ID: 321428
Cookbook: browseurl.jbs
Time: 03:40:48
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

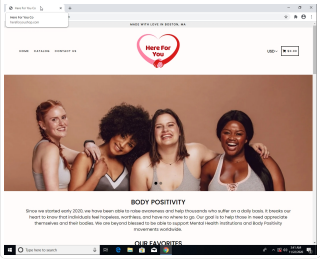
Analysis Report http://hereforyoushop.com

Overview

General Information

Sample URL:	http://hereforyoushop.com
Analysis ID:	321428

Most interesting Screenshot:



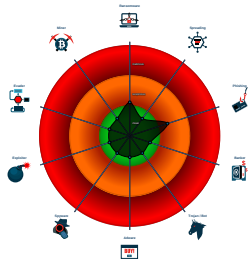
Detection

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

Signatures

- Form action URLs do not match mai…
- Found iframes

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 4952 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://hereforyoushop.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4796 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,13729553244047984668,6139627914611722907,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1720 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

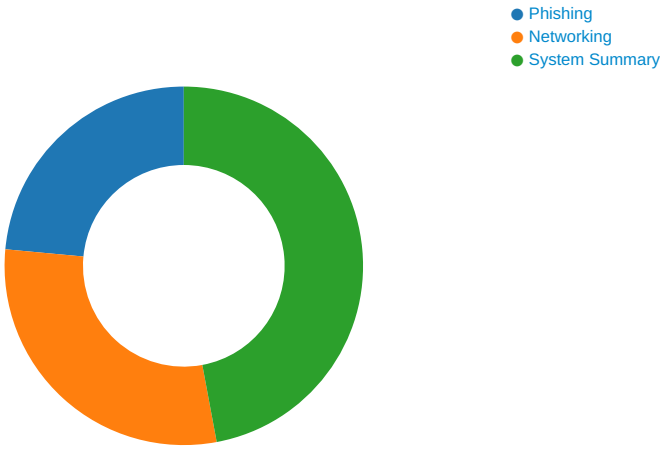
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



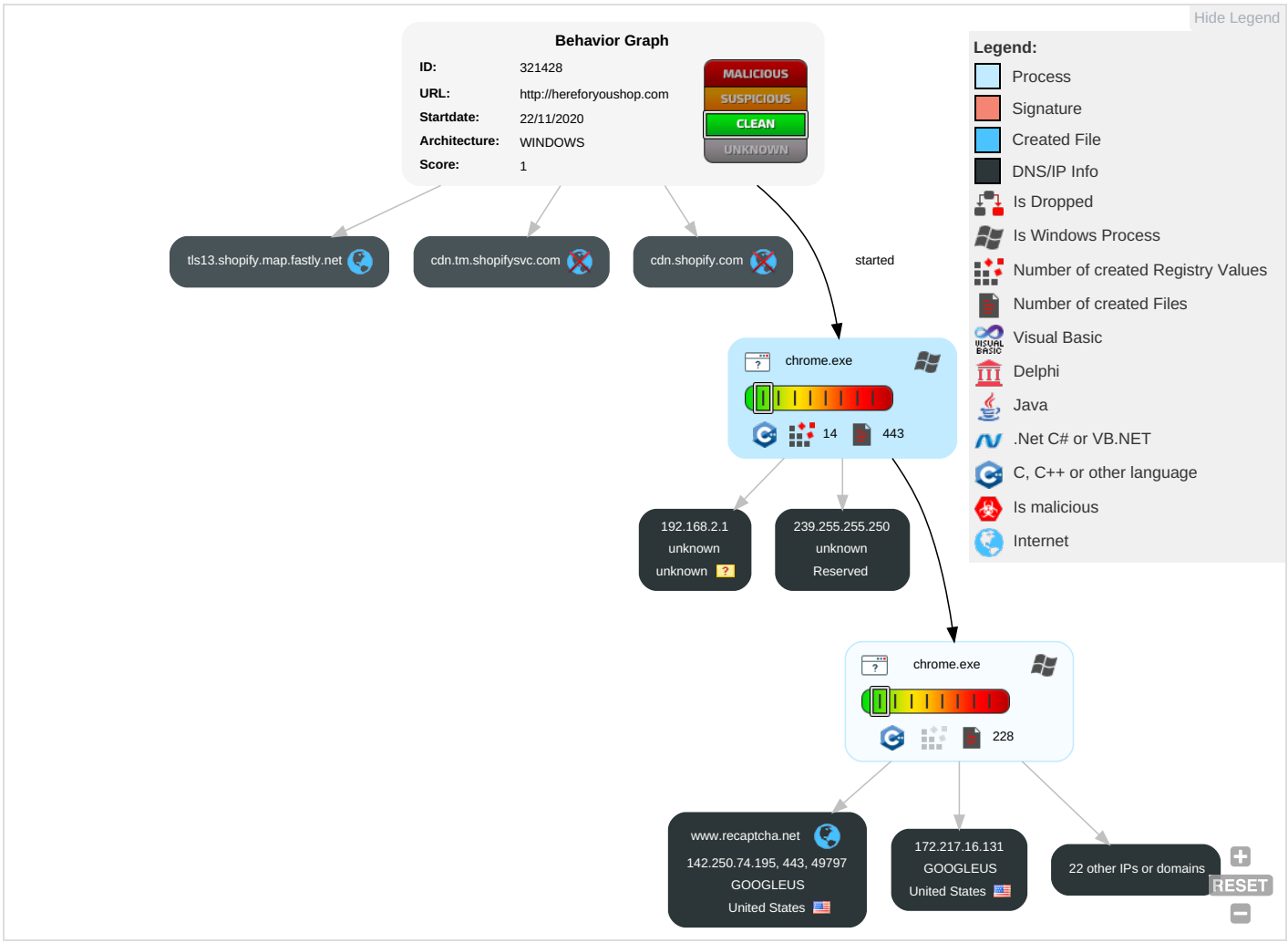
Click to jump to signature section

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

Mitre Att&ck Matrix

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

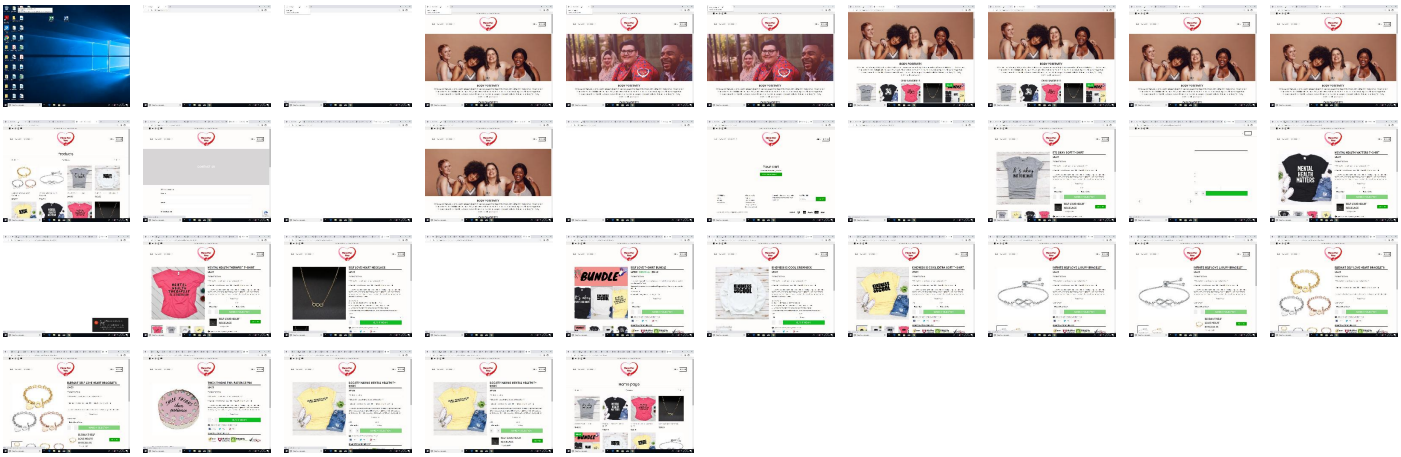
Behavior Graph

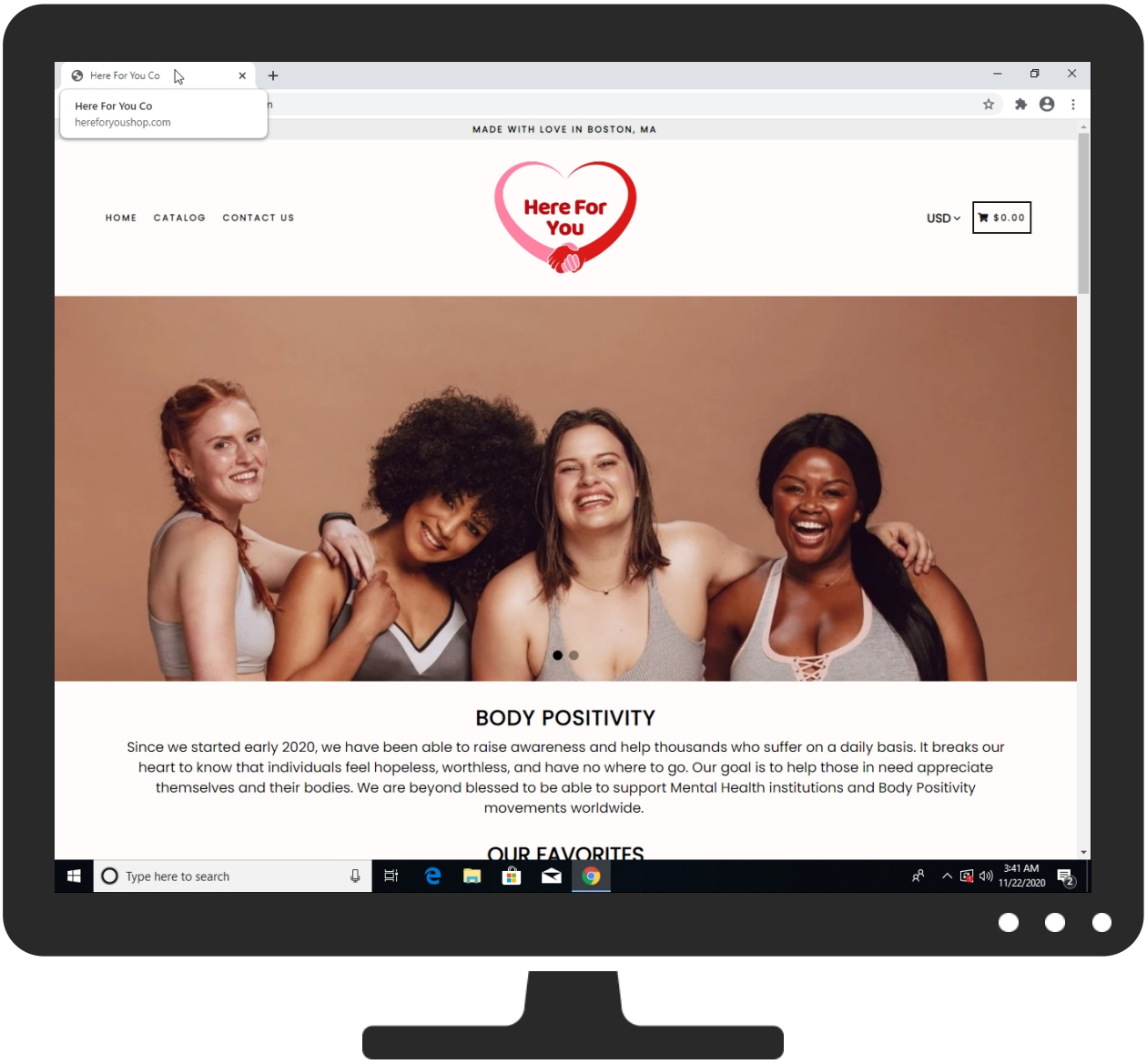


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://hereforyoushop.com	0%	Virustotal		Browse
http://hereforyoushop.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
prod.pinterest.global.map.fastly.net	0%	Virustotal		Browse
hereforyoushop.com	0%	Virustotal		Browse
www.recaptcha.net	0%	Virustotal		Browse
sellup.herokuapp.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://hereforyoushop.com/&	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/#C	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/elegant-self-love-heart-bracelets0Elegant	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/pages/contact-usContact	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/its-okay-soft-t-shirt-1IT	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/thick-thighs-thin-patience-pin-Thick	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/.	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/0	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/mental-health-matters-t-shirtG	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/mental-health-therapist-t-shirt-1MENTAL	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/elegant-self-love-heart-braceletsElegant	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/F	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/A	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/1u	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/C	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com(_https://hereforyoushop.com	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/N	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/J	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/#MainContentHere	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/kindness-is-cool-t-shirtKINDNESS	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/mental-health-matters-t-shirtMENTAL	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/2	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/3	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/collections/frontpageE&	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/kindness-is-cool-crewneckKINDNESS	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.comh	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/its-okay-soft-t-shirt-1%IT	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/cartYour	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/:	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/e	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://hereforyoushop.com/contact#contact_form	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/b	0%	Avira URL Cloud	safe	
http://hereforyoushop.com/Dv	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/p	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/t;	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/society-harms-mental-health-t-shirtSOCIETY	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/k	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/S	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/_	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/kindness-is-cool-crewneck(KINDNESS	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/products/society-harms-mental-health-t-shirt2SOCIETY	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/r	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/t	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/y	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/collections/allProducts	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/z	0%	Avira URL Cloud	safe	
http://https://monorail-edge.shopifysvc.com/unstable/produce_batch	0%	Avira URL Cloud	safe	
http://https://hereforyoushop.com/cartR	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
monorail-production-web-apps-a-us-central1-1.shopifycloud.com	34.68.85.43	true	false		high
scontent.xx.fbcdn.net	185.60.216.19	true	false		high
prod.pinterest.global.map.fastly.net	151.101.0.84	true	false	• 0%, Virustotal, Browse	unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hereforyoushop.com	23.227.38.65	true	false	• 0%, Virustotal, Browse	unknown
www.recaptcha.net	142.250.74.195	true	false	• 0%, Virustotal, Browse	unknown
sellup.herokuapp.com	52.6.203.110	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.16.193	true	false		high
tls13.shopify.map.fastly.net	151.101.1.12	true	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
monorail-edge.shopifysvc.com	unknown	unknown	false		unknown
s.pinimg.com	unknown	unknown	false		high
cdn.shopify.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
ct.pinterest.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://hereforyoushop.com/collections/frontpage	false		unknown
http://https://hereforyoushop.com/pages/contact-us	false		unknown
http://https://hereforyoushop.com/collections/all	false		unknown
http://https://hereforyoushop.com/#	false		unknown
http://https://hereforyoushop.com/products/mental-health-matters-t-shirt	false		unknown
http://https://hereforyoushop.com/#MainContent	false		unknown
http://https://hereforyoushop.com/products/mental-health-therapist-t-shirt-1	false		unknown
http://https://hereforyoushop.com/cart	false		unknown
http://https://hereforyoushop.com/products/its-okay-soft-t-shirt-1	false		unknown

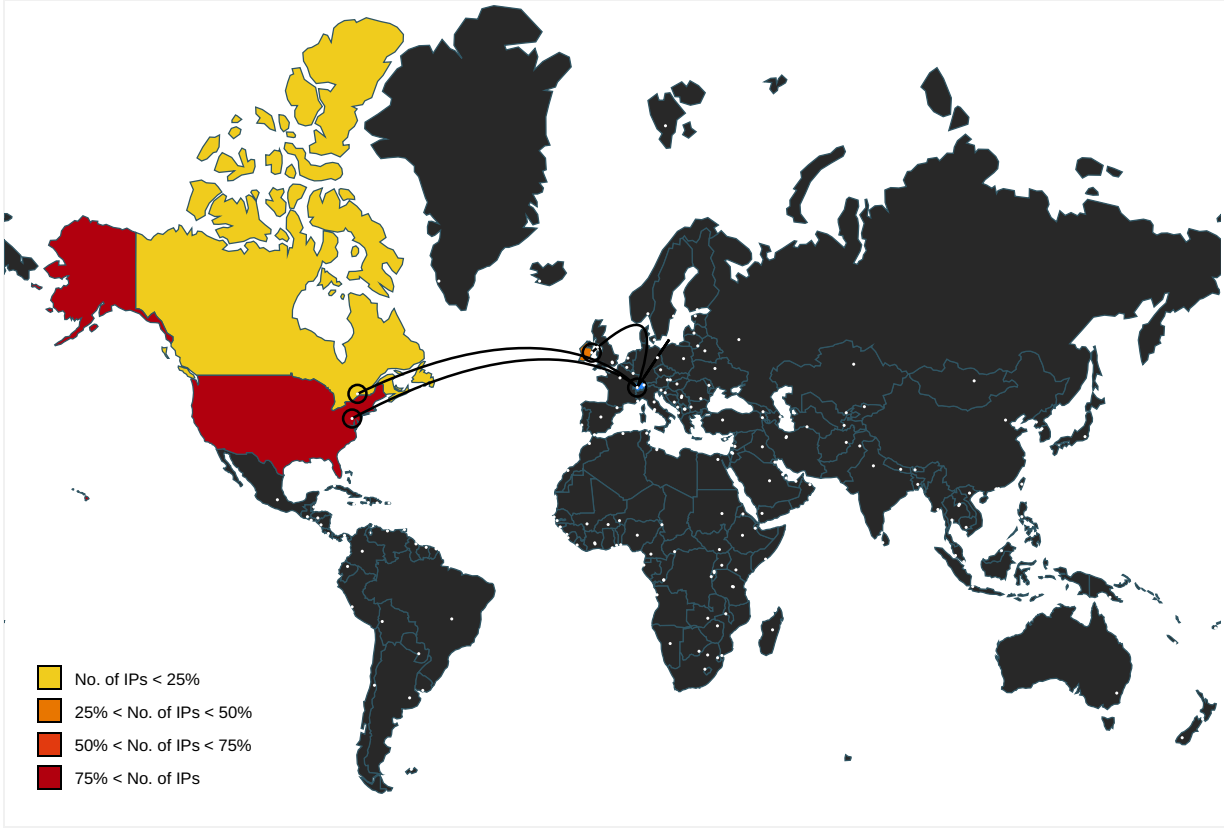
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hereforyoushop.com/&	5d760ce477ab20fb_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/#C	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/elegant-self-love-heart-bracelets0Elegant	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/pages/contact-usContact	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/its-okay-soft-t-shirt-1IT	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/thick-thighs-thin-patience-pin-Thick	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/s/javascripts/currencies.jsaD	5c5bd7a64ba48473_0.0.dr	false		high
http://https://hereforyoushop.com/products/kindness-is-cool-t-shirt	Current Session.0.dr	false		unknown
http://https://hereforyoushop.com/#	Current Session.0.dr	false		unknown
http://https://hereforyoushop.com/products/self-love-t-shirt-bundle	Current Session.0.dr	false		unknown
http://https://hereforyoushop.com/.	86df87e775f96432_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/	6872ce7adcf25f4b_0.0.dr	false		high
http://https://hereforyoushop.com/0	5d760ce477ab20fb_0.0.dr, b6e0bfd2dc8319e1_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/shopifycloud/consent-tracking-api/v0.1/consent-tracking-api.js	b6e0bfd2dc8319e1_0.0.dr	false		high
http://https://cdn.shopify.com/s/trekkie.storefront.3bc22f7b201bea3154c99666f2373bcf9a3e8fb1.min.js	589454532e0beb88_0.0.dr	false		high
http://https://hereforyoushop.com/products/mental-health-matters-t-shirtG	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/mental-health-therapist-t-shirt-1MENTAL	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ct.pinterest.com	70747a5c451cd1e1_0.0.dr	false		high
http://https://hereforyoushop.com/products/elegant-self-love-heart-braceletsElegant	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/F	b6e0bfd2dc8319e1_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://connect.facebook.net/signals/config/713019789423044?v=2.9.29&r=stable	998808883a4f4580_0.0.dr	false		high
http://https://hereforyoushop.com/A	6ed4a4600e77f5dc_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/1u	6ed4a4600e77f5dc_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/C	0e0db2eb3425f0d0_0.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/bootstrap.min.js?v=7372439028658456128	1be31ae4a43afd1e_0.0.dr	false		high
http://https://s.pinimg.com	085dab5f-e2a8-4406-a215-a48f5f42dc5c.tmp.1.dr	false		high
http://cdn.shopify.com/s/files/1/0481/0922/4087/products/product-image-1526576412_1200x1200.jpg?v=15	Current Session.0.dr	false		high
http://https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/theme.js?v=7548532355862316605	1280eaf7baf34351_0.0.dr	false		high
http://https://hereforyoushop.com(_https://hereforyoushop.com	000003.log3.0.dr	false	• Avira URL Cloud: safe	low
http://https://hereforyoushop.com/N	b6e0bfd2dc8319e1_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://monorail-edge-ca.shopifycloud.com/unstable/produce_batch	576c556eec03cace_0.0.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	2eaa7ed6113c80dc_0.0.dr	false		high
http://https://s.pinimg.com/ct/lib/main.d71a97dd.js	0b236b7f5bf72364_0.0.dr, 70747a5c451cd1e1_0.0.dr	false		high
http://https://hereforyoushop.com/J	1280eaf7baf34351_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/mental-health-matters-t-shirt	Current Session.0.dr, History-journal.0.dr	false		unknown
http://https://hereforyoushop.com/#MainContentHere	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/collections/frontpage	Current Session.0.dr	false		unknown
http://https://hereforyoushop.com/products/kindness-is-cool-t-shirtKINDNESS	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/mental-health-matters-t-shirtMENTAL	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/3	5d760ce477ab20fb_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/collections/frontpageE&	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/pages/contact-us	Current Session.0.dr	false		unknown
http://https://hereforyoushop.com/products/kindness-is-cool-crewneckKINDNESS	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.comh	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/its-okay-soft-t-shirt-1%IT	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/cartYour	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/thick-thighs-thin-patience-pin	Current Session.0.dr	false		unknown
http://https://hereforyoushop.com/:	2eaa7ed6113c80dc_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://schema.org/Offer	Current Session.0.dr	false		high
http://https://hereforyoushop.com/e	998808883a4f4580_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	02166985-a922-4ec8-9a1a-5c07bb44bdeb.tmp.1.dr, 45921a99-a900-4bb3-aa55-cf4e939b5ad4.tmp.1.dr, ac3d092f-84eb-4010-84a8-8a5c9f7ef356.tmp.1.dr, 085dab5f-e2a8-4406-a215-a48f5f42dc5c.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hereforyoushop.com/contact#contact_form	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/shopifycloud/storefront-recaptcha-v3/v0.1/index.js	e7bec4ed4587ef3d_0.0.dr	false		high
http://https://hereforyoushop.com/b	6ed4a4600e77f5dc_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://hereforyoushop.com/Dv	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/vendor.js?v=10210318190529598248a	c51a1ddf68b31515_0.0.dr	false		high
http://https://hereforyoushop.com/n	Current Session.0.dr	false		unknown
http://https://hereforyoushop.com/p	998808883a4f4580_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/infinite-self-love-luxury-bracelet	Current Session.0.dr	false		unknown
http://https://hereforyoushop.com/t;	bba70edea388aead_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://s.pinimg.com/ct/lib/main.d71a97dd.jsa	70747a5c451cd1e1_0.0.dr	false		high
http://https://hereforyoushop.com/products/society-harms-mental-health-t-shirtSOCIETY	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/s/files/1/0481/0922/4087/products/product-image-1526576412_1200x1200.jpg?v=1	Current Session.0.dr	false		high
http://https://hereforyoushop.com/k	b6e0bfd2dc8319e1_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/lazysizes.js?v=6844146596460774066	15e065da0daca7fd_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/readmore.min.js?v=11994212879037969866aD	814f1d3aefbc13c7_0.0.dr	false		high
http://https://hereforyoushop.com/S	b6e0bfd2dc8319e1_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/_	5d760ce477ab20fb_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/readmore.min.js?v=11994212879037969866	814f1d3aefbc13c7_0.0.dr	false		high
http://https://s.pinimg.com/ct/core.jsaD	0b236b7f5bf72364_0.0.dr	false		high
http://https://cdn.shopify.com/shopifycloud/boomerang/shopify-boomerang-1.0.0.min.js	5d760ce477ab20fb_0.0.dr	false		high
http://https://hereforyoushop.com/	000003.log0.0.dr	false		unknown
http://https://hereforyoushop.com/products/mental-health-therapist-t-shirt-1	Current Session.0.dr	false		unknown
http://https://hereforyoushop.com/products/kindness-is-cool-crewneck(KINDNESS	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/society-harms-mental-health-t-shirt2SOCIETY	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/r	6872ce7adcf25f4b_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://schema.org/Organization	Current Session.0.dr	false		high
http://https://hereforyoushop.com/s	998808883a4f4580_0.0.dr	false		unknown
http://https://hereforyoushop.com/t	5d760ce477ab20fb_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://hereforyoushop.com/y	6ed4a4600e77f5dc_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/collections/allProducts	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/z	6ed4a4600e77f5dc_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/bootstrap.min.js?v=7372439028658456128aD	1be31ae4a43afd1e_0.0.dr	false		high
http://https://cdn.shopify.com/shopifycloud/shopify/assets/storefront/features-87e8399988880142f2c62771b9d8	1437dc07a563bc7f_0.0.dr	false		high
http://https://monorail-edge.shopifysvc.com/unstable/produce_batch	576c556eec03cace_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/cartR	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://hereforyoushop.com/products/elegant-self-love-heart-bracelets	Current Session.0.dr	false		unknown
http://schema.org/InStock	Current Session.0.dr	false		high
http://https://hereforyoushop.com/products/its-okay-soft-t-shirt-1	Current Session.0.dr	false		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.6.203.110	unknown	United States		14618	AMAZON-AESUS	false
151.101.0.84	unknown	United States		54113	FASTLYUS	false
151.101.1.12	unknown	United States		54113	FASTLYUS	false
34.68.85.43	unknown	United States		15169	GOOGLEUS	false
142.250.74.195	unknown	United States		15169	GOOGLEUS	false
185.60.216.35	unknown	Ireland		32934	FACEBOOKUS	false
23.227.38.65	unknown	Canada		13335	CLOUDFLARENETUS	false
185.60.216.19	unknown	Ireland		32934	FACEBOOKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.16.193	unknown	United States		15169	GOOGLEUS	false
172.217.16.131	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321428
Start date:	22.11.2020
Start time:	03:40:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://hereforyoushop.com

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@60/214@11/13
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://hereforyoushop.com/#MainContent • Browse: https://hereforyoushop.com/ • Browse: https://hereforyoushop.com/collections/all • Browse: https://hereforyoushop.com/pages/contact-us • Browse: https://hereforyoushop.com/# • Browse: https://hereforyoushop.com/cart • Browse: https://hereforyoushop.com/products/its-okay-soft-t-shirt-1 • Browse: https://hereforyoushop .com/products/mental-health-matters-t-shirt • Browse: https://hereforyoushop .com/products/mental-health-therapist-t-shirt-1 • Browse: https://hereforyoushop.com/products/self-love-heart-necklace • Browse: https://hereforyoushop.com/products/self-love-t-shirt-bundle • Browse: https://hereforyoushop .com/products/kindness-is-cool-crewneck • Browse: https://hereforyoushop .com/products/kindness-is-cool-t-shirt • Browse: https://hereforyoushop .com/products/infinite-self-love-luxury-bracelet • Browse: https://hereforyoushop .com/products/elegant-self-love-heart-bracelets • Browse: https://hereforyoushop.com/products/thick-thighs-thin-patience-pin • Browse: https://hereforyoushop .com/products/society-harms-mental-health-t-shirt • Browse: https://hereforyoushop .com/collections/frontpage

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.43.139.144, 216.58.210.14, 172.217.18.173, 216.58.206.14, 74.125.173.136, 173.194.151.123, 172.217.18.106, 216.58.205.227, 216.58.212.170, 2.20.84.189, 216.58.212.163, 168.61.161.212, 172.217.22.42, 172.217.16.138, 172.217.22.106, 142.250.74.202, 172.217.21.234, 216.58.205.234, 172.217.23.138, 216.58.207.42, 216.58.207.74, 172.217.16.202, 216.58.206.10, 172.217.22.10, 172.217.16.170, 216.58.208.42, 216.58.210.10, 204.79.197.200, 13.107.21.200, 172.217.18.99, 216.58.208.36, 51.11.168.160, 2.20.84.85, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, r3---sn-4g5ednsy.gvt1.com, e6449.dsca.akamaiedge.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, 2-01-37d2-0006.cdx.cedexis.net, clients2.google.com, redirector.gvt1.com, 2-01-37d2-0018.cdx.cedexis.net, www-bing-com.dual-a-0001.a-msedge.net, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, fonts.gstatic.com, dual-a-0001.a-msedge.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, www.googleapis.com, r3.sn-4g5ednsy.gvt1.com, r5---sn-4g5edn7y.gvt1.com, a-0001.a-afdentry.net.trafficmanager.net, s.pinimg.com.edgekey.net, blobcollector.events.data.trafficmanager.net, clients.l.google.com, r5.sn-4g5edn7y.gvt1.com • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\249370ef-920f-4b0b-9e0e-3f9b2f766f1b.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):	162692
Entropy (8bit):	6.083155411217885
Encrypted:	false
SSDEEP:	3072:0A2A2NNCxQM9b0q+szv+tnMIGFcbXafIB0u1GOJmA3iuRp:b2rExQM9b7fD+ZM7aqfIlUOoSiuRp
MD5:	D2122C5DC76E7A7C8C4CFC988EA85EF7
SHA1:	C93E17D7E6687F9F2B1D52BE381E144CEBAC4C96
SHA-256:	370473D3FA8F610DE820730189163BE251E7D0E3C4DB3075CED3F221CB36211A
SHA-512:	BC0580B20535C6DD3B7775AC9B32298D2CF3F969A53DB491E95804A6E9A78DD17CD93EA1503723DB297B7B41B06A257A572765E389241EBDB4D306535BCF504
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":1.606045298496035e+12,"network":1.6060129e+12,"ticks":96489047.0,"uncertainty":4294516.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016785017"},"plugins":{"metadata":{"adobe-flash-player":{"display

C:\Users\user\AppData\Local\Google\Chrome\User Data\2b34ab78-60dc-4bac-ba1a-73b41dfff88e.tmp

C:\Users\user\AppData\Local\Google\Chrome\User Data\2b34ab78-60dc-4bac-ba1a-73b41dfff88e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92068
Entropy (8bit):	3.7512294007711025
Encrypted:	false
SSDEEP:	384:XrcTbJWI55+/aN/r8vrR3s7Z4HhoGwvrK1/7xMV1Rkr+jmeJWB/f3lOVNHNi1328:A61Na1lQ0eLDF14XHOBKTRfsf
MD5:	ECD708B99DA8602A13240BE1300DC95B
SHA1:	6DF22CF910EB090B5F6E26FA223D1AB0B3AF5C30
SHA-256:	CA3BEF2BD0D913B176F79F90CDFBB445C8BA69291871851610B5C695209E79D3
SHA-512:	AFE6A30F313D15CF884A6546E4EEEA156569C2042356CAB7B49C08B66EA534293F210F4C31A83C97B5A1964AC64FB1C55D262A449F76FB25FBC1B2A1BB5D55FB
Malicious:	false
Reputation:	low
Preview:	.g.....*...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\2f531ef8-eeeb-4f0f-8832-923c48fe55a1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94052
Entropy (8bit):	3.751858008386486
Encrypted:	false
SSDEEP:	384:YrcTbJWI9S5lViY/aN/r8vrR3s7Z4HhoGwvrK1/7xMV1Rkr+jmeJWB/f3lOVNHNc:+O61Na1lQ0eLDF14XHOBKTRfs9
MD5:	2BF9951AB23EB129B9AEEA3DDB447C64
SHA1:	3FDAA9E9D37F9BA84A0125B6D73BD52AB453718D
SHA-256:	4F7B60D7F786E65CF2118C364F2CD518FEB6DD2DC8535E501BC41605B609ED66
SHA-512:	81122863D0B047227696F8CC5F79707BB0AC1B431C67629D8303477283A5732A62F1DD16A896A36344C7436061F302060A80850929BCA5B80727A869919F22E9
Malicious:	false
Reputation:	low
Preview:	`o.....*...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\4b213a39-2965-4451-9a51-2b7126404cdf.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):	162441
Entropy (8bit):	6.082729457733012
Encrypted:	false
SSDEEP:	3072:vTnA2NNCxQM9b0q+szv+tnMIGFcbXafIB0u1GOJmA3iuRp:bnrExQM9b7fD+ZM7aqfIlUOoSiuRp
MD5:	4638FC2D288C00A9A4F90D6BC24BBE93
SHA1:	871D8C908F1019FE67CEED5405BC0EF36A99E512
SHA-256:	D611EBC892C8CFACED4A6575ADACB4233C2D734A397690346A87864B41D2D1B5
SHA-512:	0F2756D4E892DD4EB64BC8D0C4CDF92F8CD26A8F80249E9A8C6490B159C6BF7E226DFB96ACDA0CAC4412333C1A3B57055CA8EF2E4D52A4CAB5156F577B46834
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":1.606045298496035e+12,"network":1.6060129e+12,"ticks":96489047.0,"uncertainty":4294516.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"display

C:\Users\user\AppData\Local\Google\Chrome\User Data\59b5bf53-2f73-46c1-859d-87271f8df6a9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\59b5bf53-2f73-46c1-859d-87271f8df6a9.tmp	
File Type:	data
Category:	dropped
Size (bytes):	94772
Entropy (8bit):	3.7516523162644857
Encrypted:	false
SSDEEP:	384:GrcTbJWI9S5lViY/aN/r8vrR3s7Z4HhoGwvrK1/7xMV1Rkr+jmeKUWB/f3IOVNHu:wO61Na1MQ0eLDF14XHOBKTRfsN
MD5:	8B6DECF224697093614E98CCD0B285ED
SHA1:	EEE3017FF7F36B0AB84EB2864908D419AE2EADA1
SHA-256:	3269B66997C3FD28795C307263CB18767F081749195E7ED9BEEE0657E3376536
SHA-512:	0DC39453EF79AA6440FE59177A4BE024F39E6AC790B8976E8F5FCA688C9EBD97C56DE7950FD90F79A39953C62C1110727CA6DC80762ABD4C6A33BB810DEC8DC
Malicious:	false
Reputation:	low
Preview:	0r.....*...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\5ae0deeb-e1a9-4e51-ab70-dbf90750197a.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):	6.082726818179956
Encrypted:	false
SSDEEP:	3072:0vUA2NNCxQM9b0q+szv+tnMIGFcbXafIB0u1GOJmA3iuRp:YUrExQM9b7fD+ZM7aqfIlUOoSiuRp
MD5:	55D3D43A5A9B0909A3FB382BECD796E8
SHA1:	A86757C0695A78745B77BD575C2284459C74C5C2
SHA-256:	A6E31C4AA3F8E20D8C23349EC806DE2FD52EC46E131D4C12C03B1428EC002863
SHA-512:	76A47851296E3DB8D9A639ADD1CFE9C5F91BCCB522844833C6065B93C9A09AA2195A106D84E539165C03D0263763118C0AF8558AAD96999FD9FB95DA1D22FE3
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":1.606045298496035e+12,"network":1.6060129e+12,"ticks":96489047.0,"uncertainty":4294516.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016785017"},"plugins":{"metadata":{"adobe-flash-player":{"display

C:\Users\user\AppData\Local\Google\Chrome\User Data\6927b8e5-2692-4f59-8ac1-b49678c26b44.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):	162441
Entropy (8bit):	6.0827274883299545
Encrypted:	false
SSDEEP:	3072:vCdA2NNCxQM9b0q+szv+tnMIGFcbXafIB0u1GOJmA3iuRp:qdrExQM9b7fD+ZM7aqfIlUOoSiuRp
MD5:	494459FBFD0AD86E9F1C4F15A5B95C91
SHA1:	960891B331EF795CB055E3567335914F2958854C
SHA-256:	D3F471873431A1D9F6748B1FC85E2C5EC930ABF85DEC633048303BD71D823E55
SHA-512:	80AE62EF8969DE081BDE49D8028893380CCD1B5FEF8F3942B69D385C59E85B89BE5A737A5A7DC53B825712C9DFE124B70501D3711D1B0E2734ADFFE8521B954
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":1.606045298496035e+12,"network":1.6060129e+12,"ticks":96489047.0,"uncertainty":4294516.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"display

C:\Users\user\AppData\Local\Google\Chrome\User Data\6cd7cfe7-b841-4028-bfab-3cd5e6724986.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\6cd7cfe7-b841-4028-bfab-3cd5e6724986.tmp	
Category:	dropped
Size (bytes):	162440
Entropy (8bit):	6.082726840109263
Encrypted:	false
SSDEEP:	3072:vYHA2NNCxQM9b0q+szv+tnMIGFcbXafIB0u1GOJmA3iuRp:wHrExQM9b7fD+ZM7aqfIlUOoSiuRp
MD5:	8B575FC578A0BB9848D2D1F2D85EC0D3
SHA1:	3E5042CFC79372278233CED7F3DF4555729A4B8E
SHA-256:	896E5EA31B71D1AF541822B4B2968CA3C3022BA7B61E9C6615D677D7937BCD70
SHA-512:	8AEA42364A47B15A4B87C485A7B3C5F620FFB27DD390703EA28C3E8CDE9D23A900B8475D22051EA678EAB883B393159846C0E42EBF68E407ECEB84A32CFDDB83
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":1.606045298496035e+12,"network":1.6060129e+12,"ticks":96489047.0,"uncertainty":4294516.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"display

C:\Users\user\AppData\Local\Google\Chrome\User Data\7e230694-752d-47d2-86d9-e9bddbdc1a2b.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):	6.082724019025458
Encrypted:	false
SSDEEP:	3072:0h2A2NNCxQM9b0q+szv+tnMIGFcbXafIB0u1GOJmA3iuRp:22rExQM9b7fD+ZM7aqfIlUOoSiuRp
MD5:	F27E2C796124BD07982E728B15396980
SHA1:	C939D0FB83CA7F1068626CC18CA36118DBAE2007
SHA-256:	D037AB054CFD831897D64E9D084D980C30B198F9CD6AA85EB23F40F85519D140
SHA-512:	41AE68A1BAA8AE7A179F0125F60040CFAACF959AE5B5B87E7E5FB294F59E44485A7EE356925E29759E96EB5100A3C39CAF698C396239069F078ADF83FF0ACCFB
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":1.606045298496035e+12,"network":1.6060129e+12,"ticks":96489047.0,"uncertainty":4294516.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016785017"},"plugins":{"metadata":{"adobe-flash-player":{"display

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\041e4a77-1f7d-4b98-b751-aa54b2b1c313.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):	5681
Entropy (8bit):	5.193421211068794
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\041e4a77-1f7d-4b98-b751-aa54b2b1c313.tmp	
SSDEEP:	96:nCVF7f4RMPpQqcVx6ok0JCKL8xkU1AbOTQVuwn:nWR4gQqct4KykUE
MD5:	79805752FAFD81C05854EBE58F135C02
SHA1:	F889CC9A9E926A81C512D1EFED2704B46B160248
SHA-256:	27A80B36CBFAEE9CAA5F9F074D755D54741AF401DEA57D1E83BF5377E7DD0ED4
SHA-512:	18D4A936A708E937485BF66F7DD5939EDFBE8B4ED255B2123156987F85BBED498E20F7AF7C294C08F5904C6D0AF2D2A954AFEAAB07D1BD6E646CFA924D063F 4
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250518895990780","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",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\085dab5f-e2a8-4406-a215-a48f5f42dc5c.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):	3653
Entropy (8bit):	4.882326487926205
Encrypted:	false
SSDEEP:	96:JOXGDHz5bJi6bItcBfZmGFG/GpUGEjUtUgs6v0hH:JOXGDHz5bJi6M6DmUEIUBjUtUgs6v4
MD5:	074CB767876B7D471849D08DE711715B
SHA1:	7182D6C4A5CAD165FD7C33B59E23039B475C0EDD
SHA-256:	53816A9FD4FBBE348842B1DE0F9451F0B3759E9A26E565849AFD94348215877B
SHA-512:	3C9940359BBDA3D59396F650950B8329586BBEA01C7CFE3F46F6C2A4DBCBEB5DCDBC6D67553EF61F25990DE25B7566F8EB1351DD3BAD3EC24909BC81D5F26 10
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.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":"13253110898303927","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253110898311731","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253110898528768","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13253110898528770","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0a3549c1-154b-4792-a56f-0651bb26e606.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):	2125
Entropy (8bit):	5.59375497834693
Encrypted:	false
SSDEEP:	48:Y1ujEiHdZ3HUd6UUh8EUIHdHU0CwU3KUdqPeUer2UefWwUUUepUd:TjEMdZUUUUvU+dHU0vU3KUoPeU9UETUl
MD5:	3A466138F93E0A2B5A1AC02857AB66CC
SHA1:	72AD2F5BDDD9E5F7A64C118C248F85D4C3456343
SHA-256:	ACDA486F8BC27F462C62B8D34E7A4F23B0834284CA25BC7AF5664E704804D563
SHA-512:	3B2A83026210A5C5090C881A0B6065AB62541FF73B8A6949FCB6F45E4291E4127B52F5A6197D11F7D0DC322BCEFD37C89A6FB608756BEB547EF4603CE704BCF
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606650168.410006,"expect_ct_observed":1606045368.410006,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","nik":[]}],"sts":[{"expiry":1637581368.117772,"host":"HFBiDP29QImD8tsB7lDVLwtFW1q+2JoXdNXZBg4nogg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045368.117776},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1637581368.450363,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045368.450368},{"expiry":1613934606.409995,"host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606045368.409999},{"expiry":1637581364.005725,"host":"WhnJUA5xp3SC0QTjQcML3o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\12d3c9cd-1bf9-437b-a472-e5426d3eeffb.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):	2124
Entropy (8bit):	5.593951569680122
Encrypted:	false
SSDEEP:	48:Y17iHdZGUX6UUhjEUIfHdHU8m1wUCJKUdqPeUer2UefWwUUUe2hUNCF:aMdoUKUUyUI/dHUFWUMKUoPeU9UETUUc

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\12d3c9cd-1bf9-437b-a472-e5426d3eeffb.tmp	
MD5:	A78053AA4038B0664C5AF0BE8359B05A
SHA1:	066F3C7C498B0A38945C660962BB9ED1A1491DAA
SHA-256:	B92BAEB8E5E3E1142CC8138E21D978E19B7A3CA8BA3A88C143852198CD5C4A11
SHA-512:	04BC9ED11B38712C836637B69FDE8EE37588BB2F2A28847AB5D271903EA0BB923965BF20629AEA66AC2DE9A945A92F167B7EE5619A150D0C12B65784B9B7C01B
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606650116.572719,"expect_ct_observed":1606045316.572719,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","nik":[]}],"sts":[{"expiry":1637581317.608336,"host":"HFBiDP29QImD8tsB7lDVLwtFW1q+2JoXdNXZBg4nogg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045317.60834},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1637581317.932053,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045317.932058},{"expiry":1613934554.572704,"host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606045316.572708},{"expiry":1637581316.786928,"host":"WhnJUA5xp3SC0QTjQcML3oD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2d4442a6-cb8a-4427-a1ea-811da7ff7ddf.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):	2125
Entropy (8bit):	5.5926012170369335
Encrypted:	false
SSDEEP:	48:Y177JiHdZQ0Ut+6UUhS+EU0HdHUAJZwUNKUdqPeUer2UefWwUUUeCUs:e7JMdJUtjUUgUCdHUm6UNKUoPeU9UET0
MD5:	6CE1A90B3B1F30599AC7093635C6C530
SHA1:	464023418E8F5E7671C85B1CD7F86B12DFA93019
SHA-256:	B04F4F7CAA4C02EFCDEFDBF5C6B5927CF539FFE34CB9E0F7C715E90F5D8E461A
SHA-512:	3C38FA2BB6A49CF71ACB692F5F9F67BC0EE21E787AE9DFCEFCF50DB8D011AD73416B910EB35A0702A6A5EA057534DD3033BD45B81502C96F3A66B5E4ACAE366
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606650149.135357,"expect_ct_observed":1606045349.135357,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","nik":[]}],"sts":[{"expiry":1637581347.065027,"host":"HFBiDP29QImD8tsB7lDVLwtFW1q+2JoXdNXZBg4nogg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045347.065033},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1637581347.348897,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045347.348901},{"expiry":1613934587.135344,"host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606045349.135347},{"expiry":1637581349.347661,"host":"WhnJUA5xp3SC0QTjQcML3o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3e379afd-6365-4349-90d1-b5f01ead71ef.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):	16763
Entropy (8bit):	5.578630626092019
Encrypted:	false
SSDEEP:	384:apRttLlaUXM1kXqKf/pUZNCgVLH2HfDyrUEgOiYDlp4B:mLl9M1kXqKf/pUZNCgVLH2Hf2rUVYp+
MD5:	D4DB55685BF0806163F688C55532ADFC
SHA1:	3DB255451356F5A5C6125501876AB8B0C7EFFB80
SHA-256:	E622B62A8083BC7CF81D6B884095417940E15E3DA8B55BE041B811BD237D66C8
SHA-512:	BE687F5BD9CF00F5A015BEF28D3A2D9D3273666A1FAD7B4D88AD3E1957F28A70370DC4FF6E39E8FD213B14B08B7DF8E0E9DF1D8B0A874A3DBC95EC4503071D97
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":"13250518895749224","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4564e511-a27b-4738-9538-4c7f75dd468f.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):	5682
Entropy (8bit):	5.193221988597653
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4564e511-a27b-4738-9538-4c7f75dd468f.tmp	
SSDEEP:	96:nCVF7f4RMPpQqcVxBok0JCKL8xkU1AbOTQVuwn:nWR4gQqco4KykUE
MD5:	2BCB99F1D2576363882501BAB6B8C654
SHA1:	0ECAE2F5CCD9EF9F1EA3A85610B3BD4B048FFED4
SHA-256:	E8E334C56A0AD650F395B44B7F86A48CE550EEB234E45CDF34D1A9A74B3A527B
SHA-512:	799A3D2881DE32A207A9C7FFA294C2D2E6B138C6D52C36740AE316E2C19D69F82664D3CBE92C274BE0346DE4923180FC8C5FEFCA79C74F719305B2F58B18903
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250518895990780","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcom e_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":1 0,"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","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\45921a99-a900-4bb3-aa55-cf4e939b5ad4.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"},{"advert ised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","support s_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":"1324854350 1454994","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\58e554af-3cbf-4d53-a439-cdac933807f4.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):	5708
Entropy (8bit):	5.195784804693402
Encrypted:	false
SSDEEP:	96:nCVFCgf4RMPpQqcVxybok0JCKL8xkU1AbOTQVuwn:nWgW4gQqcN4KykUE
MD5:	1F55E4DE39F7F176159021867107B0E1
SHA1:	E33F6D2E3E0FF0B54BD269B87A72FCBF3E6C3412
SHA-256:	205ADC4DE21F98860869C0E4AA8438592FC0BC2B94C6D3B4A5CB2E9527C88954
SHA-512:	FAEE7AF77B42A37CCE5C95FE106DDC5C37DAB2E0542962CE1A53802B4A23DCEE18EA5FE2DD239A284B987C3624972586E1328CFFDB6146FD14D61AB9715795 25
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250518895990780","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcom e_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":1 0,"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","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\5e309bd2-e5ae-4b1f-b203-aa7e0b8ad46b.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):	2125
Entropy (8bit):	5.598597032984414
Encrypted:	false
SSDEEP:	48:Y1ViHdZQUr6UUhoEUXHdHUEwUC/KUdqPeUer2UefWwUUUeaU9:0MdmUuUUrU3dHUJUC/KUoPeU9UETUUUK
MD5:	7577945365BBE90F937399D27DEBD18F
SHA1:	25723944B1A24BB6482EB16E3B66460BB9FEAB99

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5e309bd2-e5ae-4b1f-b203-aa7e0b8ad46b.tmp	
SHA-256:	7462677966D1D6CD371BF1816A72D2F578F5E6B6F130002F472360B86D99514B
SHA-512:	02CA0EC06220FEE076CDC5CFCF793708C4EA420CF6291A78AFE5BF26CE9B30A60090F6D135EDE8CA5836A7A41C7256F9050431E7B03B1855A89BCECEA9E1B01D
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606650126.875867,"expect_ct_observed":1606045326.875867,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","nik":[]}],"sts":[{"expiry":1637581328.138293,"host":"HFBiDP29QImD8tsB7lDVLwtFW1q+2JoXdNXZBg4nogg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045328.138298},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1637581328.581443,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045328.581448},{"expiry":1613934564.875853,"host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606045326.875857},{"expiry":1637581319.130413,"host":"WhnJUA5xp3SC0QTjQcML3o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5fb9ffee-f460-4579-8090-8eb763260b1c.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):	5682
Entropy (8bit):	5.193578715340854
Encrypted:	false
SSDEEP:	96:nCVF7f4RMPpQqcVxlok0JCKL8xkU1AbOTQVuwn:nWR4gQqcs4KykUE
MD5:	B4550BBAB05E36D3D699D5A6C3DC7AE5
SHA1:	622BEB9503098CD2E3DC4A21FE12095D10C9B36D
SHA-256:	8143523C3EA2FC0ADC234A9DF2E862D8D00ADA7EE18D1BED3462365C2BBB61EE
SHA-512:	2A81643E030D43443DE3EA0B23D4067535E958DA97D1AA5C9F07A4A64E40394D5BCB2446DF5107D1C24D2B773D0BCBE754407814D0E94AC497142F065BC5496
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250518895990780","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","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",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\85cef5b8-75c0-4916-a2a8-3a37f2e72737.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):	2124
Entropy (8bit):	5.596432155031589
Encrypted:	false
SSDEEP:	48:Y1diHdZZUbI6UUhPEULHdHUPwU1KUdqPeUer2UefWwUUUeyU+:kMdXUbBUUyUDdHU4U1KUoPeU9UETUUUx
MD5:	0A1B30D3D1F58639EC4BB12C48777B02
SHA1:	356561592A85D8AAB2F6F33A72FE53176190CA99
SHA-256:	279C1FA1013A48012B5B3FF2CAB562C5D426CE299379D2F015220D3E79A17B0F
SHA-512:	618FB226554A8F2B76F0545221C72A84C01B0E213E9A3627A7FBE9CC6086FB0A9C13E3669C0ED013A1286E457045651DC8B8FF70D7AAB7C67D93EB1FD9C15D0
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606650138.874878,"expect_ct_observed":1606045338.874878,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","nik":[]}],"sts":[{"expiry":1637581335.735846,"host":"HFBiDP29QImD8tsB7lDVLwtFW1q+2JoXdNXZBg4nogg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045335.73585},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1637581336.056387,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045336.056392},{"expiry":1613934576.874864,"host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606045338.874868},{"expiry":1637581339.088054,"host":"WhnJUA5xp3SC0QTjQcML3oD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\89fc8a1f-302d-46b2-85d5-fe713e5f60dc.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):	2125
Entropy (8bit):	5.598046676148603
Encrypted:	false
SSDEEP:	48:Y1BiHdZaUY6UUhDNdEUpHdHURwUTKUdqPeUer2UefWwUUUe9U74w:AMdsUxUU9cU1dHUSUTKUoPeU9UETUUUl
MD5:	9384A274CDCF269C067315F4F252E8A0
SHA1:	DB43C188CB7334C02D6A0D88725005E52FA84C0F
SHA-256:	7B511D5BE19E484FF3CA8A8A2E26BDFE8B579754A536965F5ED2403ADBE9F72C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\89fc8a1f-302d-46b2-85d5-fe713e5f60dc.tmp	
SHA-512:	141B4C4EFBF5F3547448C819D99624C04395FADC2214323AEFA580336B51466DB8813670A99DCDB3623196FFDF3508767D2A678C9EA9BC7415DB77B1FD5A8B9
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606650158.962535,"expect_ct_observed":1606045358.962535,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","nik":[]}],"sts":[{"expiry":1637581358.036965,"host":"HFBiDP29QImD8tsB7lDVLwtFW1q+2JoXdNXZBg4nogg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045358.036969},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1637581358.421239,"host":"TZmujbl93Yt3Jl8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606045358.421244},{"expiry":1613934596.962523,"host":"T5AcgYcH9l2Z1a3JL5NWYpr+A+aKlk8e2eQ5R4y8JaE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606045358.962527},{"expiry":1637581359.508152,"host":"WhnJUA5xp3SC0QTjQcML3o

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):	331
Entropy (8bit):	5.225737739352505
Encrypted:	false
SSDEEP:	6:itBL+q2PWXp+N23iKKdK9RXXTZIFUtwRWZmwyRSVkwOWXp+N23iKKdK9RXX5LJ:i2va5Kk7XT2FUtwRW/yRq5f5Kk7XVJ
MD5:	45EA39AD6A796E19F7F5B1EE9431FF24
SHA1:	FE491DCDBDA3B535006DC912683F7EB4C33238D0
SHA-256:	EE1F6C5CDB0AD194DE07245571E3FB9CA183EECF8D008B761D8D18B117287FB7
SHA-512:	E17CEA9DB3793FC9004B61CDEC6BC73BB8E8CB33991264D934859B5B656BCF5684F58AEE2ADB6BACAB1A954F3C5B728B7E9E9C21C08681BAA28DBF364C713357
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:49.014 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2020/11/22-03:41:49.015 dd8 Recovering log #3.2020/11/22-03:41:49.015 dd8 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):	315
Entropy (8bit):	5.202015872047732
Encrypted:	false
SSDEEP:	6:iIT+q2PWXp+N23iKKdKyDZIFUtwRISXZmwyRI9VkwOWXp+N23iKKdKyJLJ:izva5Kk02FUtwR//yRM5f5KkWJ
MD5:	A5329CBE75DC425D36C4E52D577D87A1
SHA1:	7D06376A02CBA8B82CC9BD89E8C7928D013863B1
SHA-256:	C760589994F0D21404235F6309C1C748BABA649D50DA737C10A3D2B002D81769
SHA-512:	F2B82532A4D6F746044BE3E579681B92163AC2D1C660D27C56929CF7F6600FDCDD9B3FDEA8F843D201C106AB57AE3A9E7576F229F1DBD5FF45C3CF171E5825F
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:49.006 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2020/11/22-03:41:49.007 dd8 Recovering log #3.2020/11/22-03:41:49.008 dd8 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\0b236b7f5bf72364_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2440
Entropy (8bit):	5.432101209698512
Encrypted:	false
SSDEEP:	48:yJu2VnayPB9AOtVrnNv4MtdLiBwHyLWhqEqw7hszlbxOzRQP:kVayPBmOtVrnN4+1lUX0WBbiq
MD5:	777DB7EB70662F015FB5ECA2CEC35F8E
SHA1:	F8E0AEDC9661F569191B6B4764B287B6A1709D4E
SHA-256:	43129F1DFF6445028BB020B93EDFF901761C8E86B8DCDA0FD14A2350874D5091
SHA-512:	7E87406CB77EB5D80C4DB77EDC858B7BEE083D5A234D29244EB68C4CC29BAB472E8C25F9BE76DAC5AA5AD55383409FC1182DF5644211EBEFE23D465B9798CC8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0b236b7f5bf72364_0	
Preview:	0\r..m.....@...._keyhttps://s.pinimg.com/ct/core.js .https://hereforyoushop.com/.O..F./.....}.....r.J..6s.C.n&E..M.{..,8.I..8N..A..Eo.....Q.|.....A..Eo..... ....O..F./.....'.v.....O....@.....(S.D..`>.....L`.....(S...`.....LL`"....@Rc.....Qb&.....e.....Qb6J.....r.....R..b$.....I`....Da.....(S...`.....L`.. ....Q.@..-.....exports..$..a.....S.C..QbF.E.....I...H..I....a.....Qb^.....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...& ...&.'..W.....-...(.....,Rc.....`....Da@...8.....a.....e..... P.....@....@.-....,P.....https://s.pinimg.com/ct/core.js.a.....D`....D`F...D`.....<...`....&...&....&....&.(S.....Pb .....u.d.a.....l.....d.....&.(S.....Pb.....u.r.a.....l..a..d.....&.(S.....Pb.....u.t.a.....d.....0@..I..d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0e0db2eb3425f0d0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4541
Entropy (8bit):	5.43456929286074
Encrypted:	false
SSDEEP:	48:3XLETdXLJhgdXLuQ4dXLcfdXL8DtzdXLV1jdXLojgdXL4MdXL/fdXL31LdXLF0dH:3eKoiAX5XlpRzT8NE6mzBbyqe
MD5:	F30CC13BBB81E636D42E0065834D72FE
SHA1:	F4162BA4BBF3BB66BEFD9371C4C6847FE7C1AE0E
SHA-256:	0AB9FFD720BBC66AE19A1D3CFBCFC9422C895765E81341079771BA0738C47A17
SHA-512:	4BED7215CAB49E26081CDD77894B7D0BB6CF7F2E3F1BC93490E00E2C742B6F1D5B1A5C774D70DF428B41B762C4B4D798D701D1951F05F75ABDB8ECB85ADE8 24
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...ZR....._keyhttps://sellup.herokuapp.com/upseller.js?shop=imhereforyouco.myshopify.com .https://hereforyoushop.com/..).F./.....*.....J..v.l.r.]?.<l..~v.. ..Xd.e.FZE..A..Eo.....[.....A..Eo.....0\r..m.....k...ZR....._keyhttps://sellup.herokuapp.com/upseller.js?shop=imhereforyouco.myshopify.com .https://hereforyo ushop.com/2...F./.....q.....J..v.l.r.]?.<l..~v....Xd.e.FZE..A..Eo.....=.....A..Eo.....0\r..m.....k...ZR....._keyhttps://sellup.herokuapp.com/upseller.js?sho p=imhereforyouco.myshopify.com .https://hereforyoushop.com/._..F./.....J..v.l.r.]?.<l..~v....Xd.e.FZE..A..Eo.....v..0.....A..Eo.....0\r..m.....k...ZR..... _keyhttps://sellup.herokuapp.com/upseller.js?shop=imhereforyouco.myshopify.com .https://hereforyoushop.com/.E,.F./.....J..v.l.r.]?.<l..~v....Xd.e.FZE..A..Eo..... .....A..Eo.....0\r..m.....k...ZR....._keyhttps://sellup.h

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1280eaf7baf34351_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	34195
Entropy (8bit):	5.5755724042505586
Encrypted:	false
SSDEEP:	768:tnkRilchDC4Tgud8YGC98i7qmlDng79o2+cgMYGc:WRifm4TVdK9xmlDg79o2kb/
MD5:	297CB6DB2E1872952021591913C084AC
SHA1:	BFA149A3DAD5FE162CFECA8EBD6DEF7F58902E6D
SHA-256:	E9D2C92647004F01D637A14B0610731B5E075D45F84C50161FB19F87C793FFCC
SHA-512:	F8C006B72A7F95503C1F70383DABD28141589F87ED3784883E6DB184A909640DE3429A59A6A8AED7250DFBDBE6BF481C8C9D9940E8C35C2D8E3DDF78D847B7 D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{.....5....._keyhttps://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/theme.js?v=7548532355862316605 .https://hereforyoushop.com/J...F./.....-z.....5.| ..w..>..e.4.#Y..).. ..h0.R#.A..Eo.....A..Eo.....'..b....O.....X.....(S.E...`@.....L`.....<L`.....(S.....Ia.....$Qg*. .....onYouTubeIframeAPIReady.E.@.-....hP.....Z...https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/theme.js?v=7548532355862316605..a.....D`....D`....D`.... .I....` ...&...&.(S...Ia....e.....Qc2.....SectionsE..A.d.....&.(S.....5.a....).....QcB.....theme.....a....$.....a....#.....3...a.....a.....QbB*.....,.....a.....a.....Qc .....assignIn...a.....Qe.....,_createInstance.a.....q8E.d.....&.(S.....a....(.....a5...a....#.....a....".....a.....a.....6...a.....a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1437dc07a563bc7f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	63092
Entropy (8bit):	5.5666842737847055
Encrypted:	false
SSDEEP:	1536:nHMcmMPUpUAoYDAN7ATJUKcUvKz94zmQis:scPMpUAoYD8MJUKcUvKzezm/s
MD5:	55DD65964A9BCC0AE41A7BB496F222FD
SHA1:	4C130F0FAF43B11DFF1CAFBEDC5AB6E2A51BF099
SHA-256:	8803ABFAD1ED41B55512CCE9C0C26A0AC9999689C3831C8F6EDC2AFC8EE266C8
SHA-512:	FA53375477103FF66685D6784A4476156026DA9C82DAFF300B89C731FB58C1B63B16EFA46ECEEC31A14DFE613DD642B3081DF55AACF05BD11D376E3B905D9FD E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1437dc07a563bc7f_0	
Preview:	0\r..m.....<.D...._keyhttps://cdn.shopify.com/shopifycloud/shopify/assets/storefront/features-87e8399988880142f2c62771b9d8f2ff6c290b3ff745dd426eb0dfe0db9d1dae.js .https://hereforyoushop.com/ ...F./.....{.....7ES.....,...:..0..+..O....f.A..Eo.....W.....A..Eo.....'.....O....`....~b.....4.....P.....(S.L..`N.....L`.....(S.e..`~.....L`.....Rcf.....Qb...'....d.....Qbb|.....v.....Qb".....T.....Qb.~.....o.....QbF.E.....l.....Qb::.b....j.....Qb>."...F.....Qb.G.....k.....Qb>.C5....h.....Qb.#.W....m.....Qb.l.{....p.....O...R....Qb..50....c.....Qb.H.....y.....S...Qbrt.....E.....Qb>.....O.....Qb.&.Y....B.....Qb.xF.....L.....Qb..2....s.....Qb.-v\....f.....Qb.....n.....Qb..?1....M.....Qb.....C.....Qbn.5.....I.....Qb.s.....R.....Qb..G.....D.....QbB*....._.....M...Qb.....w.....Qb.6.`....x.....Qb:."....A.....Qb&....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\15e065da0daca7fd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16543
Entropy (8bit):	5.807162207671899
Encrypted:	false
SSDEEP:	384:K3n0CqYg2l7lF+OfLVMaldaO3ft32UIO3rldu8K7Wu38X:K30Gj7IlwCalx3ft3tI8lddK7WoS
MD5:	108FAC576FF8C2FF6788B9131C991ECA
SHA1:	4F050CE85BABBAF95E55209C8B96D7605EB0B094
SHA-256:	299968670B0AA4364F77E592D3897BFCC8CBAB00948F96D2882DA08D253657C1
SHA-512:	B423744059E9258D3ED44BF5FD53FE99D4F962AFE6BAF5BF397FFB2B995A25E9604D2EFB3D8D1B524AA9E0035E82BA6EF6B9A83ADB0A13679AA53FF4EB382D6A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....unH2...._keyhttps://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/lazysizes.js?v=6844146596460774066 .https://hereforyoushop.com/.@..F./.....{.....<-..cB..@.....j...^*!...2....A..Eo.....m,-.....A..Eo.....'.RU....O.....>....F.....L.....(S....`.....0L`.....(S...`.....LL`"....hRc0.....M....O...Qb...'....d.....Qb.-v\....f.....Qb>.C5....h.....S...Qb::.b....j...g.....I`....DaF.....(S.....Ia=.....A..@.-....lP.....^...https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/lazysizes.js?v=6844146596460774066..a.....D`....D`<...D`.....!....`....&...&....&....&.(S.....Ia....-.....i .....@.....@.....@.....@.+.....O...A.....d....@.....D&.(S.....Ia.....I..d.....@.....&.(S.....`.....lL`2.....Rcd.....*.....M.....Qb&.....e....!.....a....S.....Qb.G.....k.....QbF.E.....I.....Qb.#.W....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1be31ae4a43afd1e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22299
Entropy (8bit):	5.7021904204875105
Encrypted:	false
SSDEEP:	384:hEDCb4+eHWhBtTZGOT4q8yDQRH1y740DHziWK25bR15E9u:hEY4z2h7Zx4qlDQbaLzia5lTJ
MD5:	5DA438C91F09C0CB7A37BE18595A367F
SHA1:	4DC8242E66CEAA95E014C4BD2940066CBAF26D5D
SHA-256:	D2CC8D8C5D38D13FC064368DCCCA11FC9A0013A1AC64FBABBD1AF6BD371CA2A5
SHA-512:	FF666064ADD09DD88525683006E56BB91C836CBE082E76521CB5BF3E993EDE5B2E94649B754B4BAAFDC9F922B2597E8219577695CB3D657F2EA6C35CABD210BA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z..`...._keyhttps://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/bootstrap.min.js?v=7372439028658456128 .https://hereforyoushop.com/^...F./.....2z.....1..j...).....-.2.S[p.w.....A..Eo.....aV.....A..Eo.....'.....O....`U.._%.....L.....(S.....`.....HL` ....Q.@r.{.....jQuery.....4Qk.ui8&...Bootstrap's JavaScript requires jQuery...(S...`0....$L`.....Qb..F....fn....Qc.....jquery....Qc.....split.....K.....dQw"...X...Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4..K`....D...(.....(...&.(...&...&.Y....&..*..&.(...&...&.Y....&..*..&...i.....*..&...i...8..&..*..g.....&...*..g.....*..&...i.....*..&...j.....&...&.%.e..."......(Rc.....l`....Da....t....$..g$.....P.. P.. ..."..."....@..@.-....pP.....b...https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/bootstrap.min.js?v=7372439028658456

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2eaa7ed6113c80dc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4009
Entropy (8bit):	5.545594975424936
Encrypted:	false
SSDEEP:	48:8K5NCKcCKkCKECKhVWCKaCKttCKYCKICKHCKYCK2CKYCKdCKUCK2rCKCCKBCK8K:8TCSugkyk2GnCwCB6A8Z
MD5:	F016D90F8A3ABBB5718D6DF4E8A1CAFE
SHA1:	48107F8CE1027B5E00C2171E26875F8E152029BE
SHA-256:	5049B9DD9C5141CAB7F4476AB1F104A45264FEF7B169041552928BB50D1A6175
SHA-512:	35437F9E7C561B2DBF9DD461E091CBC39E90B10FFB5BAD670ADA96BEA1CB73D3F158E9086A9004436092E943AA15B396C6EE2532FBE66C732B4FBD5E3E54D952
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2eaa7ed6113c80dc_0	
Preview:	0\r..m.....O...h!....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://hereforyoushop.com/.X..F./.....|.....d.H....<..c....5O....A..Eo.....3,]..... .....A..Eo .....0\r..m.....O...h!....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://hereforyoushop.com/....F./.....6.....d.H....<..c....5O....A..Eo.....4.+..... ..A..Eo.....0\r..m.....O...h!....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://hereforyoushop.com/<_..F./.....d.H....<..c....5O....A..Eo .....F.....A..Eo.....0\r..m.....O...h!....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://hereforyoushop.com/.=&.F./.....W.....d.H....< ..c....5O....A..Eo.....S.7.....A..Eo.....0\r..m.....O...h!....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://hereforyoushop.com/'.D.F./..... .....d.H....<..c..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\576c556eec03cace_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	72504
Entropy (8bit):	5.715177937701449
Encrypted:	false
SSDEEP:	1536:jNXz6eBNjGuo6KCr/PuJ2LFR4yakQw7dVo:B7BNNoaNSbGo
MD5:	BBE8A76065C199D9793005936CFE7781
SHA1:	BF028D680171C87D6C1F5407A54B4836E257080D
SHA-256:	09170C5053D7D9C75638AA47FCBAE245C57E276E460001F8AE6C69BFEFBA6971
SHA-512:	BCC31C69FB78EEF7FA90F195A7E2B500C29064E06DF7E245C20A2BA9A0CF7F293FF5F0DE95DB515ACA65CFD40B2C90E6B3F954B6061462A475CEB71932C6FF 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....c....88E6B4C3C82B1D92E2F7FB8CEBEA23149C3800AF8E5787F3FC24ACF1A628AC8D.....'..*....O.....F.....p.....D..... .....X.....(S....`.....L`@....(S...`.....LL`"....@Rc.....Qb&.....e.....Qb.'vY....t.....Qb.....n...b$.....I`....Da.....(S...`.....L`.....Q.@..- .....exports..$..a.....S.C..QbF.E.....I...H.....a.....Qb^.....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&..(...&..(...&..'..W.....-... (.....,Rc.....I.`....Da@...8.....e..... P.....@....@.-....hP.....\...https://cdn.shopify.com/s/trekkie.storefront.3bc22f7b201bea3154c99666f2373bcf9a3e8fb1.min. jsa.....D`....D`2...D`.....`....&...&..A.&..a.&.(S.....Pb.....n.d.a.....I...q.d.....&.(S.....Pb.....n.r.a.....I.....d.....&.(S.....Pb.....n.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\589454532e0beb88_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	389
Entropy (8bit):	5.788959033577932
Encrypted:	false
SSDEEP:	12:Wz3bZRGtTrKLQmv2tZSnm9K21e+wDFdKu:u3bZKKLlm9te9
MD5:	A42CD1DD04B05EB49A24C6AF5D9E4B79
SHA1:	E9F43DE8915420637BD8178832923B8399CBC176
SHA-256:	E0EFFC013A54624CFCE9CBE037C0D7D503AB8244DD0623C6D01875230FB92191
SHA-512:	4488D0F7DF221B8F660458B16D3737F80D20C1702F19F07916DABEF8F08692A0279F460FD616137E113582E003EF56C14D5D58E30AA4FD717D172AEF5CCE29BE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}...q....._keyhttps://cdn.shopify.com/s/trekkie.storefront.3bc22f7b201bea3154c99666f2373bcf9a3e8fb1.min.js .https://hereforyoushop.com/....F./.....{.....\. .LJ.....efl..6du.ee.VntP.2.A..Eo.....Fz1.....A..Eo.....F./.....88E6B4C3C82B1D92E2F7FB8CEBEA23149C3800AF8E5787F3FC24ACF1A628AC8D.\..LJ... ...efl..6du.ee.VntP.2.A..Eo.....DL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5c5bd7a64ba48473_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5956
Entropy (8bit):	6.302887762867581
Encrypted:	false
SSDEEP:	96:3kD1wULpklKdjcdAXM7jRBMqmGKRAyXok1n4mNI7QWK2bKTCAymyvc2JbG2lBcZx:3kBrpkMcSXu90GKGmn4iiQWKYg6cOlBm
MD5:	83EDB4F1091C8EBD0D5520861DBAAFB4
SHA1:	8EEBFB5914B26436AEC92DD668C927CDC5FC9F2F
SHA-256:	C97DE071BBD6B3CB000A9D2012E3BD64783A884DA7F06B46C3025EF7879A7B3F
SHA-512:	80758D1658D4C46A72AF26FFDDCD208F1D9E037BBD3F84660859E0E3248313C4C19CA8C93449A414F211262E5B4E167C9FAF0F15F9CAE63480F7FFFED479C05
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T...~.j....._keyhttps://cdn.shopify.com/s/javascripts/currencies.js .https://hereforyoushop.com/.9..F./.....{.....6...g.-.....6.`nzc..6K.'t.A..Eo..... .A..Eo.....'.....O...../k.....(S.D..`B.....L`.....L`.....Qc.....Currency....a.....Qc..W....rates.....a.....Qb.h.L....USD.`.....Qb.F.j... .EUR...Xa.x.@e..?..QbB..I....GBP...Xa5c.tv2.?..Qb..ec....CAD...Xa.Y.H.s.?..Qbb.>....ARS...Xa=.D}7..?..Qb.v.....AUD...Xa?....B.?..Qb.....BRL...Xa..>...?..Qb..z\....CLP. ..XaJ....U?..Qb.g.!....CNY...Xa.m.s.p.?..Qbr{6.....CYP...XaT..^-w.?..Qb..UU....CZK...Xa.'.ZS..?..Qb.0.....DKK...Xa5...#b.?..Qb.....EEK...Xa...E..?..Qb./f.....HKD...Xa.....?..Q b6{.....HUF...Xa...0..k?..Qb.....ISK...XaY...,"~?..Qb*.m%....INR...Xa...7.?..Qb..@f....JMD...Xaf2....{?..Qb.@U.....JPY...XaJ.....?..QbZY.g....LVL...Xa@..''2,.?..Qbz.m .....LTL...Xai..''.~.?..Qb.^.j....MTL...Xa.o`r...?..Qb.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d760ce477ab20fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4598
Entropy (8bit):	5.5640900317665585
Encrypted:	false
SSDEEP:	48:CcMsvsTsPOsRJsJsYxshT7sBsEshsVsQsCsw0sHXs1s6sz:CsEoXR22YOhTgeN+yZTw98S7
MD5:	EDB0FB149328AB5798001086043C1DCF
SHA1:	ACBC21CF0BF9D135CA0000E0631857B597EC9185
SHA-256:	DB588DCFA313C54FAC4109C25D153E229E6AEEF6482B73F115D6A5535D80CAF1
SHA-512:	5C9916093709D7E26DE63C2F62D8584B3169884F5EAB712611695AEC6A846CA975A0E38CA54CB3FC753255C7BABC8F6949C5F1AC32AA94F4BA1A0D39BC99C25 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n....J....._keyhttps://cdn.shopify.com/shopifycloud/boomerang/shopify-boomerang-1.0.0.min.js .https://hereforyoushop.com/_...F./.....|.....HH...t..z.3.1]H.c .s..I..B...A..Eo.....!.t.....A..Eo.....0\r..m.....n....J....._keyhttps://cdn.shopify.com/shopifycloud/boomerang/shopify-boomerang-1.0.0.min.js .https://herefory oushop.com/....F./.....B.....HH...t..z.3.1]H.c.s..I..B...A..Eo.....A..Eo.....0\r..m.....n....J....._keyhttps://cdn.shopify.com/shopifycloud/boomerang/ shopify-boomerang-1.0.0.min.js .https://hereforyoushop.com/....F./.....HH...t..z.3.1]H.c.s..I..B...A..Eo....._.Y.....A..Eo.....0\r..m.....n....J....._keyhttps://c dn.shopify.com/shopifycloud/boomerang/shopify-boomerang-1.0.0.min.js .https://hereforyoushop.com/.P'.F./.....e.....HH...t..z.3.1]H.c.s..I..B...A..Eo.....A. .Eo.....0\r..m.....n....J....._keyhttp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e86d2ec69a644ff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96432
Entropy (8bit):	5.826509260903223
Encrypted:	false
SSDEEP:	1536:90zAxtjcxuWSxiIaQvxougxMtPAtzhaw7WX9MkFnw5O42:YTu2CougUCzh7WXXFnw5O9
MD5:	9207BBE7BD540D5EFCA98AA6888511F1
SHA1:	F1689728D23B825687A86E246AE478744DE67590
SHA-256:	DF61A213BEB1C9806C3FCDA82A4947B36CB979B34DE7244539896F8A2921DC1C
SHA-512:	1EB02B84D62EF1E340EB089A2F9CACCC7B181442F2817EBFEA912FF6D0ECA9D2471F03A2E0D420C0EB6DFD252B10D005BEB9885A105DEDA99742865C7D983 D3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...1.....7C273629AFBEF71E8D4FF757D14DD9731EA3E9C0B30C4588489477B3E8947C37.....'..S....O!...Xw....;T.....H#..... .....,.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....Qb.'vY....t...`....I`....Da....j.....Q.@.Dp2....module....Qc..-.....exports. ..Qc.....document.(S.....5.a.....a.....a.....A....a.....a.....Pc.....exportsa..../...I.....@.-....hP.....[...https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2 /assets/jquery.js?v=8926416544707358891.a.....D`....D`....D`.....Y....`....&...&..!.&....&.(S...I#..`FF.....L`.....Rct.....2.....Qb&.....e.....Qb6J.....r.....S...Qb.~.....o.....M. ..Qb..2....s.....R....QbF.E....l.....Qb..50....c.....Qb.-v\....f.....Qb.l.{....p.....Qb...'....d.....Qb>.C5....h.....Qb.H.....y.....Qbb|.....v.....Qb.#.W....m.....Qb.6.`....x.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\617d53ca9fdcd6ce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	249
Entropy (8bit):	5.540719103394174
Encrypted:	false
SSDEEP:	6:mzVYGLKdXNQKwkE+mFV2KKqgLVtnevIam4s/bK6t:EohNQKwkE+mv2RqUus
MD5:	C271D7B493B0AE3C085D2A0BB10481A2
SHA1:	F41271DA9884A28CB8FBE1BE0157266EF6FF22B5
SHA-256:	984049D0E24D59534B162AB452CD7D663798E88B9A77159E581FF88EFBD8C531
SHA-512:	9C6B51EABEC1CFD90969991DC1FF82F7FE68489C45573D022E94B4E871FC0D4B033D36D16FCC16784E6F5A8A23169420804A04D642783265550524D7993E920F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u....'k...._keyhttps://www.gstatic.com/recaptcha/releases/UFwvoDBMjc8LiYc1DKXiAomK/recaptcha__en.js .https://hereforyoushop.com/.MI.F./.....D.....c. ..>Fq..Nh..A...um.Y]k....>]..`.A..Eo.....b.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6872ce7adcf25f4b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16024
Entropy (8bit):	5.6765813165197665
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6872ce7adcf25f4b_0	
SSDEEP:	192:4eQx0bJUFeppkyyA7IykPoA61eQhiBMsoE0MFHHgR2aSYBfykp4b/w7d6owALbLW:4eQuRpv04tgX0Eb66oNmnv
MD5:	611D6E75FF236D59B500CB54C08BCAA1
SHA1:	A4E5C4D47CA846F35687FFF6BFEADC94BC7A0D24
SHA-256:	7CFB8EEE71CEFBEB5B8B44A049BA7490CEF0A9A0ABA425F6AE164D60999AF3F8
SHA-512:	93E367E5474D5BE292B61E38F1D244ADA71FEF3ACBCAF515E53C2E2EA532A5243496869669F93256613FF521D18EA6C82B2FC708188680BCC54460432E7D93F8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....UuF....._keyhttps://cdn.shopify.com/shopifycloud/shopify/assets/storefront/load_feature-24ff1222c9aa13bb217653c0d3ea28c40a796a280e6da29ad421eec2a6075c86.js .https://hereforyoushop.com/r...F./.....{.....V._.U....L.f...D_...d...n..A..Eo.....Nh.....A..Eo.....'..$....O.....<...W.....P.....(S.L..`N.....L`.....(S....`.....\L`*.....RcX.....$.....Qb..2....s.....Qb..50....c.....Qb.....n.....R....Qb.H.....y.....Qbb|.....v.....Qb.-v\....f.....M...Qb.l.{....p.....Qb.#.W....m.....Qb>.C5....h.....S.....Qb...'....d.....QbF.E.....l.....O...Qb.....w.....QbB*....._...q.....l`....Da.....H...(S.L.`P.....L`.....a.....Q.@..-.....exports....a.....Qb^.....call.....K`....Dm0.....}...&.(...&.(...&.(...&.'..'..W....(.....,Rc.....Qb&.....e...`.....a.a4.....A.....c.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6ed4a4600e77f5dc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4712
Entropy (8bit):	5.479937135038167
Encrypted:	false
SSDEEP:	96:B3vHMb9u6zEu6mGxNB3Cn4qoicMjK9obbb3+DTaeWqGUbxx:RU5fFjihWLoBIqo/bOD+wxb3
MD5:	80093C4AA690EF0E2B2A97ED8A50E31A
SHA1:	89ACFB646BE53C95D3279966C7C7A2C5DF93CAD7
SHA-256:	C551F71C30C3B72F00138CE8319CF179E8D9E52C15D735928D8F659FBE9CA01D
SHA-512:	194933F1F9A59E9AFDB239EB2620F7AB8DB77C4D23ECDE86479DC63FA9EAC01AA5E8008400E1734494FF37FC631BFEE7716BDB1999CA8FAE82DF8929B66A3D2C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t...V>....._keyhttps://sellup.herokuapp.com/kartifyjs/kartify.js?shop=imhereforyouco.myshopify.com .https://hereforyoushop.com/b.(.F./.....{\.F.5ub.'v.#G.A\...p=.k.<..A..Eo.....A..Eo.....0\r..m.....t...V>....._keyhttps://sellup.herokuapp.com/kartifyjs/kartify.js?shop=imhereforyouco.myshopify.com .https://hereforyoushop.com/....F./.....{\.F.5ub.'v.#G.A\...p=.k.<..A..Eo.....A..Eo.....0\r..m.....t...V>....._keyhttps://sellup.herokuapp.com/kartifyjs/kartify.js?shop=imhereforyouco.myshopify.com .https://hereforyoushop.com/.q..F./.....'.....{\.F.5ub.'v.#G.A\...p=.k.<..A..Eo.....e.5.....A..Eo.....0\r..m.....t...V>....._keyhttps://sellup.herokuapp.com/kartifyjs/kartify.js?shop=imhereforyouco.myshopify.com .https://hereforyoushop.com/1u+.F./.....O.....{\.F.5ub.'v.#G.A\...p=.k.<..A..Eo.....-.l6.....A..Eo.....0\r..m..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\70747a5c451cd1e1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24453
Entropy (8bit):	5.918343775826798
Encrypted:	false
SSDEEP:	384:uAWiig1iWwpMic17BzR6PeKudjUQRDLk5VucAd8/0bCsL1xgG91Ja7TNLES3O:QiihmHNd0PeK+jfR68dP4LBe
MD5:	311BAD78F7ED667F1CF8B7977854D073
SHA1:	F86C5CBDEA43C9737798F9BABC6C270411A92447
SHA-256:	72C85D72B7E7097A97FB06A500E8F4DD22BCEF4F358EF8504502166915443D1A
SHA-512:	2FD050815490D171D700C51485ED84204651D82ED902340430822CEC4563678020C036FAAE62ABC49DA0305766EA9B9FFF4B7CCFD5FAB18C10EDF4F16D0CA12
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....'....._keyhttps://s.pinimg.com/ct/lib/main.d71a97dd.js .https://hereforyoushop.com/.b..F./.....x~.....8.h.Df..Q(/.w.E!#@<..H.+ .....A..Eo.....c.....A..Eo.....'.....O....]....B.....H.....(S.5..`....dL`.....(S...`.....LL`"....@Rc.....Qb6J.....r.....S...Qb&.....e...b$.....I`....Da.....(S...`.....L`.....Q.@..-.....exports..$..a.....C..QbF.E.....l...H..!...a.....Qb^.....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&...&.'..W.....-...(.....,Rc.....`....Da@...8.....a.....e..... P.....@....@.-....8P.....,..https://s.pinimg.com/ct/lib/main.d71a97dd.jsa.....D`....D`J...D`.....m....`2...&...&....&....&.(S.....Pb.....e.d.a.....I.....d.....&.(S.....Pb.....e.r.a.....I..a..d.....&.(S.....Pb.....e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\814f1d3aefbc13c7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3299
Entropy (8bit):	5.614322473231473
Encrypted:	false
SSDEEP:	96:XhTVow7gbd75gWCvD/mCqoidgiLhWihOwX:XhTWw7KJCjrYLHIm
MD5:	8D0670607AEDEDBF194DFAE560850B84
SHA1:	46CB3A4740E114AE15494276A253B54EE4FAD083
SHA-256:	B91D104B84FEEF787F13E4850F83F6FD215E1F241F1FA3E09DBA728C4107F9CC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\814f1d3aefbc13c7_0	
SHA-512:	4D90439AFF7C438E7718B6B011967CAD752A0B103033B44E4A993B4BE2246C8F46710FEF3FD75DCBCB8A27A4D22B9FA47B4ACDC540506802306886F0AA152A6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...._keyhttps://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/readmore.min.js?v=11994212879037969866 .https://hereforyoushop.com/....F./..... .....q;..+..:.....i:.hK...v.iN....A..Eo.....u+.....A..Eo.....F./.....'.....O....X....6Nr.....(S.8..`(.....L`.....(S.|.`.....(L`.....Q.@R.....de fine....Qb.K.....amd.....`.....M`.....Qc.....jquery....Q.@v..$....exports...Q.@..N.....module....Qc.b.....require.....Q.@vL.....jQuery....K`....Dy .....s.....&.(..... .&.z..%&.^.....4...s..$...&....&...&.]...&.]...&.-...%.....&.]........(Rc.....I`....Da..... ..f.....P.....@.....@.-....pP.....b...https://cdn.shopify.com/s/files/1/0481/0 922/4087/t/2/assets/readmore.min.js?v=11994212879037969866..a.....D`....D`2...D`.....x...`8...&...&....&.(S...`0....dL`.....xRc8.....Qb.....t.....S....M...Qb.....n.....Q b.$.....o.....Qb..r,....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86df87e775f96432_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	388
Entropy (8bit):	5.855617428584782
Encrypted:	false
SSDEEP:	6:mIgXYE4JyKKz57RWCjWpLUciRtmFV2KJ2ugcXRgVOIyAjPK6til17syKwWxsVOIp:fgzD+hUciRtmv2gXpCw7syKBk
MD5:	A6D68F186B86C4C1E1FFAE4E4E619839
SHA1:	E03DDE0A548042DB64E101BE4D0A5D2646E5EDD4
SHA-256:	0F998FF4A98B660DFC8FC15223DB0287A5079578EE237CE5AF28778726C379C3
SHA-512:	DA9CF9E114B2C99C0C84383481CC43720F7D0F083337CDEF910852C2196743CB24522BF016253E38B081C2FEDE2C15E53305808302056A7D376D647D75911AB2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|...._keyhttps://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/jquery.js?v=8926416544707358891 .https://hereforyoushop.com/....F./.....z..... q...Nn.....'Z.V8.g....{.A..Eo.....1S.....A..Eo.....F./..x..7C273629AFBEF71E8D4FF757D14DD9731EA3E9C0B30C4588489477B3E8947C37....q...Nn..... 'Z.V8.g....{.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\998808883a4f4580_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4356
Entropy (8bit):	5.756314460203362
Encrypted:	false
SSDEEP:	24:FPHgvSAL7v5XvqDJJ/Nv7hvZlHvvkvTvN55Tv3GmvRHnRvVhkvMVv4TtvfsvLCvh:Oa27VW/NVTPKVHRpxMMAZMmNNh7
MD5:	37CE223C64740E345F72F95E2E846B3C
SHA1:	F25320F93D79DB2DF1B37FCA424B5030A894AD0F
SHA-256:	963E85DA1363EBCD83BF7D55A9AD70AB4665C1435CA45D8174FDCBFC59F15716
SHA-512:	72D5629639F6C44085314003B9EBBCC2AF88F8C3A27C9FCCD029CAC367F723F65DA092E9D6328869F00C3773E3C42CC7B979047794ECA21EBA60901CB01D8EE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n....._keyhttps://connect.facebook.net/signals/config/713019789423044?v=2.9.29&r=stable .https://hereforyoushop.com/....F./.....n}.....]...`.^bm..~.... ..V:g^E....;..A..Eo.....}#*.....A..Eo.....0\r..m.....n....._keyhttps://connect.facebook.net/signals/config/713019789423044?v=2.9.29&r=stable .https://here foryoushop.com/|...F./.....]...`.^bm..~.....V:g^E....;..A..Eo.....ILs.....A..Eo.....0\r..m.....n....._keyhttps://connect.facebook.net/signals/confi g/713019789423044?v=2.9.29&r=stable .https://hereforyoushop.com/s...F./.....{.....]...`.^bm..~.....V:g^E....;..A..Eo.....D..P.....A..Eo.....0\r..m.....n..... ....._keyhttps://connect.facebook.net/signals/config/713019789423044?v=2.9.29&r=stable .https://hereforyoushop.com/..(.F./.....]...`.^bm..~.....V:g^E....;..A..Eo. .....E.....A..Eo.....0\r..m.....n....._keyhttp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b6e0bfd2dc8319e1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4769
Entropy (8bit):	5.628918864648467
Encrypted:	false
SSDEEP:	96:JgjgjcjLj8jfjzyyjMjAjrjymXjOj0NjdjwjTejXj+jYjM:JgjgjcjLj8jfjzbjMjAjrjvjOjWjdjwjm
MD5:	DF7142BE19E840AE010EF960EFB0A5E3
SHA1:	60B1CEEAE7FBFDECF1AB8702EDA18CC16EA051D6
SHA-256:	7E5D16807AA61438948977B395F68ED5233412C3A5574EB80453AF1DD0C48515
SHA-512:	4D7F6B5C390A8E793A1DBA75181BF712313B337EC03EEC462F30D8E3958D09F29B787910481D14C566E3342DAED6E3CB1AE9F2B945A749711C71B5CF5CBF222
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b6e0bfd2dc8319e1_0	
Preview:	0\r..m.....w...U..~...._keyhttps://cdn.shopify.com/shopifycloud/consent-tracking-api/v0.1/consent-tracking-api.js .https://hereforyoushop.com/.1..F./.....y|.....V.....Z &G.=g.c....O..}..L{.....A..Eo.....u.9w.....A..Eo.....0\r..m.....w...U..~...._keyhttps://cdn.shopify.com/shopifycloud/consent-tracking-api/v0.1/consent-tracking-api.js .https://hereforyoushop.com/.p..F./.....V.....Z&G.=g.c....O..}..L{.....A..Eo.....1.....A..Eo.....0\r..m.....w...U..~...._keyhttps://cdn.shopify.com/shopifycl oud/consent-tracking-api/v0.1/consent-tracking-api.js .https://hereforyoushop.com/....F./.....u.....V.....Z&G.=g.c....O..}..L{.....A..Eo.....A..Eo.....0 \r..m.....w...U..~...._keyhttps://cdn.shopify.com/shopifycloud/consent-tracking-api/v0.1/consent-tracking-api.js .https://hereforyoushop.com/F.$.F./.....V.....Z& G.=g.c....O..}..L{.....A..Eo.....d.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bba70edea388aead_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12964
Entropy (8bit):	5.866577754347543
Encrypted:	false
SSDEEP:	192:adm+wcaOFrlq3yiT2C3geU7Kkbqb4tHQpb3H4BDnZoR+z:ad7KNbG+AW2Hw7EZz
MD5:	437441C4ADCBE1425A41F3DBCB1FA173
SHA1:	54C585AEFA4EF38DAE7B47C6612951F6A0ADBF1D
SHA-256:	9B3BD4DF6E43CB79247F3EF2E85CE251EF18EBF29FE025D5959513B248D22FEE
SHA-512:	2A5C110B4D101E5916E4C79A05451D76939C3362CCCD8EADA1A1BE60AE562674F1924BED538F0E6961C2D20ED04413AD7D9F5E2E3C57D6E2F6521175C2F829E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....#...._keyhttps://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/jquery.currencies.min.js?v=17505776077200662322 .https://hereforyoushop.com/t;..F. /.....{.....|.E....,q.t.p ."...ohS....{.....A..Eo.....>..%.....A..Eo.....'.Y8....O.....0..v.....(S....`b....xL`8.....L`.....Qc.....Currency.. Q.@r.{.....jQuery...(S.....5.a.....Q...Pc.....cookie.a.....IE.@.-....xP.....k...https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/jquery.currencies.min.js? v=17505776077200662322.a.....D`....D`6...D`.....0...`....&...&....&.(S.....a.....a.....Pd.....cookie.writea ...R.....Qc...Q....write...E..!.d.....&.(S.....5.a..... ....Pd.....cookie.reada`.....Qb.}.....readE.d.....&.(S.....a.....a.....a.....Qc..Z.....cookie....Pc.....destroya.....Qc..$.....destroy.E.d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c158b458b7cee6a4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	132
Entropy (8bit):	5.404851388866697
Encrypted:	false
SSDEEP:	3:2AZcgWkSQkJUW1UFmlciS8hvmfYykRMWdJ9kP5mvxvtl/:2A3ZSUiUqTvmfYyfC9k4vxv
MD5:	929CBF30AC84554CFD256BFCACE4914C
SHA1:	CB38465D98936FBA30D43FEDA13754B1990BDEB9
SHA-256:	6C8DF3ED18CA2613E2CA41287730EBBA37B4660D1D704D890BB25887923073F1
SHA-512:	88522F51D694B77183FB34254D732732993258DEF7132EB4202E0FB02DA9FC46351FD64EF7A64CB3D214CADEDBAA931E1F07A52113ED58245C6FE86B1D3BF6F
Malicious:	false
Reputation:	low
Preview:	....F./.....A55DE3A76990158FFF0538F4B01793A3CCC798E760ECA2DFEF96B2DF52D8A7E6.....W{.[..B.Ae.5#..'.h...{....I.A..Eo.....T.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c51a1ddf68b31515_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	135280
Entropy (8bit):	5.8043901385933
Encrypted:	false
SSDEEP:	1536:96raE/39ovw8+gfESugcv4BN2/fn/ATicjW2S6/QNCtYAF/zEnGMXYyf7+4j96Wf:u/2+eVJxOc7OCe8eBGWbeITsgQm
MD5:	66D5778B2AEA48C42B0DB18608966DB8
SHA1:	73F0D849A8902B71149B8274974D975FD2E9DBC8
SHA-256:	2812DA9FBB14BD295985C353E5058B387FE84B63575740B06F31A8A4BFEB1FB4
SHA-512:	A004014DB4D7C8908D433B403DF3DA151AE209C44FFBC111AD29CCD6FEE068D654C299B698315C878F6B971ABE483C66CDC6774F89A888449277FAE94772E20
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....{.....A55DE3A76990158FFF0538F4B01793A3CCC798E760ECA2DFEF96B2DF52D8A7E6.....'.j[....O-.....".....!..... .....L.....(S....`l....PL`$....(S...`.....(L`.....HRc .....Qb.....n.....Qb.'vY....t.....Qb&.....e..... .S.c$.....$.....I`....Da....N.....Qc..{....window....Qd.}k.....matchMedia....Q.@.Dp2....module....Q.@..-.....exports...Q.@&e.<....define....Qb.0.....amd..(S.....Ia.....I..1..@.-....h P.....\...https://cdn.shopify.com/s/files/1/0481/0922/4087/t/2/assets/vendor.js?v=10210318190529598248a.....D`....D`....D`.....`@...&...&..A.&....&.(S...`.....L`F.. ..XRc(.....Q....S...Qb.~.....o.....Qb6J.....r...e$.....I`....Da~.....(S.....Ia.....Q.....d.....@.....(S...Ia%...e.....d.....@.....(S...Iao

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cbbf2764fba56c85_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cbbf2764fba56c85_0	
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.596003861218371
Encrypted:	false
SSDEEP:	6:mhAwVYGLKdXNQKwkERurgMltYij29kYgtbK6t:WRohNQKwkE8rblti4r
MD5:	A0870337B6AB3D27E83E5934DCAD9D9A
SHA1:	F5531B30A68A215EBD8FE9DC7E11EE82D4F67A50
SHA-256:	34D4B3087FAEB116C1C700EAE1536782C2C7AE1E7755D6811D3125E34F714516
SHA-512:	19653EA13EB611F266E2AA178DD63EF357AA173851F8DEACA4281098B1CD28875952FB6A45F6D34BD4F86EFCE42F40C88806EBBA5105DEB2EB62FFF1A69990D D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m...;.W....._keyhttps://www.gstatic.com/recaptcha/releases/UFwvoDBMjc8LiYc1DKXiAomK/recaptcha__en.js .https://google.com/.MI.F./.....L..... tG..i....=...M.. .L.3...A..Eo.....Y.C.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e1b5eda50cde505d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.577058732766319
Encrypted:	false
SSDEEP:	6:morYGLIkVAhpNHt4gwguTAgc5O9nBhK6t:fct9fwxTAbM9B
MD5:	930275E957C9D52431E99946CF5F0656
SHA1:	30F21F4C5438471FAB42A4B6AD0B441940D74487
SHA-256:	000600AA90B1B550FAA4E5AEB503B3E53CB6C9B8139E498A37E85C2E0D541BEF
SHA-512:	6E9633FABC70B398F430622BE664E5B55704CA304310DEC45572FA573E139E00B20A87BF61D9F4A50908E66520D975EF72C3211CD91B7EE847C365B17D4DFD3C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....E....._keyhttps://www.google.com/js/bg/O67mjpEsjT-AT91MDd0pGc2bzg3wulEAhSoq1-VXop8.js .https://google.com/..O.F./.....U.P.%F.V .0D..N=l.ElN....kt....A..Eo.....Q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e7bec4ed4587ef3d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.495426455830719
Encrypted:	false
SSDEEP:	6:mUZlgEYE4OZo01gPzJ8mFV2KDgeUHogJJH4GMhK6t:pbNToB2mv2mcIWBM7
MD5:	7D04843ED5552C242B3F8FCDD1449960
SHA1:	D53F03B15D06AE87B5A505C594CA48B26D2D0B31
SHA-256:	C960AA81A90E2314A3F4CEB8127695422BB6EE7F7D0B8B46A630E29AD352BE61
SHA-512:	3C37D5C0C844B52B8BFDA409FA105C90983FB22F3FD32E6249F516C61B911E5436932026D7B7262C944BC331B086457FEA10EAD282A2B9ADCD6EBA02C5830AE B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k.....1....._keyhttps://cdn.shopify.com/shopifycloud/storefront-recaptcha-v3/v0.1/index.js .https://hereforyoushop.com/F.C.F./.....y.7...QF9..b..x.&....> .U*Y..o8...A..Eo.....6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\efbb20c56b919bd6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5621
Entropy (8bit):	5.4845753068252145
Encrypted:	false
SSDEEP:	96:Lu5VVmFwUu5V0srbRpNQNGoDebEAg+affrlr+k:Lu5au5CsrjoDCEA4sk
MD5:	3CC9CD8557E13FB9D4841A7619CF4D1F
SHA1:	DBB17FF703570D9A4C632B88518E168E70E83306
SHA-256:	0DF7F3FE7A7AF2DA1060B8F89F35F5488A060A81B605D5FFCDCEDB7A7CF071D9
SHA-512:	6F93511B40129CE33407103847EE82432F3C914D6CADB0C082CC6F0D2B58683FC71D84A92C7745DE07E1D604B7BB1DDFF0982CFD26CDF66E5D5F5F6673E3FE
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\efbb20c56b919bd6_0	
Reputation:	low
Preview:	0\r..m.....9.0...._keyhttps://cdn.shopify.com/shopifycloud/shopify/assets/shop_events_listener-68ba3f1321f00bf07cb78a03841621079812265e950cdccade3463749ea2705e.js .https://hereforyoushop.com/....F./.....|.....{}.e^.rH.vr.}..K&R.....on....A..Eo.....Q.....A..Eo.....'.....O.... .....y.....(S.L..`N.....L`.....(S.P.`\.... L`.....@Rc.....Qb..2....s.....Qb>.C5....h.....Qb.-v\....f...b.....I`....Da.....9...(S.L.`P.....L`.....a.....Q.@..-.....exports....a.....Qb^.....call...K`....Dm0.....}...&.(...&.(...&.(...&.'..'..W....(.....,Rc.....Qb&.....e...`.....A.a4.....c.....@.-.....P.Q.....https://cdn.shopify.com/shopifycloud/shopify/assets/shop_events_listener-68ba3f1321f00bf07cb78a03841621079812265e950cdccade3463749ea2705e.jsa.....D`....D`>...D`.....`V...&...&..!.&..A.&.(S.4..` .....L`.....4Rc.....Qb

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):	147456
Entropy (8bit):	3.5295788367523913
Encrypted:	false
SSDEEP:	768:BMcOyBGNLjrcE9xTPhVrAlFLPOnAAHJUHzL0HJUHzdtp:BzOHLHhjaFLPOf1q
MD5:	2446DECE96F381933858E833D7FC08A5
SHA1:	D0C6BB03F603AE00BBAD744A4F3121F39F530043
SHA-256:	DB8EB54AD3DE33718699618B8B4CE74979732D2F0F85FC2475A6CC7729A99767
SHA-512:	1BE844492D21BA782064634B965E8815806892421EDE0A2BC897CEFF57056B99E92A41679B5EC7F9AD18B82335AA57C0C204D90ED4EA16A02207E242E80D5329
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):	139624
Entropy (8bit):	3.2595086402465308
Encrypted:	false
SSDEEP:	768:c6c+y7dlNLVyQj/xTjyHAlFLPOfdz7HJUHzS:cN+svLVBhFLPOfx9
MD5:	FD82DB81CA83C06062A20FA381445243
SHA1:	0A5025D7262F72009F44DCE6B715E756D56F3881
SHA-256:	6D36900C9470489EC1A96BFD7E65706C615767CE9BB1928054DC0E30A34F2FB0
SHA-512:	480AE69365ED5A7A36A41E8185C3E82CA920D6C6A6D8CF0F516368B0B6382A65118F93EDF7498E27FC1E142BE4F356D9989ACA5407EC20E8F59DBE5520573EC
Malicious:	false
Reputation:	low
Preview:	.....i4S.....

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):	125003
Entropy (8bit):	4.2686443503238936
Encrypted:	false
SSDEEP:	3072:PcKXNY85FzMPeISUNlQNkKK1L2Gsl4q5zURnn:JXP5iPwNO1i5Ynn
MD5:	384F14E8309E8FEFBF60141D0E65E347
SHA1:	E109C8916EB3EB59165DE83FFE94115D3CFDB742
SHA-256:	CBBD2738B07D3C4994D5127DDAA61CA1924E8E30DE40E5BB908EC838F9898B3B
SHA-512:	BBED3E2D1C744EEE07CA08C209B662A234587898484E33B0E7E590E3DD8C4453550B5C99C6E9D1A3E73B33DD5C245F7B4EC86285ECF1EEC503D44B8FD868379
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...f8125b1a_8a6b_4e88_80ec_53f96a2069e6.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....q..l.....https://hereforyoushop.com/.....H.e.r.e. .F.o.r. .Y.o.u. .C.o.....h.....`.....N.....O.....(.....>.....h.t.t.p.s.:.//.h.e.r.e.f.o.r.y.o.u.s.h.o.p...c.o.m./.....(.....0.....H.....p.....0.....H.....`.....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. .....=.&.....d.....

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
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
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):	317
Entropy (8bit):	5.232230243141146
Encrypted:	false
SSDEEP:	6:ivB8+q2PWXp+N23iKKdK8aPrqIFUtwRtQZmwyR5VkwOWXp+N23iKKdK8amLJ:ivrva5KkL3FUtwRtQ/yRH5f5KkQJ
MD5:	71EA05DD0CDBB9CC4FF66B085CD22693
SHA1:	CF1F022BC4820E68D8B8A79FDD6AE7C81FCE358F
SHA-256:	D1EA9A75A08EC3E37DB190D89463B07CD7A3D8E7C83D9C8BADD0D9605A414C23
SHA-512:	EDBF17FDA153C501023390EA947E8408F8FE44803BA6D526B2F287A27B7E0EEA064A8DDE9A3C2D07323ECA009E259A0184E8C84CE9F1374FBF6076DF32BD793
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:35.994 c68 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2020/11/22-03:41:36.001 c68 Recovering log #3.2020/11/22-03:41:36.002 c68 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:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
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):	5.164849959533361
Encrypted:	false
SSDEEP:	6:isQ+q2PWXp+N23iKKdK8NIFUtwRmgZmwyRmQVkwOWXp+N23iKKdK8+eLJ:isVva5KkpFUtwRmg/yRmI5f5KkqJ
MD5:	49FD1B28D2BFF0EDDEF09D296EF93D3F
SHA1:	2805FBFC8B577B44BC9A5BE2159351D3F75D77D7
SHA-256:	FAC029905B8CBB5893A61299D1CA20338F20FA27277A3997285C386DD580712C
SHA-512:	64F761B3F6507A043E9A260284C36E8F100417CEDB9D77B1EE85AAEA9562B315B3F43AB523BBD3C4843F0E5671E9DEB5AC2C722A7AAEE4A372567A53A35BFD4 D
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:38.050 1238 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2020/11/22-03:41:38.052 1238 Recovering log #3.2020/11/22-03:41:38.052 1238 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:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49I C
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2I/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/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:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"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=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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):	369
Entropy (8bit):	5.2837730752371925
Encrypted:	false
SSDEEP:	6:iVFBBd3+q2PWXp+N23iKKdK25+Xqx8chI+IFUtwRU7ZmwyRfFBBd3VkwOWXp+N2k:iZyva5KkTXfchI3FUtwRc/yRfFBBT5fk
MD5:	E0C86CE06CB1F15E02F630152C3F0E8B
SHA1:	3781BD61860D6813BA10A439E117A9F2F314284A
SHA-256:	9383B93CC0C2DF7469B274857A08BC95E437B8318A5C9A03AC4155001AC2AD04
SHA-512:	8823E52C3F448D838FADE7B5EFFB9E9BB236D04795C120680A9D676BDB26C604F2305DC3343DDE87D9AEAE58D70B7722CBE8782AD91FA632C6E736E199B90F6
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:48.992 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2020/11/22-03:41:48.997 dd8 Recovering log #3.2020/11/22-03:41:48.998 dd8 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):	355
Entropy (8bit):	5.267641147436525
Encrypted:	false
SSDEEP:	6:id7r3+q2PWXp+N23iKKdK25+XuoIFUtwRcXZmwyRc3VkwOWXp+N23iKKdK25+Xu6:iNOva5KkTXYFUtwRcX/yRcF5f5KkTXHJ
MD5:	790525AF10D2CC62CF02F02A480980B4
SHA1:	718253E474772460DD54B86F0D43BE2120CE6A58
SHA-256:	176735AA8A623AC5716E5CAEFF0555A9BD8F9842B01A2B041A49D386039F581A
SHA-512:	E0D7E4682C5EFF779BABC0F070D7FF33AD9CAD7048025867384CE2FAD12613A9573C0CA49453076C4F58DCAD96E41C31AA36CE67FFC380D099210E68E752319
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:48.974 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2020/11/22-03:41:48.975 dd8 Recovering log #3.2020/11/22-03:41:48.975 dd8 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\File System\Origins\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\000001.dbtmp	
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	102
Entropy (8bit):	4.707425199545215
Encrypted:	false
SSDEEP:	3:w1tsm1iILeNlA1jPqciKPnSc+VVn:w1tsmRLVP1/Sc+VV
MD5:	7E6074135B54581D9C9A50EC25141C6A
SHA1:	362BE82BA04A240771813665F436B0EF9D24C35F
SHA-256:	8A14329F2C4F6E9CD07FDABA314C1F29FDE90C936695F0E95118778B2E0CD7A2
SHA-512:	D715BD9AE5A94DC6F30D6B8A475DFD69DE15C3915987D6A2D9E6F761237055AB1409B24431F9F6497FE0CDF664449F13F3D52FB0C49E4221CE3145862D9048F8
Malicious:	false
Reputation:	low
Preview:	mP.....LAST_PATH.-1.X7.>.....LAST_PATH.000..ORIGIN:https_www.google.com_0.000

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	142
Entropy (8bit):	5.260535064174571
Encrypted:	false
SSDEEP:	3:tVPnfxf/LX3TEAQWMLKqFkPWXp5cViE2J5iKKKc64E/+MOMcWIDMGk4cWIV//Uv:5TpM+q2PWXp+N23iKKdK29MRgPRIFUv
MD5:	E89A58A2582EC662F10764ED188D481E
SHA1:	85EBAEE6D79565980E1D77CF13102445C28783B6
SHA-256:	4F410FCB5D825163316B4AD224BA4FF52A7BC84A5D30D41BEDC547F65704A517
SHA-512:	75FD015F196407E29EB21B268D0D1E66248324D38C0A8F31AF4A233D1D1D7DA212A876AA3DC783E7894BC6E108B56BEE2C2148D8AD84DA1E108957F09F4E61DA
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:42:00.259 f6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins/MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAIxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C235B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\MANIFEST-000001	
Preview:	.|..".....leveldb.BytewiseComparator.....

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):	327
Entropy (8bit):	5.235404186572822
Encrypted:	false
SSDEEP:	6:i/Ft+q2PWXp+N23iKKdKWT5g1IdqIFUtwRiZZmwyR93VkwOWXp+N23iKKdKWT5gZ:i/Fova5Kkg5gSRFUtwR2/yRj5f5Kkg5i
MD5:	711159D6DBA261B2073E27A89B2243C2
SHA1:	5A73E861ADC8BF1F2BF38012BBD0EB8BF1754436
SHA-256:	0B33A1F7EE588EF746AC40436F7524E21B374FFC0CD9244B0136C97D70CD78CD
SHA-512:	FCCCAC59690DE9C007D58F6CD4581C8A01E89C6D2309BEF2908394B233C84B1C2781CEAF0B9C98857B5BF2820C848E519231F825B59E4D720B100380B94D3E6
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:48.910 dd8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2020/11/22-03:41:48.911 dd8 Recovering log #3.2020/11/22-03:41:48.912 dd8 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):	0.8267259015190671
Encrypted:	false
SSDEEP:	192:B2lo2/xOGyo2kxjxOGvjo2qkxjxOGCJo20ZNxHpkxjxOGwPJo2n9X:2xOGHxjxOGvCkxjxOGzxJkxjxOGYX
MD5:	701CDCF8CDB890652527D34B69E970D8
SHA1:	90440E80E34937F41A8759201A441129584E665A
SHA-256:	41EB078C62A3E9C550B660F2D19143F639932758DFF3F687453C5ED4E9B72BE2
SHA-512:	71C88E446E511E3038A9AF238CA78F764D6355AD2F4E4C6208909A7BB65AF13FCF1DD3E0D163CBB054294C93360D18CFF0741CACCDCB3ECC2D20103F472C657
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):	577
Entropy (8bit):	5.243719721852462
Encrypted:	false
SSDEEP:	12:ARv5JBXQXs2mvRsSYggijnlFOVPgu23tVu/zVaZ0Gwyeav2l1FBtJ8mTmv2l1ytn:A8Xs2jvijnPop2dHPRKM
MD5:	1E84071BEE19B1B0ECCE488B6348BDE0
SHA1:	D4B006A8A389403B30587BDA3B51898B18FB3EAD
SHA-256:	D39838293F2186AE9BA622A911AC8D1A099436387C187AF4F212997CB662E2A9
SHA-512:	E8071B9AC69249995680105D230A6F2593650E9E6E52B7570EE3C827C13BC7B077D1616EB520A753082BDAA3E41A29A0316F8D00748F4F35420ED078979F9689
Malicious:	false
Reputation:	low
Preview:	....."8....co..com..for..here..hereforyoushop..http..you..https*X.....co.....com.....for.....here.....hereforyoushop.....http.....https.....you..2.....c.....e.....f.....h.....m.....o.....p.....r.....s.....t.....u.....y....:P.....B.....M..... .....*.http://hereforyoushop.com/2.Here For You Co:.....S..... .....*.https://hereforyoushop.com/2.Here For You Co:.....J .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	187824
Entropy (8bit):	0.6136450679764024

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Encrypted:	false
SSDEEP:	192:OE2no2sxOGVo2lxjxOGYIjo2/PWkxjxOGbYJo2m:OoxOGrxjxOGYIekxjxOGB
MD5:	E46E802684C3017A34776E5B3683E61C
SHA1:	7E9BA63E993CE08BF8C82DBE99579E508A48336C
SHA-256:	82561133CE64D6BCC6ED613908CB4A64E8FAAA3AABC1F03A0117D6480B17BA12
SHA-512:	30CA81D91900ADD595E9EA4EC6C2E9437251DDC8AB3FBA4F12D13FAC9346CBC71860E8EFCD05492B198FF5FCB1652BDD6C06667D1AAF9AA3F474944D48B794A
Malicious:	false
Reputation:	low
Preview:	.....~.f..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3256
Entropy (8bit):	5.576274478244544
Encrypted:	false
SSDEEP:	48:ZKUCjGqja7aMU8dbL+OBbQSefgGMNrS0U9RdiN9tx:fwa7aMndbL+OBbQ5fgGMrS0p
MD5:	A0FACDA7E60DFCFC8A1740E96480DB80
SHA1:	545AB588E5DC6CD5364FA111E466784A64F716BD
SHA-256:	E6AB2B6CE06875D8B4250695A8FDB7C03EEA5D5769ED039FA2960CD749624354
SHA-512:	4E2FC02BEC92C590F69D7480B9880DB79F8EF4F40FE62CD1B8F86C65AEF9E9CDE24D2CA6E93576BAFF2D5BA3663A4867407C977D66DD7171A1A7DCC2E72954B2
Malicious:	false
Reputation:	low
Preview:	....W..*.....META:https://hereforyoushop.com.(_https://hereforyoushop.com.._boomr_clss.Ap.k..,.....META:https://www.google.com....._https://www.google.com..rc::a..b3IwcjJjMTB5ZnI2cQ==...C.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..56675000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2020-11-22 03:41:51.98][INFO][mr.Init] MR instance ID: f3b1153a-b2f0-4412-9925-57fc30a18b21\n","[2020-11-22 03:41:51.98][INFO][mr.Init] Native Cast MRP is disabled.\n","[2020-11-22 03:41:51.98][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2020-11-22 03:41:51.98][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2020-11-22 03:41:

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.240776875459552
Encrypted:	false
SSDEEP:	6:ivlb0Vq2PWXp+N23iKKdK8a2jMGIFUtwRvlhQgZmwyRvdIkwOWXp+N23iKKdK8as:ivyVva5Kk8EFUtwRvTQg/yRvdI5f5Kkw
MD5:	9746831CED951018596915D1B1B61DF5
SHA1:	16FCBDB6526833057C791C91949FE50E4C55E701
SHA-256:	FBE765E5B784ACB06F75757AEEF70DF1B66ED996F2997022938CBFCC27C8FC97
SHA-512:	8652F72FF2D922E0422B3F43344A623B3940AD268405831F99D0489865F82ABC17C8D28D36D8C14E03E65076DD8097EF85F1B44B33CD20443205CDB8C7630785
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:35.777 1664 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2020/11/22-03:41:35.779 1664 Recovering log #3.2020/11/22-03:41:35.781 1664 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
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):	49152
Entropy (8bit):	1.1751324122743059
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOsOqAuhjspnWONuOqAuhjspnWOxOqAuhjspnWOgL:HPOYgzL
MD5:	7542C514842EEA45AB3480FEC29F0B42
SHA1:	482877491685C09851DDBFD5E74F9E968BAF1D49
SHA-256:	367370988B107CE2A06E5E8C8DCCE2BB69671277AA81F12D3BAF648FDF2933F4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
SHA-512:	B651287B7BB03F88A1504380D95201516F8191ECB55BDAE91ED0C06F44440D023DDC3E1237146228A14770ED73064F6725DC1493FF137AE2949FC2CBE0A66F14
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	51344
Entropy (8bit):	1.0906425112074614
Encrypted:	false
SSDEEP:	96:n8UOqAuhjspnWODkOqAuhjspnWOUX0OqAuhjspnWOdoEOqAuhjspnWOq:8yGiVSKoCt
MD5:	88935295F6321FC7623B8DA779D1F503
SHA1:	1F3654E5615A5D3F928CAD6001614E5D1BCC96C5
SHA-256:	93A182C59E245C3BA4F95BDF123E91D5816D8DDB31D6AC26DB4ED059DD4C3CC4
SHA-512:	19A2EFB2B75C6CE3D2DBE3A06C39349C3705CE2A57AFE85108935C7582E291C03AE8BE51A3F70ECBECEA52C9AC4F33B29B7C01DE7D2F044590B2644C0F9167A4
Malicious:	false
Reputation:	low
Preview:	.....>G..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.200579131445832
Encrypted:	false
SSDEEP:	6:iZutQ+q2PWXp+N23iKKdKgXz4rRIFUtwRZcSgZmwyRZcSQVkwOWXp+N23iKKdKgi:iAVva5KkgXiuFUtwReSg/yReSI5f5Kkt
MD5:	0ABE203859AE3FC5118B3FEBDEC4C069
SHA1:	18201F42949A293F7C2E9B47F27D6A7DF2BAE077
SHA-256:	0F895F5C86E6BD5CA11ACFA91ED6C708BB44B39C0C0F7CD258920EBD14967F50
SHA-512:	D198FB89E4B06C57FD1A9F3E65C156B3C2C18ABCF837A48B4D4F92AAAAEBD5DAE0C462AE5648D452C2F12A0FA2C602D5EC19F35CAD871C4CB6FC22F9D1BDD2CA
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:36.038 1238 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2020/11/22-03:41:36.039 1238 Recovering log #3.2020/11/22-03:41:36.039 1238 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager	
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):	77824
Entropy (8bit):	0.4792174628264173
Encrypted:	false
SSDEEP:	96:vCIG+6bDdsDaBJvtHIm50I4sX/CIG+6bDdsDaBJvtHIm50I4Gr1:a96EJTv4sXK96EJTv4Gr1
MD5:	9D63FF7573A761D5046866D345BE2455
SHA1:	79E3301EB54FE1785DB9DDA494B72CC931D3DECB
SHA-256:	8D6BC62D878AD79AA870D6167E9C8A8FC49AE8E6FAB8CA5DB5246E521AEB088A
SHA-512:	DD769EDE8585CA7CE8CA8C94FD675ED7029A2BF03027E7AC6A09149C1833CE1AC4EA4B31CE87D1F99331571DEAB309CAC903AF43F3CBC8F72C79B57CEF784E9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager	
Preview:	SQLite format 3.....@ .....C.....g.....*.W.L.[.....".....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	0.6535675147301822
Encrypted:	false
SSDEEP:	48:UMLgqzLbCIG+6bDdsDaKgJgKtHIm50I9a+Uj5:UagsCIG+6bDdsDaBJvtHIm50I4H
MD5:	64DF8045DA7194EE7E918515C9711480
SHA1:	E7F926F4EFF8C5B29CB39CE3981C2D16D3A3E95B
SHA-256:	5AF8D2F841A8474A3AA7BA83106C13AA8C3C342949CC533F2BF059A0CE574DB6
SHA-512:	DB34E0E9C9E2109E0DE074FDFE0CF443D0E3062CF6A0CCC8B8C15934454CC39005C9C4D58866C0C767C7C51ADBF5209EACD3DF4360D134AF79C59BDEE4CFEC
Malicious:	false
Reputation:	low
Preview:	.....<.}..... .c.....f...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
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):	45056
Entropy (8bit):	0.9203143995287396
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU2V9nvDEIopK2K:wIElwQF8mpcSOQIElwQF8mpcS0
MD5:	DA4469DB9F956143D8FA98B7E16DC9EB
SHA1:	08F8DF55821004BCB445FA14B18889EB7F213A57
SHA-256:	229D36C08E2A2CCFCD251F8C59133B06E87639CFCCF650208D2CAF2084F6703C
SHA-512:	542DD2CED0FD6CFA2EC83A62FA8786C37728C63C66CF2B56273065424EFA8612D21BADE548EBD91FA061C5F0A67665C56B4E9FF5108285CF42147E99FD2F31CE
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	46192
Entropy (8bit):	0.8140217830768338
Encrypted:	false
SSDEEP:	48:PUqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUdbqqUIopK2A:PUhIElwQF8mpcSsxIElwQF8mpcSW
MD5:	9654F824304CCCE358D2490F14A71A6C
SHA1:	90C7D496D7435C4066147B53DE8D669B9963C1DC
SHA-256:	63D3F216D1D235C2534D1250B9E69EF9D3A4948BB361DE0CDBC2E9783FA911FD
SHA-512:	CDA13C15595A4513F28D2DDCCBBE2C123DECA6571925263803BB6DBAF2BD00F850F5BD41AA2E646C03AD43495A75016E912AD3A08F44EF137AC0711F72950EC
Malicious:	false
Reputation:	low
Preview:	.....T.S%.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2495
Entropy (8bit):	5.357350007788234
Encrypted:	false
SSDEEP:	24:7Hz3nwNvs2XB7Xk8k8NfyAoQ93lF3mA7ol3mA7Kk3OAiuIFE641ut6djXGA5ZF6J:7H6lVUKLzIgtSjXGkRcxGEns6tJd5
MD5:	33B73C04D46C35A525804D673BE79B7E
SHA1:	AD4AC64052EC206169CD82CFBAF3ED879572F343
SHA-256:	B9772513832A6C36836BCC58077FAB2196319678F9BBEBC3B1A06211A446F789
SHA-512:	31E5A3E85EF80BCDBE59E14B1A6C9066518B77FA32E5D69E7A62EA0472D01422AF455F840740763AF58BFFEE722C9765BEEC325D1E2CE667766FD473A1EB1356
Malicious:	false
Reputation:	low
Preview:	..&f.....x...i.....next-map-id.1.Jnamespace-f8125b1a_8a6b_4e88_80ec_53f96a2069e6-https://hereforyoushop.com/.0...i.....next-map-id.2.Jnamespace-63b8e221_bc9c_43bb_8b94_b9efac8eb54f-https://hereforyoushop.com/.1. ....i.....next-map-id.3.Jnamespace-a72820b0_a6f7_4d5b_b954_f69c1f871e45-https://hereforyoushop.com/.2.Sp.i.....next-map-id.4.Jnamespace-75f70319_736f_4978_99dd_66f8e9f481ba-https://hereforyoushop.com/.3..Hni.....next-map-id.5.Jnamespace-299cac94_3da7_4a6b_81c9_65849469e9f6-https://hereforyoushop.com/.4.~l.e.....next-map-id.6.Fnamespace-299cac94_3da7_4a6b_81c9_65849469e9f6-https://www.google.com/.5...i.....next-map-id.7.Jnamespace-33159d52_5c02_45ab_b2c6_99d486e56fff-https://hereforyoushop.com/.65.....map-5-rc::cnB.H.K.B.S.T.l.G.t.t.x.l.a.-.d.z.3.C.o.p.I.Z.E.l.Y.9.W.p.i.M.2.P.C.V.a.V.K.p.w.O.Z.Z.0.J.C.q.4.5.N.Q.e.7.x.5.g._

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.2319041172347625
Encrypted:	false
SSDEEP:	6:iv5+q2PWXp+N23iKKdKrQMxIFUtwRvHGT5ZmwyRvNc3VkwOWXp+N23iKKdKrQMFd:iv0va5KkCFUtwRvk5/yRvC5f5KktJ
MD5:	DAC9BBB37123B89B8E8C71C8FBDA65D5
SHA1:	A1A4C91AD06EE8CFD29406127D1ECB6A1C456D31
SHA-256:	72C81D8EFBBC3693EB5565059CB4D2732B4569F8C9853CBA9A36920809C0E83F
SHA-512:	20271195C6DF5694A9AC85964336333539EECBBC75F1E5E25C26B92EC63DCCED8C7E682BFBE29434400C64839E1BE8E377099A1826326F3219C98939E96A6175
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:35.948 c68 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2020/11/22-03:41:35.949 c68 Recovering log #3.2020/11/22-03:41:35.950 c68 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.196831831762903
Encrypted:	false
SSDEEP:	6:ivh80Vq2PWXp+N23iKKdK7Uh2ghZIFUtwRvhlT0gZmwyRvhlT0IkwOWXp+N23iKm:ivVVva5KklhHh2FUtwRvTQg/yRvTQI5A
MD5:	E7CA0D8E5F6F055365B69799E533B7C8
SHA1:	53D0F817B1AAFFFFC7AA3BD65C569E640B25E9A1
SHA-256:	ADC3AB92A1F8CAABC6CE3DEA916D58B60EC13D3CEDD70BE7A8E960B6C2F2F464
SHA-512:	D9060C9F3260274DF95E8A0C107F0B1D26C097530570BC5808A299229F25F1B52B2A6A9C2F3ECBE160BAF94ABA51F2934C986AD81BEE418CB3BCBB25B9177B76
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:35.734 1664 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2020/11/22-03:41:35.735 1664 Recovering log #3.2020/11/22-03:41:35.735 1664 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.300807002705313
Encrypted:	false
SSDEEP:	6:ivP5+q2PWXp+N23iKKdKusNpV/2jMGIFUtwRvz9ZmwyRvlNVkwOWXp+N23iKKdKK:ivP0va5KkFFUtwRvz9/yRvl5f5KkOJ
MD5:	14C082F8439B2E0158CA322BF62024F5
SHA1:	1E4B9C44DC6B33CE4016381DB9FAF2BD797A2513
SHA-256:	08302D80C0E7C1F1195ABA4B3264DCAF7287BB11503C7F3CB3B8CDDB0609BD1E
SHA-512:	6F6C1BB05F91928873E20174E9421AE0286F69904FB2D4D146B9231BB95CE8CEF70220FA98EDA55BB9B11C9DBB42F7F2D2DD8E2C71A2A405D68B4A6B9CEFF6 4
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:35.979 c68 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Local Storage\leveldb/MANIFEST-000001.2020/11/22-03:41:35.980 c68 Recovering log #3.2020/11/22-03:41:35.982 c68 Reusing old log C:\Users\user\AppD ata\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.259883273967046
Encrypted:	false
SSDEEP:	12:iuL+va5KkmiuFUtwR3/yRsN1LV5f5Kkm2J:dYa5KkSg72Df5Kkr
MD5:	6BB898FDF4F48F7FB616EC13DE7C0515
SHA1:	D86EE784D88AD4B54CF5D613D46F2AC5FF6EB775
SHA-256:	1E40584D3E782144924F8D08D949B52B4D0043A7E22800D3C5F36257CF610808
SHA-512:	D1AF013BB9B22558B9193FC2FBF498CF91DBD444A05BDE092B8DB7BF9A023F9378FB9332AE9BDA5F8D093F335BD5BA97A21564756D34A0706B024BD1D81E7C F
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:36.032 17c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2020/11/22-03:41:36.033 17c Recovering log #3.2020/11/22-03:41:36.034 17c Reusing old log C:\Users\user\AppData\Local \Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.288043788898763
Encrypted:	false
SSDEEP:	6:it+q2PWXp+N23iKKdKusNpZQMxIFUtwRFU9XZmwyRFU93VkwOWXp+N23iKKdKusx:iova5KkMFUtwRFU9X/yRFU9F5f5KkTJ
MD5:	DF9597D1AF577A7D747F9C47E103BA32
SHA1:	005DE4ABA425F01663BDDFAE1EBA0A4665F7DAC0
SHA-256:	C2BFC6D608F5122122C7418F1FCF6C03AAF9AAF4F58D420393415B376268CDC2
SHA-512:	C05B8DCAE81356F4A3103D700219FA011217AB1BC4C25546C4FAE65CB31088BE20A04B7057F0C7DE034F6537DBB1AA710FA18FEC3F87D50E4175C6AA6293BA5B
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:52.064 1578 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2020/11/22-03:41:52.065 1578 Recovering log #3.2020/11/22-03:41:52.065 1578 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\ac3d092f-84eb-4010-84a8-8a5c9f7ef356.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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\02166985-a922-4ec8-9a1a-5c07bb44bdeb.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):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.208545338138224
Encrypted:	false
SSDEEP:	12:iAM+va5KkkGHArBFUtwRK/yROlMV5f5KkkGHAryJ:Ha5KkkGgPgecQf5KkkGga
MD5:	FC794B113BD4087FA8143F094C8C56F8
SHA1:	793E580507C43467DA5F631A17F41AAF8F6C3B20
SHA-256:	B4BCFCBFECED72C03A7EDFF6B812F8C166B939BFED1D40FE1EF325E4163388BA
SHA-512:	00367FB80762C9E605F11EE43F55D65FD4CBC5CA0073EFD10273F8FCA75BF35EE404ED5B678B8B535153C8A2FCC86C02C0CF98EFDEB6331068F54A6C6DF17E3
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:48.146 f6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2020/11/22-03:41:48.152 f6c Recovering log #3.2020/11/22-03:41:48.153 f6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.243627347014604
Encrypted:	false
SSDEEP:	12:iZSi+va5KkkGHArqiuFUtwRUB/yRYV5f5KkkGHArq2J:ba5KkkGgCg78Ef5KkkGg7
MD5:	07ABF3F09CF8BFBE87A328063E12303C
SHA1:	2FF5C396B42BC61243BDB31E7510ABFB87E16A9D
SHA-256:	7A063CFDD38FB600251689049F9E63167C100911CE493F29010E67105FB7F475
SHA-512:	75327E3CB0E5118D55EBE892415E54929116427D6314C612A5F57B09E0B73102F28FD35AB52948557441D2EA5EFCD3BFF205BEABEC498487A49C609F8E37119C
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:48.158 159c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2020/11/22-03:41:48.162 159c Recovering log #3.2020/11/22-03:41:48.164 159c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.199616034159196
Encrypted:	false
SSDEEP:	12:dM+va5KkkGHArAFUtw+/ysMV5f5KkkGHArfJ:Ha5KkkGgkgIFf5KkkGgV
MD5:	ED25576B62029A56569A07DBE74BCC93
SHA1:	F3B2DDF6ECD7EB8715AC14672A0B7CCDDE016187
SHA-256:	F0699787374 73C80645AE5F45DB8F7F2EC38C19F84963A5E957F34EE4F0EA7E0
SHA-512:	F9D6111F16C64F0D470FFB929E91A81BE9A317DC98B1424444F77FA968D5917BCD7F91830E63ADD0ABB494403BD119FDD1A2663427FF8739F1AB927A6ACBD85
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:42:03.496 f6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2020/11/22-03:42:03.497 f6c Recovering log #3.2020/11/22-03:42:03.498 f6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

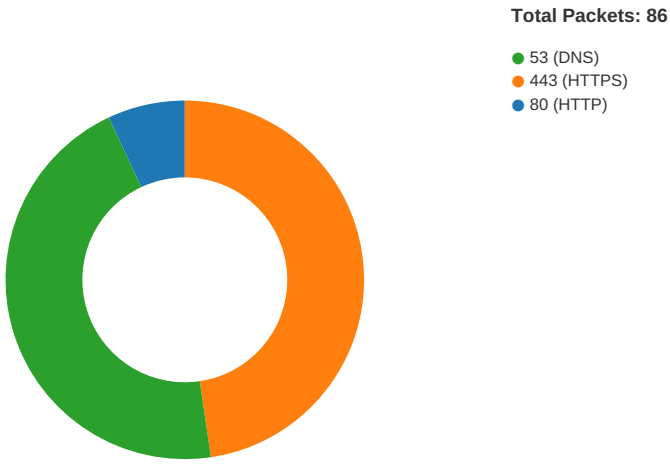
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.252781183916421
Encrypted:	false
SSDEEP:	6:ivcuMVq2PWXp+N23iKKdKpIFUtwRve1gZmwyRvtKQIkwOWXp+N23iKKdKa/WLJ:ivcuMVva5KkmFUtwRvkg/yRvtI5f5Kk7
MD5:	1B4DE7A5EAF841A3E5EF56A1830B5227
SHA1:	D2ED7AC21928D07DA42C9B2370426E1F0C16D45F
SHA-256:	FF15D1E194C6458BDC86BA851C7C4F1CD64AC9C1ADD7F732FC3FED97D378A981
SHA-512:	D9CD42608B5C926A3A30217AFE98AB3A29CFCA8359551B34118754514C78B8134817C1198B8784B4D0DC1E8416A35DCD21CF16195CD99000CF6AE3F1089CB88
Malicious:	false
Reputation:	low
Preview:	2020/11/22-03:41:35.760 1664 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2020/11/22-03:41:35.762 1664 Recovering log #3.2020/11/22-03:41:35.763 1664 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 03:41:38.554687023 CET	49717	80	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.556027889 CET	49720	80	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.571151018 CET	80	49717	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.571299076 CET	49717	80	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.572340965 CET	80	49720	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.572422981 CET	49720	80	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.573961020 CET	49717	80	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.590259075 CET	80	49717	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.735410929 CET	80	49717	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.735455036 CET	80	49717	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.735570908 CET	49717	80	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.750134945 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.766587019 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.766684055 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.767004013 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.783327103 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.786787987 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.786827087 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.786904097 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.811945915 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.812081099 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.812342882 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.828282118 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.828309059 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.828339100 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.828536987 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.828608990 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.844944954 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997042894 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997081041 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997143030 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997150898 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.997180939 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997226954 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997265100 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997291088 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997292042 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.997328043 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997334003 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.997375011 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997381926 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:38.997445107 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997483015 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997504950 CET	49722	443	192.168.2.3	23.227.38.65

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 03:41:38.997522116 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997562885 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:38.997595072 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:39.001950979 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.001980066 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002016068 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002051115 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:39.002053022 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002078056 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:39.002080917 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002118111 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002149105 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:39.002156019 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002193928 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002223015 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:39.002229929 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002270937 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002298117 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:39.002309084 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002347946 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002376080 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:39.002386093 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002424955 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002449989 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:39.002463102 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002490997 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002521038 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:39.002531052 CET	443	49722	23.227.38.65	192.168.2.3
Nov 22, 2020 03:41:39.002583027 CET	49722	443	192.168.2.3	23.227.38.65
Nov 22, 2020 03:41:39.142843008 CET	49727	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.143016100 CET	49728	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.143501043 CET	49729	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.143750906 CET	49730	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.143954992 CET	49731	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.144259930 CET	49732	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.161928892 CET	443	49727	151.101.1.12	192.168.2.3
Nov 22, 2020 03:41:39.162081003 CET	49727	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.162092924 CET	443	49728	151.101.1.12	192.168.2.3
Nov 22, 2020 03:41:39.162162066 CET	49728	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.162307978 CET	49727	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.162436008 CET	49728	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.162614107 CET	443	49729	151.101.1.12	192.168.2.3
Nov 22, 2020 03:41:39.162688971 CET	49729	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.162698984 CET	443	49730	151.101.1.12	192.168.2.3
Nov 22, 2020 03:41:39.162791014 CET	49730	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.162879944 CET	443	49731	151.101.1.12	192.168.2.3
Nov 22, 2020 03:41:39.162903070 CET	49729	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.162951946 CET	49731	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.163126945 CET	443	49732	151.101.1.12	192.168.2.3
Nov 22, 2020 03:41:39.163276911 CET	49732	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.163362026 CET	49731	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.163585901 CET	49730	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.163629055 CET	49732	443	192.168.2.3	151.101.1.12
Nov 22, 2020 03:41:39.181526899 CET	443	49727	151.101.1.12	192.168.2.3
Nov 22, 2020 03:41:39.181659937 CET	443	49728	151.101.1.12	192.168.2.3
Nov 22, 2020 03:41:39.181934118 CET	443	49729	151.101.1.12	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 03:41:31.306077957 CET	58361	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:31.333606005 CET	53	58361	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:32.425080061 CET	63492	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:32.452440023 CET	53	63492	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 03:41:33.732486963 CET	60831	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:33.759965897 CET	53	60831	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:34.659470081 CET	60100	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:34.694869041 CET	53	60100	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:36.799650908 CET	53195	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:36.826941013 CET	53	53195	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:38.501116991 CET	49563	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:38.501941919 CET	51352	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:38.508342028 CET	59349	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:38.508454084 CET	57084	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:38.544989109 CET	53	49563	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:38.547972918 CET	53	51352	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:38.548008919 CET	53	57084	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:38.551884890 CET	53	59349	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:38.686127901 CET	58823	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:38.722018957 CET	53	58823	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:38.798491001 CET	57568	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:38.842278004 CET	53	57568	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:38.937704086 CET	50540	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:38.983262062 CET	53	50540	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:39.105460882 CET	54366	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:39.105631113 CET	53034	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:39.141256094 CET	53	53034	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:39.142091036 CET	53	54366	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:39.242805958 CET	57762	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:39.278192043 CET	53	57762	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:39.636014938 CET	50713	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:39.671721935 CET	53	50713	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:39.735172033 CET	56132	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:39.778904915 CET	53	56132	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:39.897454023 CET	58987	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:39.902348042 CET	56579	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:39.904230118 CET	60633	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:39.924774885 CET	53	58987	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:39.929424047 CET	53	56579	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:39.944102049 CET	53	60633	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:40.144541979 CET	61292	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:40.184884071 CET	53	61292	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:40.402805090 CET	63619	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:40.405446053 CET	64938	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:40.443933964 CET	53	64938	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:40.446549892 CET	53	63619	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:40.586308956 CET	61946	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:40.623846054 CET	53	61946	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:41.010699987 CET	64910	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:41.046511889 CET	53	64910	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:42.071261883 CET	52123	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:42.098428011 CET	53	52123	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:43.203773022 CET	56130	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:43.239649057 CET	53	56130	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:44.015428066 CET	63978	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:44.042646885 CET	53	63978	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:47.922945976 CET	56803	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:47.966799974 CET	53	56803	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:51.330241919 CET	55359	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:51.386991024 CET	53	55359	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:52.837147951 CET	58306	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:52.882941008 CET	53	58306	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:54.538252115 CET	64124	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:54.574116945 CET	53	64124	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:59.622874022 CET	49361	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:59.668943882 CET	53	49361	8.8.8.8	192.168.2.3
Nov 22, 2020 03:41:59.859210968 CET	63150	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:41:59.894870043 CET	53	63150	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 03:42:00.067850113 CET	53279	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:42:00.103775978 CET	53	53279	8.8.8.8	192.168.2.3
Nov 22, 2020 03:42:01.821988106 CET	56881	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:42:01.849154949 CET	53	56881	8.8.8.8	192.168.2.3
Nov 22, 2020 03:42:06.050447941 CET	53642	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:42:06.087836027 CET	53	53642	8.8.8.8	192.168.2.3
Nov 22, 2020 03:42:17.593225002 CET	55667	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:42:17.632529020 CET	53	55667	8.8.8.8	192.168.2.3
Nov 22, 2020 03:42:18.245702982 CET	54833	53	192.168.2.3	8.8.8.8
Nov 22, 2020 03:42:18.283044100 CET	53	54833	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 03:41:38.508454084 CET	192.168.2.3	8.8.8.8	0x9782	Standard query (0)	hereforyou shop.com	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.105460882 CET	192.168.2.3	8.8.8.8	0xbd9f	Standard query (0)	cdn.shopify.com	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.636014938 CET	192.168.2.3	8.8.8.8	0x9792	Standard query (0)	monorail-edge.shopifysvc.com	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.902348042 CET	192.168.2.3	8.8.8.8	0xe992	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.904230118 CET	192.168.2.3	8.8.8.8	0x96b6	Standard query (0)	s.pinimg.com	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.144541979 CET	192.168.2.3	8.8.8.8	0x963c	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.405446053 CET	192.168.2.3	8.8.8.8	0xef31	Standard query (0)	ct.pinterest.com	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.586308956 CET	192.168.2.3	8.8.8.8	0xefd6	Standard query (0)	sellup.herokuapp.com	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:47.922945976 CET	192.168.2.3	8.8.8.8	0xdcbe	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:59.622874022 CET	192.168.2.3	8.8.8.8	0x2e79	Standard query (0)	www.recaptcha.net	A (IP address)	IN (0x0001)
Nov 22, 2020 03:42:18.245702982 CET	192.168.2.3	8.8.8.8	0x54b3	Standard query (0)	cdn.shopify.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 03:41:38.548008919 CET	8.8.8.8	192.168.2.3	0x9782	No error (0)	hereforyou shop.com		23.227.38.65	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.142091036 CET	8.8.8.8	192.168.2.3	0xbd9f	No error (0)	cdn.shopify.com	cdn.tm.shopifysvc.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:39.142091036 CET	8.8.8.8	192.168.2.3	0xbd9f	No error (0)	cdn.tm.shopifysvc.com	tls13.shopify.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:39.142091036 CET	8.8.8.8	192.168.2.3	0xbd9f	No error (0)	tls13.shopify.map.fastly.net		151.101.1.12	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.142091036 CET	8.8.8.8	192.168.2.3	0xbd9f	No error (0)	tls13.shopify.map.fastly.net		151.101.65.12	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.142091036 CET	8.8.8.8	192.168.2.3	0xbd9f	No error (0)	tls13.shopify.map.fastly.net		151.101.129.12	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.142091036 CET	8.8.8.8	192.168.2.3	0xbd9f	No error (0)	tls13.shopify.map.fastly.net		151.101.193.12	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.671721935 CET	8.8.8.8	192.168.2.3	0x9792	No error (0)	monorail-edge.shopifysvc.com	monorail-edge.tm.shopifysvc.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:39.671721935 CET	8.8.8.8	192.168.2.3	0x9792	No error (0)	monorail-edge.tm.shopifysvc.com	monorail-edge-central.shopifycloud.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:39.671721935 CET	8.8.8.8	192.168.2.3	0x9792	No error (0)	monorail-edge-central.shopifycloud.com	monorail-production-web-apps-a-us-central1-1.shopifycloud.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 03:41:39.671721935 CET	8.8.8.8	192.168.2.3	0x9792	No error (0)	monorail-production-web-apps-a-us-central1-1.shopifycloud.com		34.68.85.43	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.929424047 CET	8.8.8.8	192.168.2.3	0xe992	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:39.929424047 CET	8.8.8.8	192.168.2.3	0xe992	No error (0)	scontent.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:39.944102049 CET	8.8.8.8	192.168.2.3	0x96b6	No error (0)	s.pinimg.com	s-pinimg-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:39.944102049 CET	8.8.8.8	192.168.2.3	0x96b6	No error (0)	s-pinimg-com.gslb.pinterest.com	2-01-37d2-0006.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:40.184884071 CET	8.8.8.8	192.168.2.3	0x963c	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:40.184884071 CET	8.8.8.8	192.168.2.3	0x963c	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.443933964 CET	8.8.8.8	192.168.2.3	0xef31	No error (0)	ct.pinterest.com	www.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:40.443933964 CET	8.8.8.8	192.168.2.3	0xef31	No error (0)	www.pinterest.com	www.pinterest.com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:40.443933964 CET	8.8.8.8	192.168.2.3	0xef31	No error (0)	www.pinterest.com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:40.443933964 CET	8.8.8.8	192.168.2.3	0xef31	No error (0)	prod.pinterest.global.map.fastly.net		151.101.0.84	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.443933964 CET	8.8.8.8	192.168.2.3	0xef31	No error (0)	prod.pinterest.global.map.fastly.net		151.101.64.84	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.443933964 CET	8.8.8.8	192.168.2.3	0xef31	No error (0)	prod.pinterest.global.map.fastly.net		151.101.128.84	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.443933964 CET	8.8.8.8	192.168.2.3	0xef31	No error (0)	prod.pinterest.global.map.fastly.net		151.101.192.84	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.623846054 CET	8.8.8.8	192.168.2.3	0xefd6	No error (0)	sellup.herokuapp.com		52.6.203.110	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.623846054 CET	8.8.8.8	192.168.2.3	0xefd6	No error (0)	sellup.herokuapp.com		3.225.76.86	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.623846054 CET	8.8.8.8	192.168.2.3	0xefd6	No error (0)	sellup.herokuapp.com		54.144.192.68	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.623846054 CET	8.8.8.8	192.168.2.3	0xefd6	No error (0)	sellup.herokuapp.com		52.2.180.115	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.623846054 CET	8.8.8.8	192.168.2.3	0xefd6	No error (0)	sellup.herokuapp.com		34.192.53.253	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.623846054 CET	8.8.8.8	192.168.2.3	0xefd6	No error (0)	sellup.herokuapp.com		3.222.91.89	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.623846054 CET	8.8.8.8	192.168.2.3	0xefd6	No error (0)	sellup.herokuapp.com		34.234.209.139	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:40.623846054 CET	8.8.8.8	192.168.2.3	0xefd6	No error (0)	sellup.herokuapp.com		34.198.35.57	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:47.966799974 CET	8.8.8.8	192.168.2.3	0xdcbe	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:41:47.966799974 CET	8.8.8.8	192.168.2.3	0xdcbe	No error (0)	googlehosted.l.googleusercontent.com		172.217.16.193	A (IP address)	IN (0x0001)
Nov 22, 2020 03:41:59.668943882 CET	8.8.8.8	192.168.2.3	0x2e79	No error (0)	www.recaptcha.net		142.250.74.195	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 03:42:18.283044100 CET	8.8.8.8	192.168.2.3	0x54b3	No error (0)	cdn.shopify.com	cdn.tm.shopifysvc.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:42:18.283044100 CET	8.8.8.8	192.168.2.3	0x54b3	No error (0)	cdn.tm.shopifysvc.com	tls13.shopify.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 03:42:18.283044100 CET	8.8.8.8	192.168.2.3	0x54b3	No error (0)	tls13.shopify.map.fastly.net		151.101.1.12	A (IP address)	IN (0x0001)
Nov 22, 2020 03:42:18.283044100 CET	8.8.8.8	192.168.2.3	0x54b3	No error (0)	tls13.shopify.map.fastly.net		151.101.65.12	A (IP address)	IN (0x0001)
Nov 22, 2020 03:42:18.283044100 CET	8.8.8.8	192.168.2.3	0x54b3	No error (0)	tls13.shopify.map.fastly.net		151.101.129.12	A (IP address)	IN (0x0001)
Nov 22, 2020 03:42:18.283044100 CET	8.8.8.8	192.168.2.3	0x54b3	No error (0)	tls13.shopify.map.fastly.net		151.101.193.12	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- hereforyoushop.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49717	23.227.38.65	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2020 03:41:38.573961020 CET	73	OUT	GET / HTTP/1.1 Host: hereforyoushop.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Nov 22, 2020 03:41:38.735410929 CET	87	IN	HTTP/1.1 301 Moved Permanently Date: Sun, 22 Nov 2020 02:41:38 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive X-Sorting-Hat-PodId: 150 X-Sorting-Hat-ShopId: 48109224087 X-Storefront-Renderer-Rendered: 1 Location: https://hereforyoushop.com/ X-Frame-Options: DENY Content-Security-Policy: frame-ancestors 'none'; X-ShopId: 48109224087 X-ShardId: 150 Vary: Accept X-Shopify-Stage: production X-Dc: gcp-us-central1,gcp-us-central1,gcp-us-central1 X-Request-ID: 95c92b24-ef3b-4c2f-b374-fb55048087ec X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block NEL: {"report_to":"network-errors","max_age":2592000,"failure_fraction":0.01,"success_fraction":0.0001} Report-To: {"group":"network-errors","max_age":2592000,"endpoints":[{"url":"https://monorail-edge.shopifycloud.com/v1/reports/nel/20190325/shopify"}]} CF-Cache-Status: DYNAMIC cf-request-id: 068f6d25140000d7212037f000000001 Server: cloudflare CF-RAY: 5f5f4ae81d7cd721-FRA Data Raw: 35 64 0d 0a 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 68 65 72 65 66 6f 72 79 6f 75 73 68 6f 70 2e 63 6f 6d 2f 22 3e 72 65 64 69 72 65 63 74 65 64 3c 2f 61 3e 2e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 5d<html><body>You are being redirected.</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 22, 2020 03:41:40.487519026 CET	151.101.0.84	443	192.168.2.3	49748	CN=*.pinterest.com, O="Pinterest, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 04 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 22, 2020 03:41:40.487986088 CET	151.101.0.84	443	192.168.2.3	49749	CN=*.pinterest.com, O="Pinterest, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 04 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 22, 2020 03:41:40.488228083 CET	151.101.0.84	443	192.168.2.3	49750	CN=*.pinterest.com, O="Pinterest, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 04 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 22, 2020 03:41:40.602067947 CET	151.101.0.84	443	192.168.2.3	49752	CN=*.pinterest.com, O="Pinterest, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 04 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 22, 2020 03:41:40.831221104 CET	52.6.203.110	443	192.168.2.3	49754	CN=*.herokuapp.com, O="Heroku, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jun 15 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Wed Jul 07 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Nov 22, 2020 03:41:40.831259012 CET	52.6.203.110	443	192.168.2.3	49753	CN=*.herokuapp.com, O="Heroku, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jun 15 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Wed Jul 07 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Nov 22, 2020 03:42:09.108504057 CET	52.6.203.110	443	192.168.2.3	49834	CN=*.herokuapp.com, O="Heroku, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jun 15 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Wed Jul 07 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4952 Parent PID: 1004

General

Start time:	03:41:34
Start date:	22/11/2020
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://herefor youshop.com'
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: 4796 Parent PID: 4952

General

Start time:	03:41:36
Start date:	22/11/2020
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=1544,13729553244047984668,6139627914611722907,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1720 /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