov 20, 2020 23:03:44.904398918 CET	59943	53	192.168.2.3	8.8.8.8
Nov 20, 2020 23:03:44.940314054 CET	53	59943	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 20, 2020 23:02:02.397764921 CET	192.168.2.3	8.8.8.8	d077	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 23:02:04.821616888 CET	192.168.2.3	8.8.8.8	0x7d54	Standard query (0)	faxfax.zizera.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:05.257971048 CET	192.168.2.3	8.8.8.8	0x516e	Standard query (0)	assets-a.zizera.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:07.515034914 CET	192.168.2.3	8.8.8.8	0xa9b6	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:13.991240978 CET	192.168.2.3	8.8.8.8	0xe042	Standard query (0)	yelphaiku.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:15.477308035 CET	192.168.2.3	8.8.8.8	0x4e7c	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:15.654925108 CET	192.168.2.3	8.8.8.8	0xe7f5	Standard query (0)	vikinggenetics-my.sharepoint.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:16.477982998 CET	192.168.2.3	8.8.8.8	0x702c	Standard query (0)	yelphaiku.comimages	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:16.517004967 CET	192.168.2.3	8.8.8.8	0x12d0	Standard query (0)	yelphaiku.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:16.519455910 CET	192.168.2.3	8.8.8.8	0x660d	Standard query (0)	vikinggenetics-my.sharepoint.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:18.708484888 CET	192.168.2.3	8.8.8.8	0x3bb	Standard query (0)	x.co	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:19.674335957 CET	192.168.2.3	8.8.8.8	0x3a09	Standard query (0)	shortener.godaddy.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:20.634038925 CET	192.168.2.3	8.8.8.8	0x23e	Standard query (0)	img6.wsimg.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:20.637625933 CET	192.168.2.3	8.8.8.8	0x8071	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:21.231867075 CET	192.168.2.3	8.8.8.8	0x987c	Standard query (0)	gui.godaddy.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:21.259912014 CET	192.168.2.3	8.8.8.8	0xb68c	Standard query (0)	tags.tiqcdn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:21.515096903 CET	192.168.2.3	8.8.8.8	0x4637	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:21.526010990 CET	192.168.2.3	8.8.8.8	0x4420	Standard query (0)	events.api.godaddy.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:21.563364983 CET	192.168.2.3	8.8.8.8	0x2767	Standard query (0)	img1.wsimg.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:21.651432037 CET	192.168.2.3	8.8.8.8	0xb5a	Standard query (0)	bam-cell.nr-data.net	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:27.692682028 CET	192.168.2.3	8.8.8.8	0xac16	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:27.695708990 CET	192.168.2.3	8.8.8.8	0x96c	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:37.368416071 CET	192.168.2.3	8.8.8.8	0xad30	Standard query (0)	auth.split.io	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:37.369070053 CET	192.168.2.3	8.8.8.8	0x99de	Standard query (0)	sdk.split.io	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:37.961721897 CET	192.168.2.3	8.8.8.8	0x130b	Standard query (0)	lptag.liveperson.net	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:37.969146013 CET	192.168.2.3	8.8.8.8	0x1100	Standard query (0)	streaming.split.io	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:38.362312078 CET	192.168.2.3	8.8.8.8	0x7967	Standard query (0)	accdn.lpsnmedia.net	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:38.768889904 CET	192.168.2.3	8.8.8.8	0x8227	Standard query (0)	www.godaddy.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:42.069474936 CET	192.168.2.3	8.8.8.8	0xf220	Standard query (0)	img1.wsimg.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 23:02:43.802468061 CET	192.168.2.3	8.8.8.8	0x93f4	Standard query (0)	lpcdn.lpsnmedia.net	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:44.042614937 CET	192.168.2.3	8.8.8.8	0x49e2	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:45.134246111 CET	192.168.2.3	8.8.8.8	0xdb5b	Standard query (0)	cdn.trackjs.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:45.134287119 CET	192.168.2.3	8.8.8.8	0xed1c	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:45.378071070 CET	192.168.2.3	8.8.8.8	0xdc61	Standard query (0)	securepubads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:45.511512995 CET	192.168.2.3	8.8.8.8	0x9d73	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:46.121664047 CET	192.168.2.3	8.8.8.8	0x3070	Standard query (0)	usage.tractkjs.com	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:46.724931955 CET	192.168.2.3	8.8.8.8	0x36f4	Standard query (0)	va.v.liveperson.net	A (IP address)	IN (0x0001)
Nov 20, 2020 23:03:44.904398918 CET	192.168.2.3	8.8.8.8	0xbf58	Standard query (0)	events.split.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 23:02:04.872786045 CET	8.8.8.8	192.168.2.3	0x7d54	No error (0)	faxfax.ziera.com	bullet-pandi-1110328995.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:04.872786045 CET	8.8.8.8	192.168.2.3	0x7d54	No error (0)	bullet-pandi-1110328995.eu-west-1.elb.amazonaws.com		34.255.187.247	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:04.872786045 CET	8.8.8.8	192.168.2.3	0x7d54	No error (0)	bullet-pandi-1110328995.eu-west-1.elb.amazonaws.com		54.195.40.25	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:05.303013086 CET	8.8.8.8	192.168.2.3	0x516e	No error (0)	assets-a.zizera.com	d3cvrokiq7pmri.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:05.303013086 CET	8.8.8.8	192.168.2.3	0x516e	No error (0)	d3cvrokiq7pmri.cloudfront.net		13.224.93.109	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:05.303013086 CET	8.8.8.8	192.168.2.3	0x516e	No error (0)	d3cvrokiq7pmri.cloudfront.net		13.224.93.92	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:05.303013086 CET	8.8.8.8	192.168.2.3	0x516e	No error (0)	d3cvrokiq7pmri.cloudfront.net		13.224.93.121	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:05.303013086 CET	8.8.8.8	192.168.2.3	0x516e	No error (0)	d3cvrokiq7pmri.cloudfront.net		13.224.93.74	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:07.559329033 CET	8.8.8.8	192.168.2.3	0xa9b6	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:07.559329033 CET	8.8.8.8	192.168.2.3	0xa9b6	No error (0)	googlehosted.l.googleusercontent.com		172.217.16.193	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:14.042282104 CET	8.8.8.8	192.168.2.3	0xe042	No error (0)	yelphaiku.com		162.241.127.79	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:15.525791883 CET	8.8.8.8	192.168.2.3	0x4e7c	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:15.780277014 CET	8.8.8.8	192.168.2.3	0xe7f5	No error (0)	vikinggenetics-my.sharepoint.com	vikinggenetics.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:15.780277014 CET	8.8.8.8	192.168.2.3	0xe7f5	No error (0)	vikinggenetics.sharepoint.com	614-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:15.780277014 CET	8.8.8.8	192.168.2.3	0xe7f5	No error (0)	614-ipv4e.clump.prod.aa-rt.sharepoint.com	17825-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:15.780277014 CET	8.8.8.8	192.168.2.3	0xe7f5	No error (0)	17825-ipv4e.farm.prod.aa-rt.sharepoint.com	17825-ipv4e.farm.prod.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 23:02:16.513766050 CET	8.8.8.8	192.168.2.3	0x702c	Name error (3)	yelphaiku.comimages	none	none	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:16.552741051 CET	8.8.8.8	192.168.2.3	0x12d0	No error (0)	yelphaiku.com		162.241.127.79	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:16.554888010 CET	8.8.8.8	192.168.2.3	0x660d	No error (0)	vikinggenetics-my.sharepoint.com	vikinggenetics.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:16.554888010 CET	8.8.8.8	192.168.2.3	0x660d	No error (0)	vikinggenetics.sharepoint.com	614-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:16.554888010 CET	8.8.8.8	192.168.2.3	0x660d	No error (0)	614-ipv4e.clump.prod.aa-rt.sharepoint.com	17825-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:16.554888010 CET	8.8.8.8	192.168.2.3	0x660d	No error (0)	17825-ipv4e.farm.prod.aa-rt.sharepoint.com	17825-ipv4e.farm.prod.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:18.746208906 CET	8.8.8.8	192.168.2.3	0x3bb	No error (0)	x.co		45.40.140.1	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:19.712002039 CET	8.8.8.8	192.168.2.3	0x3a09	No error (0)	shortener.godaddy.com		45.40.140.1	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:20.664890051 CET	8.8.8.8	192.168.2.3	0x8071	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:20.664890051 CET	8.8.8.8	192.168.2.3	0x8071	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:20.671396017 CET	8.8.8.8	192.168.2.3	0x23e	No error (0)	img6.wsimg.com	global-wildcard.wsimg.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:21.270930052 CET	8.8.8.8	192.168.2.3	0x987c	No error (0)	gui.godaddy.com	gui-ipv6.godaddy.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:21.299499989 CET	8.8.8.8	192.168.2.3	0xb68c	No error (0)	tags.tiqcdn.com	tags.tiqcdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:21.552350998 CET	8.8.8.8	192.168.2.3	0x4637	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:21.565555096 CET	8.8.8.8	192.168.2.3	0x4420	No error (0)	events.api.godaddy.com	events.api.godaddy.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:21.601658106 CET	8.8.8.8	192.168.2.3	0x2767	No error (0)	img1.wsimg.com	global-wildcard.wsimg.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:21.678590059 CET	8.8.8.8	192.168.2.3	0xb5a	No error (0)	bam-cell.nr-data.net	tls12.newrelic.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:27.735008955 CET	8.8.8.8	192.168.2.3	0x96c	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:27.745466948 CET	8.8.8.8	192.168.2.3	0xac16	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:37.406402111 CET	8.8.8.8	192.168.2.3	0x99de	No error (0)	sdk.split.io	f2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:37.412615061 CET	8.8.8.8	192.168.2.3	0xad30	No error (0)	auth.split.io		184.73.218.177	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:37.412615061 CET	8.8.8.8	192.168.2.3	0xad30	No error (0)	auth.split.io		34.206.15.100	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:37.412615061 CET	8.8.8.8	192.168.2.3	0xad30	No error (0)	auth.split.io		54.226.182.229	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:37.412615061 CET	8.8.8.8	192.168.2.3	0xad30	No error (0)	auth.split.io		18.206.111.147	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:37.999579906 CET	8.8.8.8	192.168.2.3	0x130b	No error (0)	lptag.liveperson.net	lptag.liveperson.cotcdb.net.livepersonk.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 23:02:38.012711048 CET	8.8.8.8	192.168.2.3	0x1100	No error (0)	streaming.split.io	split-cname-realtime.ably.io		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:38.012711048 CET	8.8.8.8	192.168.2.3	0x1100	No error (0)	split-cname-realtime.ably.io	dz87sht31vgqa.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:38.012711048 CET	8.8.8.8	192.168.2.3	0x1100	No error (0)	dz87sht31vgqa.cloudfront.net		13.224.93.31	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:38.012711048 CET	8.8.8.8	192.168.2.3	0x1100	No error (0)	dz87sht31vgqa.cloudfront.net		13.224.93.96	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:38.012711048 CET	8.8.8.8	192.168.2.3	0x1100	No error (0)	dz87sht31vgqa.cloudfront.net		13.224.93.84	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:38.012711048 CET	8.8.8.8	192.168.2.3	0x1100	No error (0)	dz87sht31vgqa.cloudfront.net		13.224.93.2	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:38.401644945 CET	8.8.8.8	192.168.2.3	0x7967	No error (0)	accdn.lpsnmedia.net	accdn.lpsnmedia.liveperson.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:38.806492090 CET	8.8.8.8	192.168.2.3	0x8227	No error (0)	www.godaddy.com	wildcard-ipv6.godaddy.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:42.106996059 CET	8.8.8.8	192.168.2.3	0xf220	No error (0)	img1.wsimg.com	global-wildcard.wsimg.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:43.839690924 CET	8.8.8.8	192.168.2.3	0x93f4	No error (0)	lpcdn.lpsnmedia.net	lpcdn.lpsnmedia.liveperson.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:44.098819017 CET	8.8.8.8	192.168.2.3	0x49e2	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:45.172214031 CET	8.8.8.8	192.168.2.3	0xdb5b	No error (0)	cdn.trackjs.com	cdn.trackjs.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:45.172214031 CET	8.8.8.8	192.168.2.3	0xdb5b	No error (0)	cdn.trackjs.netdna-cdn.com		94.31.29.32	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:45.178139925 CET	8.8.8.8	192.168.2.3	0xed1c	No error (0)	www.googletagservices.com	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:45.178139925 CET	8.8.8.8	192.168.2.3	0xed1c	No error (0)	pagead46.l.doubleclick.net		172.217.16.194	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:45.421837091 CET	8.8.8.8	192.168.2.3	0xdc61	No error (0)	securepubads.g.doubleclick.net	partnerad.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:45.421837091 CET	8.8.8.8	192.168.2.3	0xdc61	No error (0)	partnerad.l.doubleclick.net		172.217.21.226	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:45.547097921 CET	8.8.8.8	192.168.2.3	0x9d73	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:02:45.547097921 CET	8.8.8.8	192.168.2.3	0x9d73	No error (0)	pagead46.l.doubleclick.net		142.250.74.194	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:46.148727894 CET	8.8.8.8	192.168.2.3	0x3070	No error (0)	usage.trackjs.com		167.114.119.127	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:46.148727894 CET	8.8.8.8	192.168.2.3	0x3070	No error (0)	usage.trackjs.com		138.197.155.84	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:46.148727894 CET	8.8.8.8	192.168.2.3	0x3070	No error (0)	usage.trackjs.com		158.69.52.117	A (IP address)	IN (0x0001)
Nov 20, 2020 23:02:46.760507107 CET	8.8.8.8	192.168.2.3	0x36f4	No error (0)	va.v.liveperson.net		208.89.12.87	A (IP address)	IN (0x0001)
Nov 20, 2020 23:03:44.940314054 CET	8.8.8.8	192.168.2.3	0xbf58	No error (0)	events.split.io	events-prod-1-1033355748.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 23:03:44.940314054 CET	8.8.8.8	192.168.2.3	0xbf58	No error (0)	events-prod-1-1033355748.us-east-1.elb.amazonaws.com		34.196.246.142	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 23:03:44.940314054 CET	8.8.8.8	192.168.2.3	0xbf58	No error (0)	events-prod-1-1033355748.us-east-1.elb.amazonaws.com		52.5.217.133	A (IP address)	IN (0x0001)
Nov 20, 2020 23:03:44.940314054 CET	8.8.8.8	192.168.2.3	0xbf58	No error (0)	events-prod-1-1033355748.us-east-1.elb.amazonaws.com		54.165.233.171	A (IP address)	IN (0x0001)
Nov 20, 2020 23:03:44.940314054 CET	8.8.8.8	192.168.2.3	0xbf58	No error (0)	events-prod-1-1033355748.us-east-1.elb.amazonaws.com		52.21.27.206	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- x.co

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49775	45.40.140.1	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 23:02:18.918710947 CET	2807	OUT	GET /8923bsuydn HTTP/1.1 Host: x.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
Nov 20, 2020 23:02:19.087265015 CET	2807	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Fri, 20 Nov 2020 22:02:19 GMT Content-Type: text/html Content-Length: 169 Connection: keep-alive Location: https://x.co/8923bsuydn Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx/1.16.1 </body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 23:02:04.954390049 CET	34.255.187.247	443	192.168.2.3	49725	CN=*.zizera.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jul 24 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Aug 24 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 20, 2020 23:02:04.957633018 CET	34.255.187.247	443	192.168.2.3	49724	CN=*.zizera.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jul 24 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Aug 24 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 20, 2020 23:02:06.262049913 CET	34.255.187.247	443	192.168.2.3	49736	CN=*.zizera.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Jul 24 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Aug 24 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 23:02:16.827105999 CET	162.241.127.79	443	192.168.2.3	49773	CN=yelphaiku.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Nov 20 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Fri Feb 19 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 20, 2020 23:02:19.427887917 CET	45.40.140.1	443	192.168.2.3	49777	CN=x.co, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Thu Jul 16 22:57:36 CEST 2020 Tue May 03 09:00:00 CEST 2011 Tue Sep 01 02:00:00 CEST 2009	Sat Jul 16 22:57:36 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri Jan 01 00:59:59 CET 2038	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Sep 01 02:00:00 CEST 2009	Fri Jan 01 00:59:59 CET 2038		
Nov 20, 2020 23:02:20.044795036 CET	45.40.140.1	443	192.168.2.3	49778	CN=shortener.godaddy.com, O=GoDaddy Inc., L=Scottsdale, ST=Arizona, C=US, SERIALNUMBER=F20244620, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=Arizona, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Jul 28 02:34:29 CEST 2020 Tue May 03 09:00:00 CEST 2011 Tue Sep 01 02:00:00 CEST 2009	Thu Jul 28 02:34:29 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri Jan 01 00:59:59 CET 2038	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Sep 01 02:00:00 CEST 2009	Fri Jan 01 00:59:59 CET 2038		
Nov 20, 2020 23:02:35.094593048 CET	45.40.140.1	443	192.168.2.3	49845	CN=shortener.godaddy.com, O=GoDaddy Inc., L=Scottsdale, ST=Arizona, C=US, SERIALNUMBER=F20244620, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=Arizona, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Jul 28 02:34:29 CEST 2020 Tue May 03 09:00:00 CEST 2011 Tue Sep 01 02:00:00 CEST 2009	Thu Jul 28 02:34:29 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri Jan 01 00:59:59 CET 2038	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27,29-23-24,0	7f805430de1e7d98b1de033adb58cf46
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Sep 01 02:00:00 CEST 2009	Fri Jan 01 00:59:59 CET 2038		
Nov 20, 2020 23:02:35.099426031 CET	45.40.140.1	443	192.168.2.3	49848	CN=x.co, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Thu Jul 16 22:57:36 CEST 2020 Tue May 03 09:00:00 CEST 2011 Tue Sep 01 02:00:00 CEST 2009	Sat Jul 16 22:57:36 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri Jan 01 00:59:59 CET 2038	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Sep 01 02:00:00 CEST 2009	Fri Jan 01 00:59:59 CET 2038		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 23:02:37.619240046 CET	184.73.218.177	443	192.168.2.3	49858	CN=*.split.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Sep 04 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Oct 06 02:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 20, 2020 23:02:45.254834890 CET	94.31.29.32	443	192.168.2.3	49909	CN=*.trackjs.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 11 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Sep 09 14:00:00 CEST 2021 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Nov 20, 2020 23:02:46.373155117 CET	167.114.119.127	443	192.168.2.3	49926	CN=*.trackjs.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 11 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Sep 09 14:00:00 CEST 2021 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Nov 20, 2020 23:02:47.075920105 CET	208.89.12.87	443	192.168.2.3	49929	CN=*.v.liveperson.net, OU="LivePerson, Inc.", O="LivePerson, Inc", STREET=475 10TH AVE FL 5, L=New York, ST=New York, OID.2.5.4.17=10018, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Apr 13 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Thu Apr 14 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5904 Parent PID: 2052

General

Start time:	23:02:01
Start date:	20/11/2020
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://faxfax.zizera.com/remittanceadvice'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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: 2308 Parent PID: 5904

General

Start time:	23:02:02
Start date:	20/11/2020
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1540,3317695339915788095,55565 5226975024704,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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