ID: 358579
Cookbook: browseurl.jbs
Time: 21:39:56
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

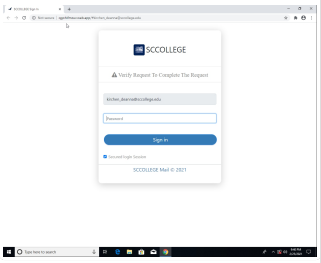
Analysis Report https://u16095581.ct.sendgrid.net/ls/cli…

Overview

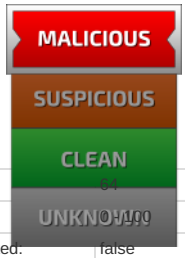
General Information

Sample URL:	https://u16095581.ct.sendgrid.net/ls/click?upn=FLaa9Uev-2B7s-2FZ9Dw3t6-2Fob...CdYW3168zSE6-2FrgVMBpTopWiclUE2uJbujZKS9qBrMxjc8wcVkUUy8Jmc7-2BKB9-2BhEc-3D
Analysis ID:	358579
Infos:	

Most interesting Screenshot:



Detection

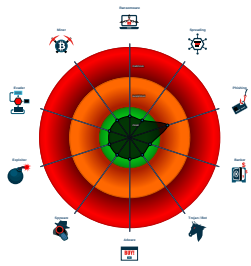


Score:	64
Range:	
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6816 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://u16095581.ct.sendgrid.net/ls/click?upn=FLaa9Uev-2B7s-2FZ9Dw3t6-2FoboxXa9RoxlkakQvTvnjy9nXTXjD6tNZcebsQGigytMZye255UswQ6f3sQ0K3qccZrkmIGtWjJPIGztPn38pYzM-3D7_6s_DwB70HpLJuR35GFtSIesHJrrx5IO6qEPxbkrEpQrYnrx-2FXwixj3Q3HnEwW-2Fs-2BBPbBxlPPFHusk7-2BufOFY4-2BYO9fqGw8G6IKDphuEsqM-2B5hWTu2tXyTpvimSzAQwQnBG-2BsgMdkv-2B3igkZIHlWGKqVkU4mGhq9zYrBUF7V0zSm4CdYW3168zSE6-2FrgVMBpTopWiclUE2uJbujZKS9qBrMxjc8wcVkUUy8Jmc7-2BKB9-2BhEc-3D' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7016 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1608,13295437612127757828,17913449545750257871,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

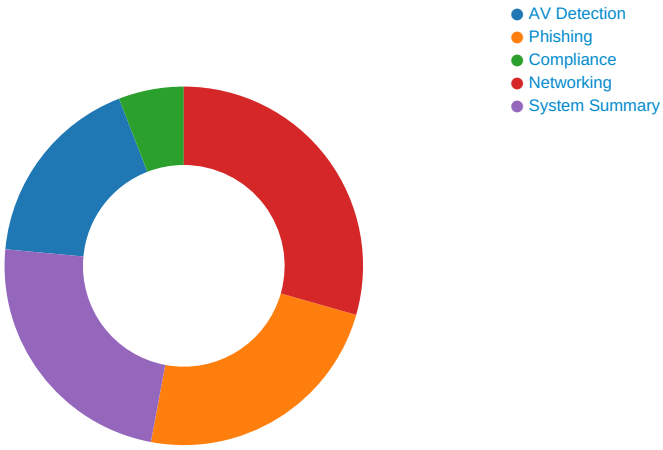
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

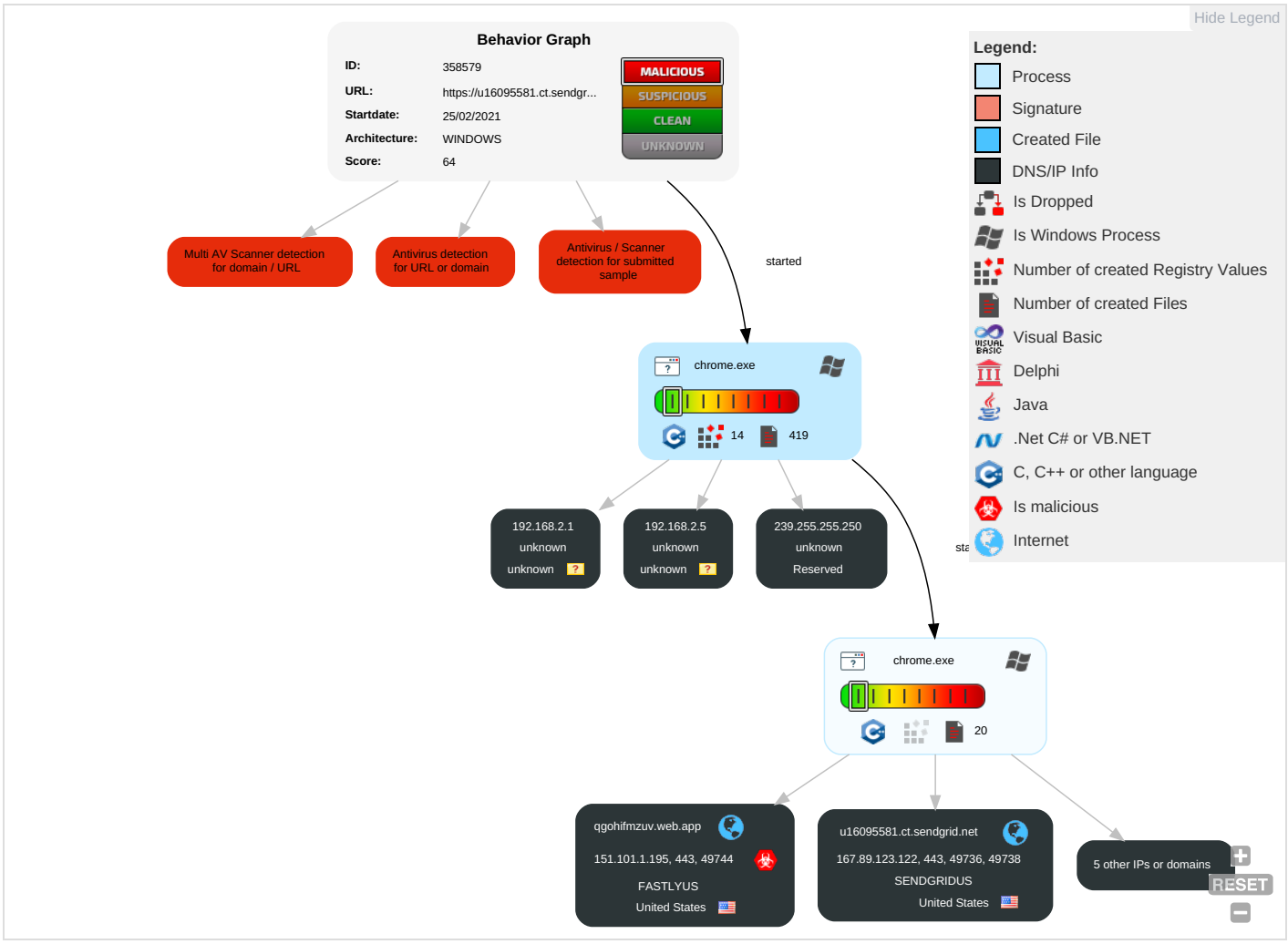
Compliance:

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

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

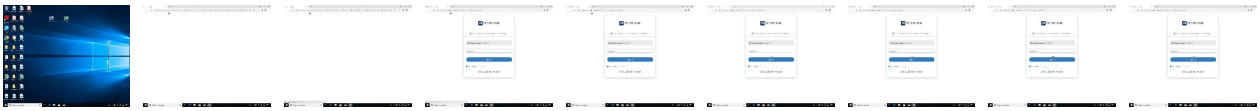
Behavior Graph

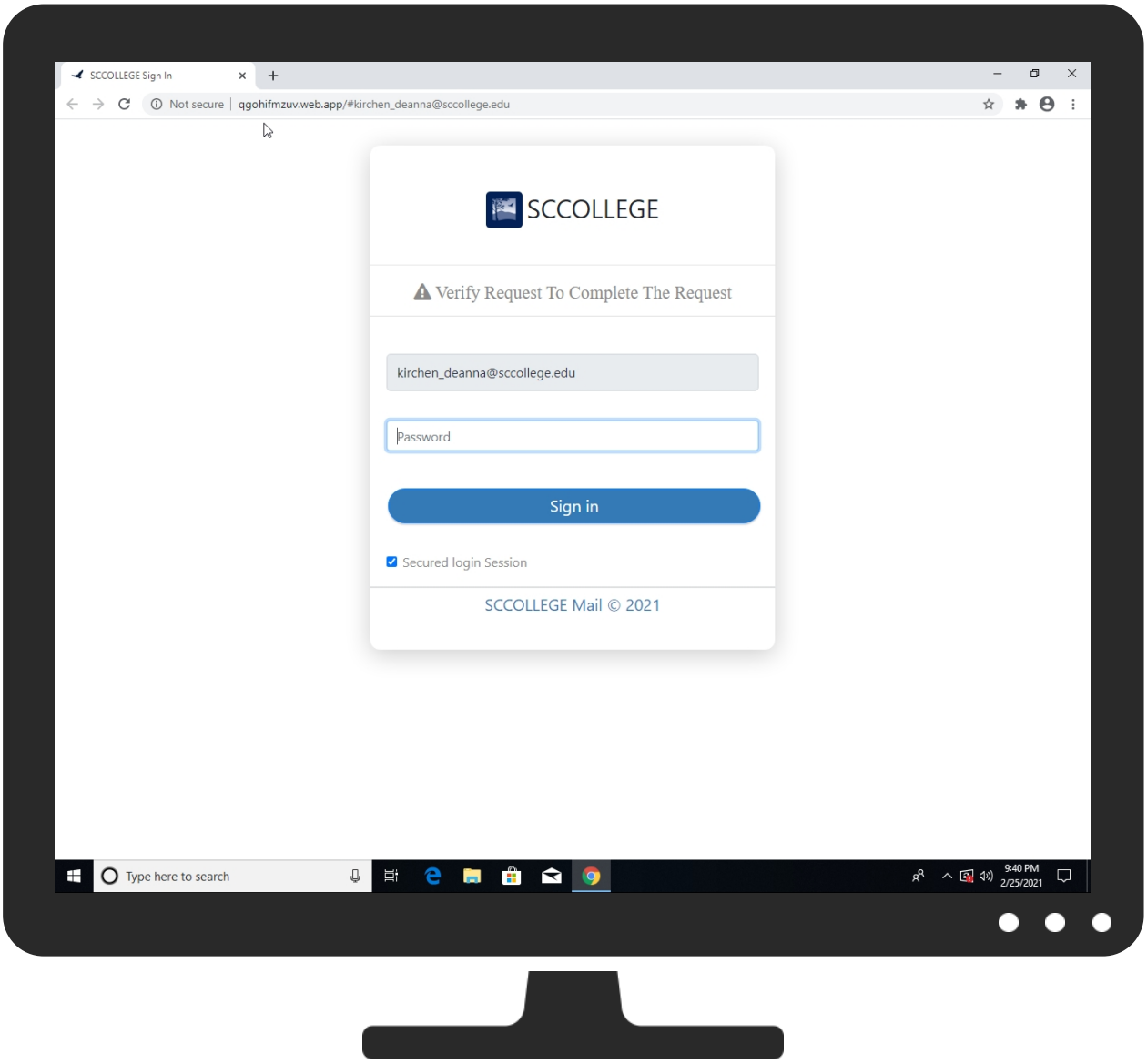


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://u16095581.ct.sendgrid.net/ls/click?upn=FLaa9Uev-2B7s-2FZ9Dw3t6-2FoboxXa9RoxlkakQvTvnjy9nXTXjD6tNZcebsQGigytMZye255UswQ6f3sQ0K3qccZrkmIGtWjJPIGztPn38pYzM-3D7_6s_DwB70HpLJuR35GFtSIesHJrrx5IO6qEPxbkrEpQrYnrx-2FXwixj3Q3HnEwW-2Fs-2BBPbBxlPPFHusk7-2BufOFY4-2BYO9fqGw8G6IKDphuEsqM-2B5hWTu2tXyTpvimSzAQwQnBG-2BsgMdkv-2B3igkZIHlWGKqVkU4mGhq9zYrBUF7V0zSm4CdYW3168zSE6-2FrgVMBpTopWiclUE2uJbujZKS9qBrMxjc8wcVkUUy8Jmc7-2BKB9-2BhEc-3D	0%	Avira URL Cloud	safe	
http://https://u16095581.ct.sendgrid.net/ls/click?upn=FLaa9Uev-2B7s-2FZ9Dw3t6-2FoboxXa9RoxlkakQvTvnjy9nXTXjD6tNZcebsQGigytMZye255UswQ6f3sQ0K3qccZrkmIGtWjJPIGztPn38pYzM-3D7_6s_DwB70HpLJuR35GFtSIesHJrrx5IO6qEPxbkrEpQrYnrx-2FXwixj3Q3HnEwW-2Fs-2BBPbBxlPPFHusk7-2BufOFY4-2BYO9fqGw8G6IKDphuEsqM-2B5hWTu2tXyTpvimSzAQwQnBG-2BsgMdkv-2B3igkZIHlWGKqVkU4mGhq9zYrBUF7V0zSm4CdYW3168zSE6-2FrgVMBpTopWiclUE2uJbujZKS9qBrMxjc8wcVkUUy8Jmc7-2BKB9-2BhEc-3D	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
qgohifmzuv.web.app	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://qgohifmzuv.web.app/#kirchen_deanna@sccollege.edu	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
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://dns.google	0%	URL Reputation	safe	
http://https://qgohifmzuv.web.app/assets/js/jquery.min.js	100%	Avira URL Cloud	phishing	
http://https://qgohifmzuv.web.app	100%	Avira URL Cloud	phishing	
http://https://qgohifmzuv.web.app/#kirchen_deanna	100%	Avira URL Cloud	phishing	
http://https://qgohifmzuv.web.app/assets/js/script.min.js	100%	Avira URL Cloud	phishing	
http://https://qgohifmzuv.web.app/8w	100%	Avira URL Cloud	phishing	
http://https://qgohifmzuv.web.app/	100%	Avira URL Cloud	phishing	
http://https://qgohifmzuv.web.app/assets/bootstrap/js/bootstrap.min.js	100%	Avira URL Cloud	phishing	
http://https://qgohifmzuv.web.app/x	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d26p066pn2w0s0.cloudfront.net	99.84.90.99	true	false		high
u16095581.ct.sendgrid.net	167.89.123.122	true	false		high
qgohifmzuv.web.app	151.101.1.195	true	true	• 7%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	142.250.184.33	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
logo.clearbit.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://qgohifmzuv.web.app/#kirchen_deanna@sccollege.edu	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://logo.clearbit.com/sccollege.edu	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	a216b292-35e3-4a8a-8ccc-1298dac27205.tmp.1.dr, 3231859a-0a2e-4d47-8b6d-78b387703288.tmp.1.dr, 813890ff-223e-45e6-91fa-77fcb9e4b480.tmp.1.dr, 962ff325-93c1-4988-b3a8-dfc330ef7561.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://qgohifmzuv.web.app/assets/js/jquery.min.js	40d8ad6f0f62e96a_0.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://qgohifmzuv.web.app	962ff325-93c1-4988-b3a8-dfc330ef7561.tmp.1.dr	true	• Avira URL Cloud: phishing	unknown
http://https://u16095581.ct.sendgrid.net/ls/click?upn=FLaa9Uev-2B7s-2FZ9Dw3t6-2FoboxXa9RoxlkakQvTvnjy9nXTXj	History.0.dr	false		high
http://https://clients2.googleusercontent.com	3231859a-0a2e-4d47-8b6d-78b387703288.tmp.1.dr, 962ff325-93c1-4988-b3a8-dfc330ef7561.tmp.1.dr	false		high
http://https://qgohifmzuv.web.app/#kirchen_deanna	History.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://qgohifmzuv.web.app/assets/js/script.min.js	dea8b6c059e7296b_0.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://qgohifmzuv.web.app/8w	40d8ad6f0f62e96a_0.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://qgohifmzuv.web.app/	6de907a866c54acf_0.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://qgohifmzuv.web.app/assets/bootstrap/js/bootstrap.min.js	6de907a866c54acf_0.0.dr	true	• Avira URL Cloud: phishing	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://qgohifmzuv.web.app/x	dea8b6c059e7296b_0.0.dr	true	• Avira URL Cloud: phishing	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.89.123.122	unknown	United States		11377	SENDGRIDUS	false
142.250.184.33	unknown	United States		15169	GOOGLEUS	false
99.84.90.99	unknown	United States		16509	AMAZON-02US	false
151.101.1.195	unknown	United States		54113	FASTLYUS	true
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358579
Start date:	25.02.2021
Start time:	21:39:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Sample URL:	http://https://u16095581.ct.sendgrid.net/ls/click?upn=FLaa9Uev-2B7s-2FZ9Dw3t6-2FoboxXa9RoxlkakQvTvnjy9nXTXjD6tNZcebsQGigytMZye255UswQ6f3sQ0K3qccZrkmIGtWjJPIGztPn38pYzM-3D7_6s_DwB70HpLJuR35GFtSIesHJrrx5IO6qEPxbkrEpQrYnrx-2FXwixj3Q3HnEwW-2Fs-2BBPbBxlPPFHusk7-2BufOFY4-2BYO9fqGw8G6IKDphuEsqM-2B5hWTu2tXyTpvimSzAQwQnBG-2BsgMdkv-2B3igkZIHlWGKqVkU4mGhq9zYrBUF7V0zSm4CdYW3168zSE6-2FrgVMBpTopWiclUE2uJbujZKS9qBrMxjc8wcVkUUy8Jmc7-2BKB9-2BhEc-3D
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.win@35/174@4/8
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.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): 23.54.113.53, 168.61.161.212, 52.255.188.83, 40.88.32.150, 13.64.90.137, 216.58.208.142, 142.250.180.77, 216.58.205.78, 173.194.187.230, 216.58.208.170, 142.250.185.131, 142.250.180.163, 142.250.180.138, 216.58.206.36, 216.58.209.42, 142.250.184.42, 142.250.184.74, 142.250.184.106, 216.58.198.42, 172.217.21.74, 142.250.180.74, 142.250.180.106, 142.250.180.170, 216.58.206.42, 216.58.206.74, 51.104.144.132, 52.155.217.156, 20.54.26.129, 216.58.208.131, 216.58.208.163, 92.122.213.247, 92.122.213.194, 173.194.164.139, 74.125.104.88, 51.104.139.180, 173.194.164.124 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, r1---sn-4g5ednly.gvt1.com, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, r5.sn-4g5e6nle.gvt1.com, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, r2---sn-4g5ednle.gvt1.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, clients2.google.com, redirector.gvt1.com, update.googleapis.com, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, www.gstatic.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, accounts.google.com, content-autofill.googleapis.com, r6---sn-4g5e6nl7.gvt1.com, fonts.gstatic.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, www.googleapis.com, ris.api.iris.microsoft.com, r6.sn-4g5e6nl7.gvt1.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, r2.sn-4g5ednle.gvt1.com, blobcollector.events.data.trafficmanager.net, r5---sn-4g5e6nle.gvt1.com, clients.l.google.com, r1.sn-4g5ednly.gvt1.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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:\Users\user\AppData\Local\Google\Chrome\User Data\05af708f-88a1-4b8c-b248-537a0e18a7b1.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):	156605
Entropy (8bit):	6.051716742999711
Encrypted:	false
SSDEEP:	3072:4TsmGflW7LtsevCLxZJasImhjp3qm4JaPlrnJFcbXafIB0u1GOJmA3iuR0:4CflkhsXNZswa2bHaqfllUOoSiuR0
MD5:	A15A6035BA8804620F51FF9B106E30A4
SHA1:	8C502231641B793994E5606CD789377FB5D531EE
SHA-256:	B9BF0770541A9B25AFEC1A1E3A377F01DCE86E9CF9D6BBE4B3DCC430DBDC51DA
SHA-512:	CF87C169B5E35877B60AF6BDDB19F4722F8BD56DE349C459E446A3FC71E52269949AD1BFA27528D1387F84A8D5D67328D870DA084A8ED5C5E6FCD3F356C08A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.61428564436891e+12,"network":1.614285647e+12,"ticks":302779923.0,"uncertainty":4548758.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715434988"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\07f56a1c-236f-49cf-840a-a232fba6d156.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):	156762
Entropy (8bit):	6.05226997551829
Encrypted:	false
SSDEEP:	3072:4osmGflW7LtsevCLxZJasImhjp3qm4JaPlrnJFcbXafIB0u1GOJmA3iuR0:4PflkhsXNZswa2bHaqfllUOoSiuR0
MD5:	3F8CE1EC9EDB1C4391094044CAC38966
SHA1:	F9F5CEFEA19DA687D1B1CC17360C8778E37553DA
SHA-256:	910C3F376D7ECE83F00A13EE995CEBC9E7184F75992C1940F1A408CBB9C26DE8
SHA-512:	B2D5881DC73F1FE06E894586E2B404B5F32A0509E900ECB4339D9B90B4B05EE34DCBDDCCE354D1CC1B37F338B8FFF1552DA3B64F4347E38A6435424C20DCC6D
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.61428564436891e+12,"network":1.614285647e+12,"ticks":302779923.0,"uncertainty":4548758.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"

C:\Users\user\AppData\Local\Google\Chrome\User Data\4c603eba-cf03-4a28-ab6e-43dec1cf915a.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):	156845
Entropy (8bit):	6.052436338379752
Encrypted:	false
SSDEEP:	3072:BosmGflW7LtsevCLxZJasImhjp3qm4JaPlrnJFcbXafIB0u1GOJmA3iuR0:BPflkhsXNZswa2bHaqfIlUOoSiuR0
MD5:	1E847548DDC009248DC7BAC985323249
SHA1:	39DE19B6624EFACE0763624753887A7C54F50732
SHA-256:	18C5D7C435670C89A4D5A875DD1165696EB119B25A2E46E0F31FBFB1FAE1F985
SHA-512:	685902EF2E78BE282A740AF9986E5C646D8C69024E7F297B8B0ECC51DB33EB57584926EF978BF472EB321549892B9FBD2E8721EA0963502AF448C483B05658A2
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.61428564436891e+12,"network":1.614285647e+12,"ticks":302779923.0,"uncertainty":4548758.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"

C:\Users\user\AppData\Local\Google\Chrome\User Data\6149b4b3-5a88-4925-af07-77dac008aaa8.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):	156931
Entropy (8bit):	6.052599560808917
Encrypted:	false
SSDEEP:	3072:JosmGflW7LtsevCLxZJasImhjp3qm4JaPlrnJFcbXafIB0u1GOJmA3iuR0:JPflkhsXNZswa2bHaqfIlUOoSiuR0
MD5:	3A3BD6CE368D10E169F83C03C5F1161D
SHA1:	7E0901E7FDD0272860C32F35FD943C4E8C5DE393
SHA-256:	1894088116D5ABE109C73BA11EBDD9741A3ECADF7E4303F3B0D204C40B1656E2
SHA-512:	77D8308277113132FE6526132CDB03B50305D8C2C4EFBF78400CEA239FA83B165480D9C8B711A9794640C2BB1DC06E4AA68381672F4C5E819E43706E570A03AE
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.61428564436891e+12,"network":1.614285647e+12,"ticks":302779923.0,"uncertainty":4548758.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"

C:\Users\user\AppData\Local\Google\Chrome\User Data\666026a8-95fd-4873-a333-6e205007a998.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):	165085
Entropy (8bit):	6.082021722593356
Encrypted:	false
SSDEEP:	3072:wHEsmGflW7LtsevCLxZJasImhjp3qm4JaPlrnJFcbXafIB0u1GOJmA3iuR0:8DflkhsXNZswa2bHaqfIlUOoSiuR0
MD5:	045C3CDB78EB224C40BCD362F2579255
SHA1:	60E4E85842427A55EE4569831B2C7140D8060761
SHA-256:	C5DB2B57042028193A3D7F86895CD254EF5E8A7331F25A7EC7713879CF3549D7
SHA-512:	D0A443CBFC10E9A14F5A08B951BE730E944C311BC0F25F7ACDD280F7D9DDB4F1F62C703469F308919AAA0980125BF8F8BB87A92D77EECCAD79C4AA7018CDA0C
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.61428564436891e+12,"network":1.614285647e+12,"ticks":302779923.0,"uncertainty":4548758.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715434988"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\6e58f150-3d8a-4687-8485-2be551ec89fb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\6e58f150-3d8a-4687-8485-2be551ec89fb.tmp

File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7464020381842027
Encrypted:	false
SSDEEP:	384:56wyth/Q6bAX3VcCR8NhrqvF/3GJfmHnCGSVrAjtJxeDrbKrolmgUegfBtZ6OnnN:8ySSFFizsasenRv383rW/KFjBhF
MD5:	AE97A1601714AC69232627B325395442
SHA1:	699673C0E6835949DFAAFC6EC7DE99CB9D7922A6
SHA-256:	B9D46A799C90130588A5C5A492FB17AB4F6B2150B58C3F5E72F3D7E1757A3294
SHA-512:	623CE554ED5EC09275FF19650AAB0F0DCC43A6C49A6B75862A5F8C95845D3FBD085A86F558D33E88534F28ED79D2B2AFB06E6EC9C182DBE3FF43A6C05D4948D
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....28.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3231859a-0a2e-4d47-8b6d-78b387703288.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324851660 7334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\67ed8a34-b10b-46c1-afd8-f19d213b8616.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):	1206
Entropy (8bit):	5.575185588173868
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\67ed8a34-b10b-46c1-afd8-f19d213b8616.tmp	
SSDEEP:	24:Ym6H0UhsSZfU4hVG1KUsUzkq/HeUe8zUek7wUlRUeiQ:Ym6UUhZUlKUsVqPeUekUeywU7UeP
MD5:	F9377A2C9180A10B1DA719A4A0A759C4
SHA1:	937681B64A6098E990386887C9DDA353A43B4B12
SHA-256:	1B7B5DF93F4E2FFE3721937ECF08A1E1EB695713023F708501308D345C51730E
SHA-512:	3EB70794C62E54499D4CE3A458D2F1EC254B99BA4A4E942EE10155A89F57CAB90D61A1E2956F1A7CA90646ED8C9F878044687AE3CB4119A69D75FFFC5220DD0
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1645821645.703075,"host":"klJs6DZaCmhP00Wxg1A5H05AizZwE1bpesnywUFEwGQ=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614285645.70308},{"expiry":1645821645.411806,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614285645.411811},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1645821644.643477,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\81e66f72-9213-4f03-8935-42b38aa9d99c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\962ff325-93c1-4988-b3a8-dfc330ef7561.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):	2278
Entropy (8bit):	4.870510327709468
Encrypted:	false
SSDEEP:	48:Y2zMKDHGXtwWsDRLs76qCYsykzsrSsWyKsa3zsdTMHTYhbw:JzMKDHGXOJwxCS9gbWTG0hM
MD5:	B51E6505AF89A6CF2E4F5D16A48E5BB6
SHA1:	3FC749FD2D9777D68811AF5934F66309A1317FF6
SHA-256:	F4270BC8EB6E3B069BB31ED21E972691984E11D55CDD8516992B90743DADBC18
SHA-512:	9D93A75FB2FE90C2E79B643E7D69E720F5CF41D1255A8FD45C9EE78A760687EC18F45583107BB488FE9EEFAC4CCC220594FAA090623C2082D0781E4CDDA6340B
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13261351244643353","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13261351245411313","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.168574912944693
Encrypted:	false
SSDEEP:	6:mN2ewsN+q2Pwkn23iKKdK9RXXTZIFUtpe2eS/XZmwPe2enVkwOwkn23iKKdK9RX3:exIvYf5Kk7XT2FUtpOUX/POV5Jf5Kk73
MD5:	84A69D456749363A73B26413F72F259A
SHA1:	9D0DE424595E6A8A16A6A87EF0957F4324079762
SHA-256:	6321A7F8FBE7A5D6B484375442FB3CDA4CF48C78A80AA16BFD39A62E46199A19

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
SHA-512:	DA266AEFFE773DEDDF430B4443993E797BB4A66C15C4E8521E1F8B42C9D3A4617630864AA5D27B6F7B647DACEDA64991CECF9EE9F7C9A6A61B84E1654204639
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:50.146 1a18 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/02/25-21:40:50.147 1a18 Recovering log #3.2021/02/25-21:40:50.151 1a18 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.127371083655669
Encrypted:	false
SSDEEP:	6:mN2e3+q2Pwkn23iKKdKyDZIFUtpe2eRZmwPe2elVkwOwkn23iKKdKyJLJ:eOvYf5Kk02FUtpOR/POL5Jf5KkWJ
MD5:	56A39F9038737D37361C37C231B12DCF
SHA1:	1163139945CDF291A60DDF821E620D38432DDEF3
SHA-256:	F491214AF512CD02216DD9EE9FDF9D11008C09067053BEF8E6489394B5661368
SHA-512:	581429F0F8CC414041546C74B4B2EC486E855208496BED7CD83953177BAECFA729C4FC3F9FA00318EF20DB8D5B1CE02503817394F3A459AD3F76286E34D99B2F
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:50.128 1a18 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/02/25-21:40:50.131 1a18 Recovering log #3.2021/02/25-21:40:50.131 1a18 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\40d8ad6f0f62e96a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.513137312487897
Encrypted:	false
SSDEEP:	6:ms7glXYJHQysQXFHg0qrk4xxfdyqvP4a/ZK6t:BMlQWQV7qrdmqHBT
MD5:	EFEA3FDB1CC229E7FD96728FCB86D982
SHA1:	BF259D462A4C497A0EFD2968B253DF89C6F91D80
SHA-256:	23778DF37EBE950464236CF1E7D0838555A8034030099B318CD7CC98C4133214
SHA-512:	3CD16094D2DD2C813BA51FCBE22ACA34883C1AB7AFE34694C6CAE02CA78B353DBEBAB27AD76F856585649B8FD3CF779222098653303510D5830A8DCB97D83936
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S.....9....._keyhttps://qgohifmzuv.web.app/assets/js/jquery.min.js .https://qgohifmzuv.web.app/8w.r../.....3..a.R..;..DK.v....,...".j.N..I..A..Eo.....c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6de907a866c54acf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.454208427255257
Encrypted:	false
SSDEEP:	3:m+lAY2K8RzYJ3MWQ/XEYH3WXET/uFvDa3+jl/lHCMztF/WaW4bh6wwTGH5mkX5tP:mASYJHQfEqgErJ0gMxMaWMMU4kbK6t
MD5:	A26C86BFB411B7952EEBC491160BC37B
SHA1:	8497FC551665025BE3ACF0DB5808F61C6F079C7B
SHA-256:	B36B73503870F5653316D66EB6C37A82AC24E9789D9E66F7D07914C953CC3336
SHA-512:	99AEFD974E96F622EB113A018201039BEBA15C59D6DDFEE51B96A5C0CE7A3DB347558D0D2FA28FFA539D84CD3C7968D01300A6D9B448F9DB3CB4C9D5DE90B62
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`....t....._keyhttps://qgohifmzuv.web.app/assets/bootstrap/js/bootstrap.min.js .https://qgohifmzuv.web.app/...r../.....#s)G|.Z...y.$6.L.e.c.]9...2v.A..Eo.....r.O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dea8b6c059e7296b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dea8b6c059e7296b_0	
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.484645698445699
Encrypted:	false
SSDEEP:	3:m+lxsv8RzYJ3MWQyOJLuFvDa3VY1/l/lHC2h//6Ag14YG470kSkvg4mZ5l/l/pK+:mssEYJHQyOJLJlYHg2x6t4xIXvAxK6t
MD5:	65BEB8D3C43AEC7382324E8FAEAF18F9
SHA1:	CB6CBE1F2129E2666AF91E7C3A9FFB5366DA0826
SHA-256:	DBA5FF9886CC29C0D8A7C208281EAB2403E37AF7AE713E10B1CCA915C5ADD4C2
SHA-512:	72E58740D12357E7F87BC8267F8F3380759832C2C2EC94AD67C39FF42AE97E2588FCACB5EDE856C72C87DEC48609BDD0426BB6AF24E3CEF376A355843A37708
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...h....._keyhttps://qgohifmzuv.web.app/assets/js/script.min.js .https://qgohifmzuv.web.app/x..r../.....!..!..E.q..C.....Q.....+.A..Eo.....L.....A..E o.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	312
Entropy (8bit):	4.881447212979647
Encrypted:	false
SSDEEP:	3:3E0l/9l+8lTNhIQKlrlUqTHrv9lptlll5/lOptlllKL8ftlll0l0qxzUsR8ftllH:ZjlIJOqjrBcTxzPawAfyDnW
MD5:	FFDA2FB1D7C51BCE136F988AFD5ADA92
SHA1:	FCAC1787BB836D3D9390BB1523067C745E3A9647
SHA-256:	8E9C797EFE420781891A4CDBFFCF971EFF9DA4E5D22E7AAE0B88D2CD50D41E97
SHA-512:	5C7CCA5541511F5886DD7177BD4424D41BAC7500778794D3B03CFAE27F3660926F70DCC4A8A3CCCBF142CC8B2FE5A22C98D24B7F2D2A38FCD3AFAB44E4980 1
Malicious:	false
Reputation:	low
Preview:	0....P.9oy retne.....k).Y....@..r../.....J.f...m@..r../.....j.b.o..@@..r../.....^}.Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&. ./.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../.....].s../.

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):	8192
Entropy (8bit):	1.358065807893325
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwIe9pdk6pf1H1oNu:TekLLOpEO5J/Kn7UL+DfvoNu
MD5:	BA9FF3CA9BA84B7B6D51A9C2BAEF0D6C
SHA1:	DD73AA21877C1DBDEA6980EE711023DF21C75E96
SHA-256:	0AD84C3061FDB10DFC3A780BBACF987D4BAD264358C975B1870CB133F6CE7AEC
SHA-512:	8CF164DCE353EE8EB7775F67B29A734DEED7BFC9D90B3CCC16B0954910E1742AA0FB736DF491CDA562E7A050B7069415C4696B585D6336B405E2CCD921C486 A
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):	8732
Entropy (8bit):	1.3165679320623291
Encrypted:	false
SSDEEP:	24:He9H6pf1H1oNGvqLbJLbXaFpEO5bNmISHn06Uwbt9:HbfvoNGvq5LLOpEO5J/Kn7UAt9
MD5:	13AC5770D0B4AA3205DF24013CC92E3D
SHA1:	E840B6A061B24479F61F972A93F887A45AD9868E
SHA-256:	D4D9EA3A1AE1348614B6B00D003B58FB021AD2E06434AB2E2362500A2DA4397E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
SHA-512:	976CEAF9FB5668D87C3D1F155AA2AB7C4FD63B1E22FDC99113841662D840BCE7028E52F450B26BECDD9A980B51D2B2C591B3D67DB242A49583E9639485040A8
Malicious:	false
Reputation:	low
Preview:	.....UNF..... ....

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):	2042
Entropy (8bit):	4.137295194443955
Encrypted:	false
SSDEEP:	24:34S3O9ENlrlJNLU4DQARjPdlscZL764GFnHMcJOlwSDCVyU5gBM9FaR7Dlr:34HexHXQARjPVNqluNLU+BMu5r
MD5:	0063298F52C04190975FCF7222FC3F19
SHA1:	68F9A40E5F2FFF28CFB68E78F690AC6D67A94C84
SHA-256:	5B5DD1F94EF67544A438A60D5D7DE8801CE0C285773D4ADCFDBC6230C319FB6C
SHA-512:	505131D5B2EA46FA67F790C7D16C69FA5F3958A493F629B8BD675382CD19606A71444FEA8F3D8C4CF49B47F59E0A1F225A161E045B1E5EBD1878C27BD5B56CA
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...ac6ca0b0_d5df_4024_be38_d9c7b7e7a077.....s..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....8...https://qgohifmzuv.web.app/#kirchen_deanna@sccollege.edu ....S.C.C.O.L.L.E.G.E. .S.i.g.n. .I.n...$... .....h.....`.....@.....q*/.....q*/.....x...8...h.t.t.p.s.:./. /.q.g.o.h.i.f.m.z.u.v...w.e.b...a.p.p./.#.k.i.r.c.h.e.n._.d.e.a.n.n.a.@.s.c.c.o.l.l.e.g.e...e.d.u.....`.....X..... .....@.....X..... .....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....N.o. .o.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.204128771145178
Encrypted:	false
SSDEEP:	6:mN2ylXQL+q2Pwkn23iKKdK8aPrqIFUtpe2yUdSG1ZmwPe2yjMQLVkwOwkn23iKKV:ydQyvYf5KkL3FUtpCUQg/PCoQR5Jf5KV
MD5:	86C33F173DA5DA83E9330D2DF49412E1
SHA1:	C3C482AD4704728EBAC775685ED6ADB44F2FE51A
SHA-256:	80F403A5C191D20C0D92DCBC7395AAE39FA24CFB22232834B51D9D72080C8E07
SHA-512:	D96F263274B850693BDA4A9D007D9F1ED2999F8D73EA7F99A7A3E5415752B06DA43764A4F03C092B7D1FD2472F9DDB63B3461D58A8FF74294B2FDF80B3D61E8
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:41.661 1ba8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/02/25-21:40:41.663 1ba8 Recovering log #3.2021/02/25-21:40:41.664 1ba8 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

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):	5.2009041745741555
Encrypted:	false
SSDEEP:	6:mN2oq2Pwkn23iKKdK8NIFUtpe22XZmwPe22FkwOwkn23iKKdK8+eLJ:ovYf5KkpFUtpm/Pa5Jf5KkqJ
MD5:	3AD385ECC6F682F09EC8C1D42DB29B6D
SHA1:	FEE40444172871047E66CCF6D4BC153CB1FDAE05
SHA-256:	2B97B4F1852F909350794FDE95DD4B73E015442CB2706517E893693490920A82
SHA-512:	FBBB83FE9010D3BE0352316636651C6ADA5478888802340E0F863CEFF63C4A5F31077C9714CC5296E0864BA5CF81048F6104BDB30DB82178E66F5D431FE2ABD7
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:43.690 1b90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/02/25-21:40:43.691 1b90 Recovering log #3.2021/02/25-21:40:43.691 1b90 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\1.0.0.6_0_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):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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
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\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.333437635718907
Encrypted:	false
SSDEEP:	96:tBC9luNLSuDPfGwt8fUT+JK72luNLSukg:7+u9zs++QEu9l
MD5:	51F08A4852E5B5A6CBF3BB88907A403A
SHA1:	BD4F524E4FA7C4B580D72A65A6619CCC9D28A4FF
SHA-256:	967A9AD6C510F10590062DD708CC6BCADD60FFF3FB58F20B68072E7360E4C516
SHA-512:	F1E3B1D9FC57AFDA6D9F3A2D8650DF48A315EB0E5B7C7DB9F8587107E8CFECC541E212F969EC90CC9295498BDEA5800CB01DDE49D7C62337CCF5E4B127EEC FC3
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.8130998352837986
Encrypted:	false
SSDEEP:	24:/yJMJqRglEgRyQJDx+WyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6UwT3n:/mQOgEcyEF+WCBmw6fUI3n
MD5:	5FED56EA3B4A40C3664B8E3C4317938D
SHA1:	70BBA6E44EBE8DB7C23C9443626F412DE0F49E2A
SHA-256:	7C9E6C4E4FA1DC42681E2B555C90A3918D52D6614A0FDB46A6609E7D06509B75

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
SHA-512:	9F3925511E61DC11E2961F7E0BD4545FF3C1B7C75D90EA8A954AD502F91BFD3C9B248D15E8DC475C38B8FA0E80CB3C05E18EC2A22F451C57795E2B7F7F4E4B 0
Malicious:	false
Reputation:	low
Preview:	.....).....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.174604855838062
Encrypted:	false
SSDEEP:	6:mN2eS+q2Pwkn23iKKdK25+Xqx8chI+IFUtpe2e4ZmwPe2eIVkwOwkn23iKKdK25N:ejvYf5KkTXfchI3FUtpO4/POg5Jf5KkI
MD5:	5ED88AE4EC9586E3DCC39E3695649A12
SHA1:	CFBFAE93C31175F2E699D0D00B7F3596B9B1C9EE
SHA-256:	3465B7BD250130783853597E219B23C477E06718C459A3FBEB0AE40D649E7CA5
SHA-512:	2E796EC43A1C3B69586C255BD96506C5294A01F03E823B858B97922F3C6F877A8BE1D5FEC39D3C9EAB4DB20E6FB0029F0AB4233EFA2969C9DD5B5B820EB3E5 1
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:50.101 1a18 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/02/25-21:40:50.103 1a18 Recovering log #3.2021/02/25-21:40:50.103 1a18 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.12830842408414
Encrypted:	false
SSDEEP:	6:mN2ehP+q2Pwkn23iKKdK25+XuoIFUtpe2ehVUZmwPe2ehV0VkwOwkn23iKKdK25y:ehWvYf5KkTXYFUtpOhVU/POhVU5Jf5Ky
MD5:	AEAF8A0375641BEFDCAE12D3AFB938D9
SHA1:	8AD3898D99F896EE0A5B19F222231A8F571B2D16
SHA-256:	4F864B6A562E29469CF054BC674DFEB2A5B9EF463C561794178CEB1A6A3FB74A
SHA-512:	2F7C6E1F6F0C3D64FF61D221D79ECC70A835839EDC8F9213DEB65821D3C06CEF61E5D5DA0360327F8E60353938DC8D9422A81B6429B53A6C84C1DE48B0C7A5 B
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:50.081 1a18 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST- 000001.2021/02/25-21:40:50.082 1a18 Recovering log #3.2021/02/25-21:40:50.082 1a18 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data \Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.248225537123425
Encrypted:	false
SSDEEP:	6:mN2Dq2Pwkn23iKKdKWT5g1IdqIFUtpe2wZmwPe24kkwOwkn23iKKdKWT5g1I3ULJ:DvYf5Kkg5gSRFUtpg/PH5Jf5Kkg5gS3e
MD5:	6682C5EA3F0D7E8B482380C37CE7E0C9
SHA1:	3B1A8C3244DA2D128EFE237B95E79C1DDBCFAE52
SHA-256:	2F9038E30DF9690A66B6DAC55BFBC22D051A4F25C6A64DD26149942A90B9C559
SHA-512:	5A6FC4F55D368FE10F15A84E5D17B80E94ABF2182FD4AA9D9CBEE90E4EB66AE0A336B9D5F8B3BB8875A17C9633A37D281005DF8C9F77307F77623EF0EFF48F0 1
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:49.730 1b14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/02 /25-21:40:49.736 1b14 Recovering log #3.2021/02/25-21:40:49.740 1b14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\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):	32768
Entropy (8bit):	0.4718337047392092
Encrypted:	false
SSDEEP:	24:TLxVyuUGnHMcJOlwSDCVyU5gBM9FaR7OT2eOADUynHMcJOlwSDCVyU5gBM9FaR79:Tz5FluNLU+BMu02NADBluNLU+BMu9
MD5:	B259ED73A1BA6C841B48F9C0D2076721
SHA1:	C0F33C2C405DC6450B360253E8ADDCDA13067287
SHA-256:	D5BC554629C4D24A29987DE221FE5E1AA37297AE7A1B8CD3EE733FC8D9FC286A
SHA-512:	2DC92D6397FFE5538BE29307FFBCC21CAB360E1FB9AF08CE9E5D859621A589250557D4ED5B6F22787DF4DD6966D739193B5A78A174261FA4C2DE1D79B298F08
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):	2789
Entropy (8bit):	6.201576140414634
Encrypted:	false
SSDEEP:	48:jhK//PHAT9WQp8MwZ//PHqhOxbj+68qMPVQeLEf6nU8JFZM5GluNLU+BMuYwfe:u/Phh/PKhMbSfPWeVU8rZLluNLSuW
MD5:	0C9EF65F5172C05FD957F8BDCB5CBB03
SHA1:	4B71A7317A37C265BB31B7E1CBCF9321960CE523
SHA-256:	9DB06A5C8617911AD6B46CF4E7204B87E4B0E2EF68D7AA6FD04D502E3BDA4561
SHA-512:	85EABA9B40E48748B404659A4E248F76CC0591504E55D5C3ADF80F6613E0AF2FB2D3EC73C9DE413CE247DA248D36732566EBFD32A1D275E6FAAF68EE53528D8 7
Malicious:	false
Reputation:	low
Preview:	....."...$.02b3igkzihlwgkqvku4mghq9zyrbuf7v0zsm4cdyw3168zse6..2b5hwtu2txytpvimszaqwqnbg..2b7s..2bbpbbxlppfhusk7..2bhec..2bkb9..2bsgmdkv..2bufof y4..2byo9fqgw8g6ikdphuesqm.Y2foboxxa9roxlkakqvtvnjy9nxtxjd6tnzcebsqgigytmzye255uswq6f3sq0k3qcczrkmigtwjjpigztpn38pyzm./2frgvmbptopwiclue2ujbujzks9qbrm xjc8wcvkuuy8jmc7..2fs..2fxwixj3q3hneww..2fz9dw3t6..3d..3d7..6s..click..ct.,dwb70hpljur35gftsieshjrrx5io6qepxbkrepqrynrx..flaa9uev..https..in..ls..net..sccollege..sendgrid ..sign..u16095581..upn..app..deanna..edu..kirchen..qgohifmzuv..web*...$.4.02b3igkzihlwgkqvku4mghq9zyrbuf7v0zsm4cdyw3168zse6.....2b5hwtu2txytpvimszaqwqnbg..... 2b7s.....2bbpbbxlppfhusk7.....2bhec.....2bkb9.....2bsgmdkv.....2bufofy4.....2byo9fqgw8g6ikdphuesqm...].Y2foboxxa9roxlkakqvtvnjy9nxtxjd6tnzcebsqgigytmzye25 5uswq6f3sq0k3qcczrkmigtwjjpigztpn38pyzm...3./2frgvmbptopwiclue2ujbujzks9qbrmxjc8wcvkuuy8jmc7.....2fs.....2fxwixj3q3hneww.....2fz9dw3t6.....3d.....3d7.....6s.....ap p.....click.....ct.....deanna...0.,d

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):	42076
Entropy (8bit):	0.11646353615906797

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Encrypted:	false
SSDEEP:	12:fRlS1pqLBj/8t3lA4nMWQASjG9LpBQZ8fOD:plSfqLBY3bf1NpTfO
MD5:	DB50475CCFB8E4C212CF64C4D0314750
SHA1:	376CF31CBC4D838D490DBF20D2A338FBDB8F23AA
SHA-256:	7FCCB586EE37F502211FA9D2B3951EA6F5B32C74F4917F1BB720F4F08F4A4903
SHA-512:	26F00BF37056E2A9E7DB4E43CFA1B51FA2B1603496817FC0961C96C6CEF2851E0F24FA19C8EE62A6AF1384FB065ED0B6C3EB38928AE887FE4C9CB3FB64F64C0 9
Malicious:	false
Reputation:	low
Preview:	.....LO.c..... ....

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):	2955
Entropy (8bit):	5.454038856923952
Encrypted:	false
SSDEEP:	48:AmZHGIWjMa7fMO8db1M5pV5VZbQSefgGOGNrS0U9RdiN9r3WN:Amyga7fMldbgPfZbQ5fgGOarS08N
MD5:	DE58C4701135D023B0C6A39AE8B26D0F
SHA1:	D566765034CD1AA43CA7D725030CCB79A128B1FC
SHA-256:	2AAAB42ACEE323DED28E41134C0C91CD4B7333B502BB579D7F050FF72109FC4A
SHA-512:	0EE54CF796D592D399EF787304C21C5502C5B419FEE26F7DF5EECEE51D0BD01388147A1C4DA25B9A773964E989D0E7B47D018DBCFF6D97F5B21B1D0950D0AE B
Malicious:	false
Reputation:	low
Preview:	T.:....*.....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..109136000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-02-25 21:40:51.24][INFO][mr.Init] MR instance ID: 5228f74e-c6d2-43dd-952a-223ec512bb70\n","[2021-02-25 21:40:51.24][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-02-25 21:40:51.24][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-02-25 21:40:51.25][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-02-25 21:40:51.25][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-02-25 21:40:51.25][INFO][mr.CastProvider] Query enabled: true\n","[2021-02-25 21:40:51.26][INFO][mr.CloudProvider]

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):	5.185103638291748
Encrypted:	false
SSDEEP:	6:mN2wFfq2Pwkn23iKKdK8a2jMGIFUtpe2oTZmwPe2PPkwOwkn23iKKdK8a2jMmLJ:AvYf5Kk8EFUtp4T/PH5Jf5Kk8bJ
MD5:	8441D96921FE72638199FE0174DB20CE
SHA1:	A87CBC61ACE9D0DF0F728C6EBF6B958CB5E94421
SHA-256:	AE0BA6CBEC839071569DFA07DC44E284E2E5815B03FB55954A7DB892A7A3FC59
SHA-512:	F60631B6C136B534E82A843DF431AF928DABB50202B26EB428A411CE4BBF0DA0CBBB3D495212096B94BA57B0BF001C2BCA7DEC2F474AE5586039AD83572A4E BC
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:41.389 1b84 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/02/25-21:40:41.391 1b84 Recovering log #3.2021/02/25-21:40:41.392 1b84 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2448329057209975
Encrypted:	false
SSDEEP:	6:mN2vL+q2Pwkn23iKKdKgXz4rRIFUtpe28MTzKWZmwPe287LVkwOwkn23iKKdKgXS:j+vYf5KkgXiuFUtptKW/PcV5Jf5KkgXS
MD5:	A0AE91FB4FF3CB05B0F22F6E4DB3B334
SHA1:	D9C286A3CD7E2469579361104E713FFCA00E1262

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
SHA-256:	7156A2F7F7850AF01C7A1BAF31888DBE3D9106D5514CFE0909E37088C357F6A0
SHA-512:	6F7DF3B8D8ED8EED98A337D819F13AEB8288C02DFE902295D57E944AE7F1EC9ACBBC3EB97E88CFDA9710FCD27E256FDCB5D52E39C678CD9D45FCEACEB62E89CC
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:41.679 1b3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/02/25-21:40:41.680 1b3c Recovering log #3.2021/02/25-21:40:41.681 1b3c 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\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

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):	320
Entropy (8bit):	5.15055676412762
Encrypted:	false
SSDEEP:	6:mN20zL+q2Pwkn23iKKdKrQMxIFUtpe2wzzKWZmwPe2wzlLVkwOwkn23iKKdKrQMT:s+vYf5KkCFUtpAPKW/PARV5Jf5KktJ
MD5:	609813F8DCE01FA87E00B0E685B9CBB3
SHA1:	74E25BB00066F079D8AA4E53683E66978422CE49
SHA-256:	EA020CAD48A425040993DA73415069C1D83144CFC9374ABE6BBE7A07D11F886C
SHA-512:	7CBEF15EF249E5CEB1AD6BF02C92783A3798D21C2001993816BDD7AD530C9AB6A92985667162F1E3EE40909DEE68B9674CBC8C17CD1E175CE46BB2AA7966AECB
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:41.609 1b3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/02/25-21:40:41.610 1b3c Recovering log #3.2021/02/25-21:40:41.610 1b3c 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):	5.1304234914563365
Encrypted:	false
SSDEEP:	6:mN2Yuaq2Pwkn23iKKdK7Uh2ghZIFUtpe2CTXZmwPe2CTFkwOwkn23iKKdK7Uh2gd:JavYf5KklhHh2FUtpoX/PoF5Jf5Kkl9
MD5:	48A05ABF293F1ED4244EFA3D78C6F7D9
SHA1:	029366531559757FCAF243DD7F68E5D4F5CC2C8E
SHA-256:	2AD8014E7B607694E8A188B0E0268E3CB449A926DBA6767507C06486EF43C82D
SHA-512:	640977B0877034B2D4A0A61D810A69514B6830DB9E900291CD1EF604462DB11415D1C1C9FC09A830C6176497CD8FBC3D0B74BD960FB7EB3DAF061A6EC5EF859
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:41.345 1b40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/02/25-21:40:41.346 1b40 Recovering log #3.2021/02/25-21:40:41.346 1b40 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
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):	430
Entropy (8bit):	5.25699261034456
Encrypted:	false
SSDEEP:	12:PN+vYf5KkFFUtpeB1KW/PeB3V5Jf5KkOJ:SYf5Kkfg6oXJf5KkK
MD5:	753FBF4EA4F48E5C9F7B2D1207F10254
SHA1:	743863911C09E90447D0158131EE7962EE55DBCC
SHA-256:	55208604B741D6D9FC224EFE41FF661CD029B35B4B103D9037AB667FF1C3EA06
SHA-512:	5923DE478FDB47F003EFE7612B4B2A6C9C29C282C9E06AE65E41F9B5F12C43498DADD67C798B85DC5C4C53C3CC4A4EBBD6EFCA908C787E18B203BD456F3F57C
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:41.637 1b3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/02/25-21:40:41.638 1b3c Recovering log #3.2021/02/25-21:40:41.638 1b3c Reusing old log C:\Users\user\AppData\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):	432
Entropy (8bit):	5.249741997287712
Encrypted:	false
SSDEEP:	6:mN28GAq2Pwkn23iKKdKusNpqz4rRIFUtpe28pZmwPe28BcFkwOwkn23iKKdKusN9:EvYf5KkmiFUtpW/PocF5Jf5Kkm2J
MD5:	A563618A5D7C239A7757CDCEAFC5D27D
SHA1:	D0EDFEBAE8D51CEBD4BF09081BC9EBC6DB5083B0
SHA-256:	2F9F263A8CAA37C15A82BFC64FCE3357A9875195C969DE9445343C0FBEAD9C61
SHA-512:	22BF964516CA1D6FF3F126DF2263CFBDC569712F877358172837FE91ECD080223E1EFA2B1E943303F23D755A44F8666760565CC19DDD219D816019FF4D05F910
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:41.681 1ba0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/02/25-21:40:41.684 1ba0 Recovering log #3.2021/02/25-21:40:41.685 1ba0 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
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):	5.285281704927617
Encrypted:	false
SSDEEP:	6:mN2e+q2Pwkn23iKKdKusNpZQMxIFUtpe2JXZmwPe2J3VkwOwkn23iKKdKusNpZQq:PvYf5KkMFUtpZX/PZF5Jf5KkTJ
MD5:	9B5AF7B666A7C11719CD075819BB79BF
SHA1:	FA0C67C03351F8DBE8E9B4A29AF0A25280668377
SHA-256:	D8FA7D5884BA3C466B369125F5A3CFBA89F9B2EB8C01E22CB16D299C4EAA3098
SHA-512:	16EA7630F679B96D71AB9B426BE3BCA04B3A721464D71FD72C0D2FEEC6D538CA6FFCDB538715A7F16F50D5DF15D744E659C168DD7131D4B79B58510B2A0FA18
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:57.838 1b78 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/02/25-21:40:57.839 1b78 Recovering log #3.2021/02/25-21:40:57.839 1b78 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\a216b292-35e3-4a8a-8ccc-1298dac27205.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):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","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\813890ff-223e-45e6-91fa-77fcb9e4b480.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):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
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\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.197635770801549
Encrypted:	false
SSDEEP:	12:A+vYf5KkkGHArBFUtpoKW/PmuV5Jf5KkkGHAryJ:JYf5KkkGgPgIIJf5KkkGga
MD5:	3235C8628C7D27F343EDF1B549E1174F
SHA1:	8235788806EA293F2AFCA1F790377ECD14614E7C
SHA-256:	2C6826FA286711F7DCC10AEF341D33919D5E37AB573C344093F690F1444A2ACA
SHA-512:	F8A70843206F28DFACD53345BA0DD7A918CEAF2A707D41A0B1EA4501CBD2BEEADD3EC053C8F19CDD93B27938509B8938CE2E892BC7F7C7567A31ADFF7F2B7F81
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:49.120 1b3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/02/25-21:40:49.333 1b3c Recovering log #3.2021/02/25-21:40:49.336 1b3c 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):	5.272635488379321
Encrypted:	false
SSDEEP:	12:OvYf5KkkGHArqiuFUtpz/Pf5Jf5KkkGHArq2J:MYf5KkkGgCgLJf5KkkGg7
MD5:	8BEEE1619F0214C43F6A16E1B2D171D8
SHA1:	985DE03197BD3C1FBAA00C6B244C52FD4EA06140
SHA-256:	AEA643CB10560AAD41012045B40F9825608C75AC8ED48C68983F2C6D0CDC6EBF
SHA-512:	002469E3F0F54012912203AA7B409886B81D0F2305A214AF6D9C417194F485044366E265D31CBB85CEBB770CDD32F1B122DD07406F08950CFE97042F4BDB3780
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:49.340 1b78 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/02/25-21:40:49.344 1b78 Recovering log #3.2021/02/25-21:40:49.346 1b78 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
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
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.202112235673865
Encrypted:	false
SSDEEP:	12:gSVvYf5KkkGHArAFUtpf6g/Pf6I5Jf5KkkGHArfJ:gMYf5KkkGgkgRJf5KkkGgV
MD5:	05F1B8399CF2C516D72CCCBCFFF45D6E
SHA1:	0BBD5472A7297EC710AB1F8EDCBB3F09D757CD97
SHA-256:	3C7A9FACB425C8290149F01B1D5065F710F92B45F594CE163CACE54732E687D2
SHA-512:	729F5938C6213A9AC54773E66221E126C8C85BDC8BFCBCCA9F16177D44D21AC447FBB9FB0E1E75BD329FD144EA380B95EE921DF6424B64E0D16535ABCF8065E
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:41:04.582 1b88 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/02/25-21:41:04.583 1b88 Recovering log #3.2021/02/25-21:41:04.583 1b88 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):	5.214117857741695
Encrypted:	false
SSDEEP:	6:mN2zeRAq2Pwkn23iKKdKpIFUtpe24FUHzZmwPe26F2kwOwkn23iKKdKa/WLJ:zeRAvYf5KkmFUtpZHz/PKF25Jf5KkaUJ
MD5:	42C5B9296450499F139279372A9A84F7
SHA1:	41BC5C3DA01589C02C949CEC80CA565B6DC30F3C
SHA-256:	36A312085AA67B53681579E88C67A0F6A14713B0648EB4DA99464011551522CC
SHA-512:	CB383A9DF4FC00E357316DB07DD160EA99D7B2CA685EA70CB027797C70C2292D96A99E554205F20A9FF31650167DDCD3939F44A4B58B9C4A851F5D2417454AF
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:41.375 1b40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/02/25-21:40:41.381 1b40 Recovering log #3.2021/02/25-21:40:41.383 1b40 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.29691909346304

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Encrypted:	false
SSDEEP:	12:5vYf5KkkOrsFUtpXvP/PXE5Jf5KkkOrzJ:FYf5Kk+gt3uJf5Kkn
MD5:	43E3003DDDEEED739CEE0958458505F9
SHA1:	B9A739A2261302529C0472E47FD00404D02D7DA8
SHA-256:	D19F4BC0B75BC2A8176939FE8E7D577DF0472652E4423DF4316FD34F802D8405
SHA-512:	B1ED093280EBF24FFB2CE9AE8873B639E54F5C36955F153FA4889C2FA099A666CE6232B5E94A2812B96F452B04A3292ECE1DAB7690241E5214956C4460D64E79
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:51.258 1b78 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmb meomcjbeemfm/MANIFEST-000001.2021/02/25-21:40:51.260 1b78 Recovering log #3.2021/02/25-21:40:51.261 1b78 Reusing old log C:\Users\user\AppData\Local\G oogle\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	3.599483981787689
Encrypted:	false
SSDEEP:	3:SLNBp:oBp
MD5:	C3551E701A4FB470C2AA25AC52BF143D
SHA1:	1F68151F9CA1AF227759F14E4BEFD7AEFD7B5FFB
SHA-256:	149C7D859A85D786BB1CF35EB047E8525BCE10C4B4878BD718013F571A22D3C3
SHA-512:	23D68BB7FC1A227C0303405D7E6201DA6A1CCE9523ABB6400C0FA42FA08AF76B68CE08692889EE31BF9864A2FF3042A627393247B5B32415E261803A2180A23D
Malicious:	false
Reputation:	low
Preview:	....vP...j:v......Q.8$..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ab51f823-ac2b-46a9-9a18-88485413c168.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):	5695
Entropy (8bit):	5.183391493522796
Encrypted:	false
SSDEEP:	96:ncM94cNurWaIVzX5k0JCKL8xlkk1ijbOTlVuHn:nc44cYIdh4K4lkkQN
MD5:	A31C113545E4308520B6A8AA31D6908C
SHA1:	3287FC8CCF446508F733A08348653886EF319BAE
SHA-256:	0F47BE235C2BC8FB201995DBDA95EDE4F4C8E620406BA92BE6E413F7838155DA
SHA-512:	5E754A7B394D261953E6F933CEBE0EE3C7D7FAD52C7BB84E7BE7FD6CDE461C53C8442F74395A2153656564D1A677FE3F75CB6B8064461357DA038EE49E82FC5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258759241650376","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_al l_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left ":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"d ata_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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bd2236e6-47c7-44e8-aaeb-f63b91b37cc9.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):	5669
Entropy (8bit):	5.181512421637315
Encrypted:	false
SSDEEP:	96:ncf94cNurWaIVzX5k0JCKL8xlkk1ixbOTlVuHn:nc14cYIdh4K4lkkQn
MD5:	A4307BA64BBABFE0CC0AFEAF8D64842B
SHA1:	6B30E4D14FC505BC46CD73098868C883F8B94A56
SHA-256:	A09C8F7815826B821622498CF6152F336A3BCB5EFF33DA6E31C9591918F94B2D
SHA-512:	3D63C6A516D59C8A1AA2FF5AFCEC250BEA43B2F51624CF521785985554C9E8FC63A678F0466F69F2CF2D718FE0D134977119C6458C80004593F95CF9F2BAA0E8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bd2236e6-47c7-44e8-aaeb-f63b91b37cc9.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258759241650376","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c7fa8ddf-888d-4dc8-a8fd-22c29d6c5204.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):	22620
Entropy (8bit):	5.53580011473154
Encrypted:	false
SSDEEP:	384:urWtCLlO5XV1kXqKf/pUZNCgVLH2HfDJrUNHGWnZaAcw46:SLlSV1kXqKf/pUZNCgVLH2HfdrUxGWn1
MD5:	7A154EAEB4E53C25A9173CC0130CD29B
SHA1:	9EC7DCF5FF24713DE7C12D36448FC496107E67DB
SHA-256:	D8B1F5AF3B520D674F04DF2166FA79EA812CD79AC2180006C710D0353BC140B4
SHA-512:	19371475DB9E50127C588AB99B695C2A54DAB013414D0BF4A6BAD82E7D8D39F31BD0CF60DEF4AA4BF533F9CDBBCB3F2DEDA1866AE166D7D691ADD6BD73BDA6F6
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":"13258759241362339","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.382469457561085
Encrypted:	false
SSDEEP:	3:tUKot2R1PcuHNyZmwv3at2R1Ph/kSV8sat2R1Ph/kSWGv:mN2WuEZmwPe2YSVve2YStv
MD5:	ECED818CC57B9FA7984D63DD42A1F249
SHA1:	414FA6B4AE9BFC614A237BE2C7C0C65C9DE8DEDE
SHA-256:	F075FC10BDBA41CE7C10A7FF0284C7BF1584E33C3A19396BA1F695F86E952452
SHA-512:	147B2FEFE7DC385ADCC1BD2952C51E04128A936474F456A7BE58C0AF3ABC7746558803B3E00727346562539129DE93252C548146630C0B71B6A9F16D9CEFC944
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:48.001 1b14 Recovering log #3.2021/02/25-21:40:48.084 1b14 Delete type=0 #3.2021/02/25-21:40:48.084 1b14 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f176bfa6-17a1-40b2-9808-d25a7d3d26b7.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):	22618
Entropy (8bit):	5.535911834444205
Encrypted:	false
SSDEEP:	384:urWtvLlO5XV1kXqKf/pUZNCgVLH2HfDJrUNHGZnZDncw4tk:fLlSV1kXqKf/pUZNCgVLH2HfdrUxGZnV
MD5:	D286B98A59F80E2895CEC0DCD7D4E286
SHA1:	B9C83C8A0503D0033EEEBC3A5E254D000012B645
SHA-256:	5F0C5F0C6B0FDC98506C5557D61E7AE2370F517ED28998F82559FA4A4ACD96A2
SHA-512:	B8715560249C79AF54BCF32F58D4C9D432CA12CE88D274BBC38C3BDD1F4B88EE1E02473B5C0A7EB984A649975435433CE231D93E94CB9CB1AC281F98133ED4F
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":"13258759241362339","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.2147625898719205
Encrypted:	false
SSDEEP:	6:mN2enQaddSQ+q2Pwkn23iKKdKfrzAdIFUtpe2enQbQgZmwPe2enQ/QVkwOwkn23m:eNddSVvYf5Kk9FUtpO6Qg/POaI5Jf5KF
MD5:	F7305EA322DFE754EBB9425BA49F60DC
SHA1:	2FB4BD020DE458D4E0BFC8CE5AF4AAF6ED53B355
SHA-256:	E18D56F7C3644A33C6371F31C9352946F84FEC5FAD3B1B4A894B8DDC3324DAE3
SHA-512:	56A988E407CFAB1077319CDB280E891BFA59F48E0FC51BEAE412BA70CF919E7F80CDD52D16B3ABD9F8CC480A1434BB3CD5F27AEB56E6BBCB0CA8CE9D6662C03C
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:40:50.654 1b88 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/02/25-21:40:50.655 1b88 Recovering log #3.2021/02/25-21:40:50.656 1b88 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\a5098b39-921b-4d83-ba3a-52e687953ddb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.746336758954295
Encrypted:	false
SSDEEP:	384:f6wyth/Q6HXwR8NhrqvF/3GJfmHnCGSVrAjtJxeDrbKrolmgbgfBtZ6OnntNE1Js:ynSFFizOasenRv383rW/KFjBhT
MD5:	F10A35ABBFCC93B94B6A9B7CA5CB9B51
SHA1:	1531DCCE9D83A5E7D01A6DDDACFE094BC79ADE1B
SHA-256:	22DDFD3E5D0C89B5869D7A52A4AD784D11F24712FA9BB8A73FF6FD62844A7B37
SHA-512:	CE0BB81384C908EFE52A6F4F3EFD57895DA90A277A5E9F6AD3FE68BEE246B56EB5CADEF83DF77D5CFCB450659B916862DEE1AF015B5F2A6A830E8C1A34C402F
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....28.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\acb745c5-9475-46b2-aced-b807c8514b68.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.747010542299055
Encrypted:	false
SSDEEP:	384:J6wyth/Q6bAX3VcCR8NhrqvF/3GJfmHnCGSVrAjtJxeDrbKrolmgbgfBtZ6Onntq:sySSFFizOasenRv383rW/KFjBhI
MD5:	2671017EA08B19844D40088036660A11
SHA1:	3E51407511D3FF1A4B339B061EC5B8B704270826
SHA-256:	48748D7D6078994E6EDF8768236568C6B0B8C48D4BAE9ACB52AD707DFC35C2CE
SHA-512:	CD6A9FF8606C5225E50CD4862C5FCB7436E2077B1FD0A0634CDD50AF9F9C028826C8D7C89195CD1F48EA278C0AF1053799849E734FAA6033D6269DC49BDED8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\acb745c5-9475-46b2-aced-b807c8514b68.tmp	
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....28.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\b4e83329-d3b9-4db0-8cca-568978d4fd5d.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):	165085
Entropy (8bit):	6.082020046311642
Encrypted:	false
SSDEEP:	3072:MHEsmGflW7LtsevCLxZJasImhjp3qm4JaPlrnJFcbXafIB0u1GOJmA3iuR0:gDflkhsXNZswa2bHaqfIlUOoSiuR0
MD5:	E04C751C0B18F08983664871AE9FF1C8
SHA1:	77E5EBE3CA374A5B6BD1D3AE895B22F628640D34
SHA-256:	76DA49D31C13D02DE56D47290428BFC5AC8C6256D5AB8EDD2E7DF820B1F58497
SHA-512:	B18118061C9454A59110B2995454FE10912DFCAA478871268BE275BB08CA5DD1761D81D90FEC172EFC75452B66731D01447363628AB632ADA6E07A70D199404E
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.61428564436891e+12,"network":1.614285647e+12,"ticks":302779923.0,"uncertainty":4548758.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\e7d9936c-39eb-46b5-987e-033bfb909415.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):	165085
Entropy (8bit):	6.082020046311642
Encrypted:	false
SSDEEP:	3072:MHEsmGflW7LtsevCLxZJasImhjp3qm4JaPlrnJFcbXafIB0u1GOJmA3iuR0:gDflkhsXNZswa2bHaqfIlUOoSiuR0
MD5:	E04C751C0B18F08983664871AE9FF1C8
SHA1:	77E5EBE3CA374A5B6BD1D3AE895B22F628640D34
SHA-256:	76DA49D31C13D02DE56D47290428BFC5AC8C6256D5AB8EDD2E7DF820B1F58497
SHA-512:	B18118061C9454A59110B2995454FE10912DFCAA478871268BE275BB08CA5DD1761D81D90FEC172EFC75452B66731D01447363628AB632ADA6E07A70D199404E
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.61428564436891e+12,"network":1.614285647e+12,"ticks":302779923.0,"uncertainty":4548758.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Temp\3cc13d65-885f-4f53-893f-07ce5223ad05.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\4526033d-5007-412a-b7cd-0225003d0ef0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..I.6r[yU...%..f.....N..V.....<+.....I..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\6816_1641461432\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9570514164363635
Encrypted:	false
SSDEEP:	3:SVCBGERJd9WaHpYx4eiXoA:SVCwERJdVMiXd
MD5:	C6ABF42CB5AF869629971C2E42A87FD5
SHA1:	6EB0FAE28D9466E76FA12E31FE6CDADD3ACCE4D1
SHA-256:	D281AFDA759075F4CB7D7CEEC4A3CB2AF135213B4D691F27090E13F238486AD1
SHA-512:	EDDF7E4883E82718743C589E8F2E48BEAD948428E730231FEFADAD380853343332BC56C9DC61C963B3F537CD4865B06FF330CEF012B152CEA35F8A0AA2C7B56D
Malicious:	false
Reputation:	low
Preview:	1.fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace

C:\Users\user\AppData\Local\Temp\6816_1877668474\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9669759926795995
Encrypted:	false
SSDEEP:	3:SfvHUTa8URTTH/BXDj6:SXD3TfB36
MD5:	E3EDA33A5C956F4FC9C5BBD91FF10252
SHA1:	182B989E299A3EC306622A9DD45C3B74A4DF6077
SHA-256:	6D7A462B703F1617286B65BFE0116F267328BEFC379812BCE774D8C640289647
SHA-512:	A49FF4979FEC3512C44899840CCF8D112806330C93812C515F09953B9B6DBA6B1DAB1828382D634235CF23E093C983AEFA860B7A75FDCB5F3F98DD928D4F47D
Malicious:	false
Reputation:	low
Preview:	1.d730fdd6875bfda19ae43c639e89fe6c24e48b53ec4f466b1d7de2001f97e03c

C:\Users\user\AppData\Local\Temp\6816_683499445\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.951770877866716
Encrypted:	false
SSDEEP:	3:SdpDtmKQzaU5KEM8aMxUDT:S1U5eKUP
MD5:	B32EF2DA53B87C2C9013454F36072740
SHA1:	794DD70931C56A4644AF3CCEA6006F11E3CBEA30
SHA-256:	50CB95C1DC2E053A5CED7C612BECAC65B93FC4129BD070EB1FBABFB5B6558E48

C:\Users\user\AppData\Local\Temp\6816_683499445\manifest.fingerprint	
SHA-512:	46F145130978814BC0EE8E91BFB27634BE36DCE49AC414105731A79D7F47F06459C40F799A63B18882AD7F3DB3E369F483927DEAB68E2BBEB16E73423005AE7B
Malicious:	false
Reputation:	low
Preview:	1.805afe719fae8dbc158c2eb6cffa75123f3a32356d7c745aee5d978d907921f6

C:\Users\user\AppData\Local\Temp\ca69d301-407f-4c62-9494-e07c629d7208.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\eab219ef-4551-40ac-a34f-03f4acc5c73f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\ar\messages.json	
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0IprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:IPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ... .".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\ca\messages.json	
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE 1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "1522140683318860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\de\messages.json	
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0blt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71E EEE

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\es\messages.json	
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas describe mejor tu red?".. },.. "12827687646031907 5": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB1120272356
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "1522140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "1282768764603190 75": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A526195205021
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\fi\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "152214068331886 0351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "180276746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C00 0
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "128276876460319075": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-s mooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smoot h".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51 B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Se fige".. },.. "1213957982723875920": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "1428448869078126731": {.. "message": "Fluidit. de la vid.o".. },.. "1522140683318860351": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "1550904064710828958": {.. "message": "Fluide".. },.. "163 6686747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\gu\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876 460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "128276 876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15507
Entropy (8bit):	5.290847699527565
Encrypted:	false
SSDEEP:	192:Pdapr6h85tRwVQgkvJryLkla5Kfndg/V6c8TEKdl:Arwot2Q7BryVce/V6uml
MD5:	3ED90E66789927D80B42346BB431431E
SHA1:	2B061E3271DF4255B1FFC47BDB207CDEC0D9724F
SHA-256:	0B41E3C42414F72C9A12C05F8772597F9685115366A774C66018467AD4B71A74
SHA-512:	92BE43F1FFC8EFBF5BBC50573AC4C65F6104416A5B6CD04404C3A9854CA3DCF2A43A4044C168590CDF83887D234495843572331ADCD5B020D2E48A3956F3C16
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Zamrzavanje".. },.. "1213957982723875920": {.. "message": "Koje od sljede.eg najbolje opisuje va.u mre.u?".. },.. "128276876460319075": {.. "message": "Otkrivanje ure.aja".. },.. "1428448869078126731": {.. "message": "Ujedna.enost videoreprodukcije".. },.. "1 522140683318860351": {.. "message": "Povezivanje nije uspjelo. Poku.ajte ponovo.".. },.. "1550904064710828958": {.. "message": "Glatko".. },.. "16366867 47687494376": {.. "message": "Savr.ena".. },.. "1802762746589457177": {.. "message": "Glasno.a".. },.. "1850397500312020388": {.. "message": "Vidite li svoj Chromecast u $START_LINK$aplikaciji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "co ntent": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15682
Entropy (8bit):	5.354505633120392
Encrypted:	false
SSDEEP:	192:CCEAproS9fZv+JwkDMrC2NSxoSgbV6c8TEKdl:5r5VZv+RDMrazoV6uml
MD5:	8E9FF7E49473C5734A2F6F0812E12EB3
SHA1:	A4F10DDD1580582533D5EB59EDF6D8048F887C81
SHA-256:	6CDD2FB39ADECE00E88B989E464B05ED1414092D0492F6D0AE58D549BFD1A46A
SHA-512:	E9A4AF31B1A276F395599BB620A3164CABF3459F3C102DD3F57DFEA734510BD985DE65CB409E1975559ACCC615075439A08E1DEBE22C90A0ABCAA3CAFEE79A C7
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Lefagy".. },.. "1213957982723875920": {.. "message": "Az al.bbiak k.z.l melyik jellemzi legjobban h.l.zat.t?".. },.. "128276876460319075": {.. "message": "Eszk.zfelfedez.s".. },.. "1428448869078126731": {.. "message": "Vide. folyamatoss.ga".. },.. "1522140683318860351" : {.. "message": "Sikertelen kapcsol.d.s. K.rj.k, pr.b.lja .jra.".. },.. "1550904064710828958": {.. "message": "Folyamatos".. },.. "1636686747687494376": {.. "message": "T.k.letes".. },.. "1802762746589457177": {.. "message": "Hanger.".. },.. "1850397500312020388": {.. "message": "L.tja a Chromecastot a $STA RT_LINK$Google Home alkalmaz.sbanEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

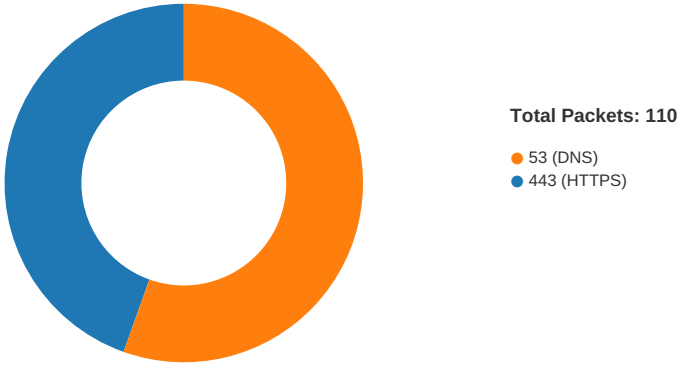
C:\Users\user\AppData\Local\Temp\scoped_dir6816_811571267\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15070
Entropy (8bit):	5.190057470347349
Encrypted:	false
SSDEEP:	192:GsprMtChjkWfrEWL0KRCnEOWV6c8TEKdl:9rtAEr3LTRuWV6uml
MD5:	7ADF9F2048944821F93879336EB61A78
SHA1:	C3DA74FB544684D5B250767BB0CB66FFB7C58963
SHA-256:	3630947E1075E3663AD3E4824D0BE42CB47C0D615D8053E83B9595047C8BA9BE
SHA-512:	1F28BB80E1839C5581106BEA3AE2501C7618249D7E3115819F5A9A87771D59F5DE346C1B9C87F7FFC390604D5B9888CE738E25F2F04A094002A0FB3B22CBEC95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Membeku".. },.. "1213957982723875920": {.. "message": "Dari berikut ini, manakah yang paling mendeskripsikan jaringan Anda?".. },.. "128276876460319075": {.. "message": "Penemuan Perangkat".. },.. "1428448869078126731": {.. "message": "Kelancaran Video".. },.. "1522140683318860351": {.. "message": "Sambungan gagal. Coba lagi.".. },.. "1550904064710828958": {.. "message": "Lancar".. },.. "1636686747687494376" : {.. "message": "Sempurna".. },.. "18027627465894571777": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Bisakah Anda melihat Chromecast di $START_LINK$aplikasi Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": " $1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:40:45.096225977 CET	49736	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.097192049 CET	49738	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.168412924 CET	49741	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.229932070 CET	443	49736	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.230060101 CET	49736	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.234747887 CET	443	49738	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.234878063 CET	49738	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.269690990 CET	49736	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.269876957 CET	49738	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.302088976 CET	443	49741	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.302180052 CET	49741	443	192.168.2.4	167.89.123.122

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:40:45.303126097 CET	49741	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.403250933 CET	443	49736	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.404087067 CET	443	49736	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.404141903 CET	443	49736	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.404191017 CET	443	49736	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.404238939 CET	443	49736	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.404289007 CET	49736	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.404355049 CET	49736	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.407051086 CET	443	49738	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.408497095 CET	443	49738	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.408560038 CET	443	49738	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.408621073 CET	443	49738	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.408626080 CET	49738	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.408675909 CET	443	49738	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.408719063 CET	49738	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.438083887 CET	443	49741	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.440696955 CET	443	49741	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.440754890 CET	443	49741	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.440814018 CET	49741	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.440814972 CET	443	49741	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.440867901 CET	443	49741	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.440915108 CET	49741	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.695804119 CET	49736	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.697011948 CET	49738	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.698056936 CET	49741	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.829508066 CET	443	49736	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.831614971 CET	443	49741	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.833898067 CET	49741	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.834501982 CET	443	49738	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:45.959193945 CET	49736	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.959747076 CET	49738	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:45.967765093 CET	443	49741	167.89.123.122	192.168.2.4
Feb 25, 2021 21:40:46.059190989 CET	49741	443	192.168.2.4	167.89.123.122
Feb 25, 2021 21:40:46.092200994 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.138238907 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.138338089 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.138607025 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.185216904 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.186906099 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.186924934 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.187010050 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.187043905 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.197751999 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.197953939 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.198138952 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.246115923 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.246133089 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.246145964 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.246156931 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.246208906 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.246591091 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.304336071 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.304718018 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.305037975 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.305392027 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.305700064 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.306035995 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.332461119 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.349530935 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.349901915 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.350464106 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.350492954 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.350517035 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.351279020 CET	443	49744	151.101.1.195	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:40:46.351320982 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.351352930 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.351358891 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.351375103 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.351397991 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.351428032 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.351448059 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.351450920 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.351491928 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.351502895 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.351528883 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.351542950 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.351567984 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.351586103 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.351608992 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.353236914 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.353280067 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.353296041 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.353322029 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.354902029 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.354978085 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.355071068 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.355123997 CET	49744	443	192.168.2.4	151.101.1.195
Feb 25, 2021 21:40:46.356698990 CET	443	49744	151.101.1.195	192.168.2.4
Feb 25, 2021 21:40:46.356736898 CET	443	49744	151.101.1.195	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:40:34.734522104 CET	59123	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:34.790865898 CET	53	59123	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:35.972237110 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:36.023984909 CET	53	54531	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:36.941675901 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:36.999326944 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:37.811148882 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:37.859842062 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:38.694195032 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:38.747512102 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:39.533368111 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:39.584446907 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:40.416198969 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:40.467854977 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:41.544291019 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:41.596034050 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:44.055166960 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:44.106873035 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:44.913562059 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:44.917016029 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:44.924336910 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:44.950102091 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:44.973767042 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:44.975161076 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:44.985008955 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:44.998583078 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:46.011910915 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:46.025914907 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:46.081907034 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:46.091387033 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:46.231648922 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:46.300012112 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:46.306649923 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:46.366175890 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:46.581906080 CET	64801	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:40:46.635662079 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:46.795720100 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:46.820035934 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:46.857541084 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:46.864165068 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:46.881892920 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:46.930825949 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:46.957978010 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:47.006833076 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:47.062146902 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:47.110824108 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:47.789551973 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:47.839423895 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:47.963212967 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:48.012749910 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:48.580615997 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:48.648298025 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:49.490230083 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:49.569485903 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:51.179030895 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:51.227988005 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:52.099646091 CET	50183	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:52.148605108 CET	53	50183	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:52.930550098 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:52.979130983 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:54.451356888 CET	55916	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:54.510742903 CET	53	55916	8.8.8.8	192.168.2.4
Feb 25, 2021 21:40:59.757529974 CET	60542	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:40:59.811772108 CET	53	60542	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:03.287744045 CET	60689	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:03.340877056 CET	53	60689	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:04.764492035 CET	64206	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:04.813308001 CET	53	64206	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:05.566411972 CET	50904	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:05.616987944 CET	53	50904	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:06.142776012 CET	57525	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:06.194088936 CET	53	57525	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:23.504556894 CET	53814	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:23.584280968 CET	53	53814	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:24.221788883 CET	53418	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:24.289515018 CET	53	53418	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:24.881195068 CET	62833	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:24.973500967 CET	53	62833	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:25.321652889 CET	59260	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:25.381496906 CET	53	59260	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:25.405577898 CET	49944	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:25.531199932 CET	53	49944	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:25.998924017 CET	63300	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:26.050962925 CET	53	63300	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:26.592772007 CET	61449	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:26.649837017 CET	53	61449	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:27.261943102 CET	51275	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:27.319437027 CET	53	51275	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:28.357237101 CET	63492	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:28.419601917 CET	53	63492	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:29.375392914 CET	58945	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:29.424509048 CET	53	58945	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:29.861347914 CET	60779	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:29.916079044 CET	53	60779	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:41.547159910 CET	64014	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:41.597861052 CET	53	64014	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:41.742706060 CET	57091	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:41.809761047 CET	53	57091	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:42.804486036 CET	55904	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:41:42.869132996 CET	53	55904	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:43.793642044 CET	54450	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:43.874866009 CET	53	54450	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:44.670932055 CET	49374	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:44.721488953 CET	53	49374	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:46.377134085 CET	50436	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:46.428771973 CET	53	50436	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:46.586894989 CET	62605	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:46.653764963 CET	53	62605	8.8.8.8	192.168.2.4
Feb 25, 2021 21:41:46.814412117 CET	54256	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:41:46.874422073 CET	53	54256	8.8.8.8	192.168.2.4
Feb 25, 2021 21:42:14.002975941 CET	52189	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:42:14.065865993 CET	53	52189	8.8.8.8	192.168.2.4
Feb 25, 2021 21:42:14.263396025 CET	56131	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:42:14.324551105 CET	53	56131	8.8.8.8	192.168.2.4
Feb 25, 2021 21:42:16.627783060 CET	62992	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:42:16.680986881 CET	53	62992	8.8.8.8	192.168.2.4
Feb 25, 2021 21:42:18.856197119 CET	54432	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:42:18.923388958 CET	53	54432	8.8.8.8	192.168.2.4
Feb 25, 2021 21:42:37.682037115 CET	57227	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:42:37.747345924 CET	53	57227	8.8.8.8	192.168.2.4
Feb 25, 2021 21:42:37.883785963 CET	58383	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:42:37.932782888 CET	53	58383	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:40:44.924336910 CET	192.168.2.4	8.8.8.8	0x6065	Standard query (0)	u16095581.ct.sendgrid.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:46.025914907 CET	192.168.2.4	8.8.8.8	0xd4a2	Standard query (0)	qgohifmzuv.web.app	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:46.864165068 CET	192.168.2.4	8.8.8.8	0x8a25	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:49.490230083 CET	192.168.2.4	8.8.8.8	0x5d4f	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:40:44.975161076 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	u16095581.ct.sendgrid.net		167.89.123.122	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:44.975161076 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	u16095581.ct.sendgrid.net		167.89.118.28	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:44.975161076 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	u16095581.ct.sendgrid.net		167.89.118.35	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:44.975161076 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	u16095581.ct.sendgrid.net		167.89.123.16	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:46.091387033 CET	8.8.8.8	192.168.2.4	0xd4a2	No error (0)	qgohifmzuv.web.app		151.101.1.195	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:46.091387033 CET	8.8.8.8	192.168.2.4	0xd4a2	No error (0)	qgohifmzuv.web.app		151.101.65.195	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:46.930825949 CET	8.8.8.8	192.168.2.4	0x8a25	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:40:46.930825949 CET	8.8.8.8	192.168.2.4	0x8a25	No error (0)	d26p066pn2w0s0.cloudfront.net		99.84.90.99	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:46.930825949 CET	8.8.8.8	192.168.2.4	0x8a25	No error (0)	d26p066pn2w0s0.cloudfront.net		99.84.90.18	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:46.930825949 CET	8.8.8.8	192.168.2.4	0x8a25	No error (0)	d26p066pn2w0s0.cloudfront.net		99.84.90.42	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:40:46.930825949 CET	8.8.8.8	192.168.2.4	0x8a25	No error (0)	d26p066pn2w0s0.cloudfront.net		99.84.90.26	A (IP address)	IN (0x0001)
Feb 25, 2021 21:40:49.569485903 CET	8.8.8.8	192.168.2.4	0x5d4f	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:40:49.569485903 CET	8.8.8.8	192.168.2.4	0x5d4f	No error (0)	googlehosted.l.googleusercontent.com		142.250.184.33	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- logo.clearbit.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49753	99.84.90.99	80	C:\Program Files\Google\Chrome\Application\chrome.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Feb 25, 2021 21:40:46.985209942 CET</td><td>1545</td><td>OUT</td><td>GET /sccollege.edu HTTP/1.1
Host: logo.clearbit.com
Connection: keep-alive
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: image/avif,image/webp,image/apng,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8</td></tr>
<tr><td>Feb 25, 2021 21:40:47.046876907 CET</td><td>1554</td><td>IN</td><td>HTTP/1.1 200 OK
Content-Type: image/png
Transfer-Encoding: chunked
Connection: keep-alive
Date: Mon, 22 Feb 2021 15:32:03 GMT
access-control-allow-origin: *
Cache-Control: public, max-age=2592000
Server: envoy
X-Cache: Hit from cloudfront
Via: 1.1 acc9aed747aea07d6138203ddfb2dcd9.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: MUC50-C1
X-Amz-Cf-Id: 4vNxMFVT1vGkgevkQ6tYZSLx5xfayn5DePyHPGGvrELd7gM8FkoFPA==
Age: 277724
Data Raw: 32 34 61 63 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 80 00 00 00 80 08 02 00 00 00 4c 5c f6 9c 00 00 24 73 49 44 41 54 78 9c ec 7d 07 9c 5c 57 75 f7 39 f7 be 37 6d 7b af da 95 76 57 2b ed ae 7a b3 8a 25 59 b2 2d d9 b2 e5 82 7b 0c c6 26 71 80 40 20 40 48 20 c0 2f 09 81 90 7c 7c 24 a1 7d a6 d8 60 30 c4 06 db d8 b8 60 64 2c 5b cd 56 ef da 5d 6d d1 6a 9b b6 97 a9 3b e5 bd 77 cf f7 7b f7 cd ec ae 64 39 58 9e b1 46 fc 32 7f cd 6f f5 e6 cd cc 7b f7 de 73 ef e9 f7 3c 85 cd ba 1b 52 48 1e 58 b2 1b f0 bf 1d 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 29 02 24 19 4a c2 ae 84 08 40 48 04 e6 7f 00 c4 cc 63 04 42 79 0e cd f3 48 88 e6 1f 5d 1e 73 00 04 d0 01 b8 fc 3d 11 30 3a ef 8a e6 cf 61 da 29 34 df 30 f3 2c 92 79 4c d6 19 eb ab 17 87 d9 92 e8 6f f1 1d bf 74 a9 1d 35 2f 14 eb 52 dc 48 1c 01 a2 fd c3 d8 60 23 a3 68 4b a7 9a 8a 40 24 80 b8 3c 43 04 0a 60 04 48 35 c9 05 02 41 80 a4 9f f9 2d b3 97 16 05 71 da 2d 44 6c 28 05 58 5f 98 fa f4 e2 a3 c1 88 a6 7d 01 13 d4 53 14 c0 62 f4 8c 97 0a 09 23 40 74 90 49 21 73 34 0d 04 43 00 47 73 5d 58 23 2b 07 0b 0d 42 83 0b 87 a4 82 2e 07 94 11 31 60 9a 0e 2a 23 dd 5c 45 b2 7b f2 7a 44 68 2d 9f c9 7b 70 b2 98 a6 b5 bc e4 fa 32 d7 8f 30 2c 3a bd 7d 30 c4 34 1e 4b 09 1a 7f b3 53 d6 3c 89 5d 38 9e ab 25 90 05 91 39 94 48 69 0e 65 d6 8c 32 04 3a 7d a6 b7 7a 76 75 7b 6b 33 70 56 90 5f 38 30 30 0c c4 1c 36 65 f6 cc b2 d1 51 cf c0 88 37 3d c3 9e 9e 9e 3d d8 37 96 9f 9f 95 9f 9b c7 49 d7 09 23 a0 76 76 f6 1a 5a 78 76 d5 0c 87 c2 c4 34 b6 64 d2 04 48 20 eb 3d 37 ea f3 05 00 89 01 54 96 e7 13 41 57 ef 30 4d 23 95 35 36 05 79 b9 f9 79 99 72 35 5a 27 cc 05 04 14 ef 9c 65 92 94 03 a3 de a1 31 0f 45 89 f1 de 11 27 01 30 36 b1 cc 19 49 c8 80 c0 30 f4 f5 eb d7 9c eb ed 6f 69 e9 b8 7e c3 ea 33 2d 4d 24 a8 a1 a1 7e 60 60 27 00 ab 9c 51 fa c0 bd 5b 07 07 46 fe f3 87 4f 57 cf 9c 31 e6 0d 28 0a 3d 70 e7 96 b2 dc ec ee fe 91 c3 4d ed 8d 6d 67 41 f3 6f b9 66 cd c6 ab 57 20 e9 c4 60 c4 e3 0f 86 23 25 79 d9 36 0e 44 34 ee 8f fc df ef fd 54 8e 03 53 38 ac 5a b6 a4 a7 bf bf ab 67 08 4d be c4 08 14 06 ba 64 7d c2 ed 19 59 b1 a8 7a ed aa 15 24 34 5f 20 ec 52 95 34 87 8a 44 02 79 94 18 ef b9 cf c0 7e bf eb c0 ef 77 1f 8c 7f 51 25 66 05 20 10 27 23 37 3b 4d 10 b9 bd de 47 1e 7b 82 c0 9e 9e 9e 73 f4 c4 49 03 14 12 d4 de 7e 16 e4 ec 2b 2f 2f e4 42 2f 2b cc a9 a9 99 d1 7e b6 67 c2 ef dd 7a e3 b5 39 99 19 3f 79 7e 7b 63 63 8b a2 b0 82 bc cc db 6e 58 bf 66 e9 02 85 26 04 30 32 94 df bd b2 f3 44 fb 39 bb 4d 5d bd a4 76 ed 9a 95 fb 0e 9f 0c 19 96 fe 46 9a 01 ed 9d 7d 8d 4d a7 80 68 d1 fc b9 bd 7d 3d 23 a3 be b4 8c
Data Ascii: 24acPNGIHDRL\$sIDATx}\Wu97m{vW+z%Y-{&q@ @H /||$}`0`d,[V]mj;w{d9XF2o{s<RHX)$)$)$)$)$)$)$)$)$)$)$)$)$)$)$)$)$)$J@HcByH]s=0:a)40,yLot5/RH`#hK@$<C`H5A-q-Dl(X_}Sb#@tI!s4CGs]X#+B.1`*#\E{zDh-{p20 ,:}04KS<]8%9Hie2:}zvu{k3pV_8006eQ7==7I#vvZxv4dH =7TAW0M#56yyr5Z'e1E'06I0oi~3-M$~``'Q[FOW1(=pMmgAofW `#%y6D4TS8ZgMd}Yz$4_ R4Dy~wQ%f '#7;MG{sI~+//B/+~gz9?y~{ccnXf&02D9M]vF}Mh}=#</td></tr>
</table>

HTTPS Packets

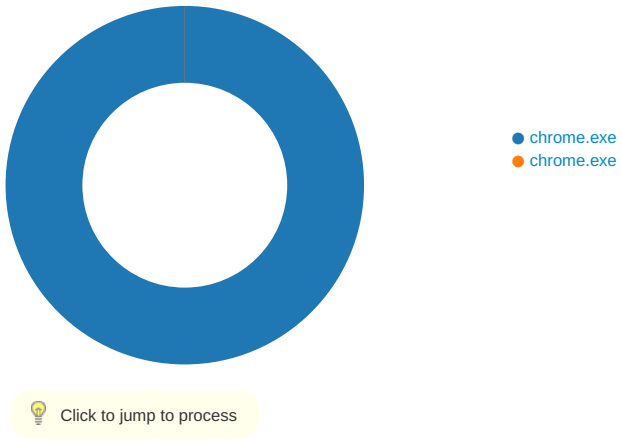
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:40:45.404238939 CET	167.89.123.122	443	192.168.2.4	49736	CN=*.ct.sendgrid.net, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon May 18 21:12:26 CEST 2020	Sun Jun 12 03:36:38 CEST 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
Feb 25, 2021 21:40:45.408675909 CET	167.89.123.122	443	192.168.2.4	49738	CN=*.ct.sendgrid.net, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon May 18 21:12:26 CEST 2020	Sun Jun 12 03:36:38 CEST 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
Feb 25, 2021 21:40:45.440867901 CET	167.89.123.122	443	192.168.2.4	49741	CN=*.ct.sendgrid.net, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon May 18 21:12:26 CEST 2020	Sun Jun 12 03:36:38 CEST 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6816 Parent PID: 5112

General

Start time:	21:40:40
Start date:	25/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://u16095581.ct.sendgrid.net/ls/click?upn=FLaa9Uev-2B7s-2FZ9Dw3t6-2FoboxXa9RoxlkakQvTvnjy9nXTXjD6tNZcebsQGigytMZye255UswQ6f3sQ0K3qccZrkmIGtWjJPIGztPn38pYzM-3D7_6s_DwB70HpLJuR35GFtSIesHJrrx5IO6qEPxbkrEpQrYnrx-2FXwixj3Q3HnEwW-2Fs-2BBPbBxlPPFHusk7-2BufOFY4-2BYO9fqGw8G6IKDphuEsqM-2B5hWTu2tXyTpvimSzAQwQnBG-2BsgMdkv-2B3igkZIHlWGKqVkU4mGhq9zYrBUF7V0zSm4CdYW3168zSE6-2FrgVMBpTopWiclUE2uJbujZKS9qBrMxjc8wcVkUUy8Jmc7-2BKB9-2BhEc-3D'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

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

Analysis Process: chrome.exe PID: 7016 Parent PID: 6816

General

Start time:	21:40:41
Start date:	25/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1608,13295437612127757828,17913449545750257871,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly