ID: 458985
Cookbook: browseurl.jbs
Time: 00:25:24
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

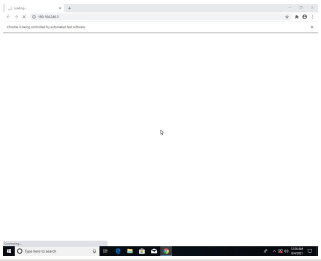
Windows Analysis Report http://180.104.246.3

Overview

General Information

Sample URL:	http://180.104.246.3
Analysis ID:	458985
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

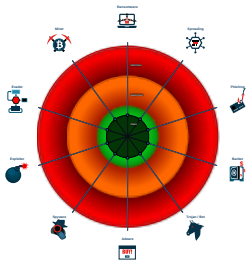
Detection

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

No high impact signatures.

Classification



Analysis Advice

Joe Sandbox was unable to browse the URL (domain or webserver down or HTTPS issue), try to browse the URL again later

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Process Tree

- **System is w10x64**
- chrome.exe (PID: 5760 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://180.104.246.3' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1848 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1576,17160568527506305237,18363554842373443119,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1712 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

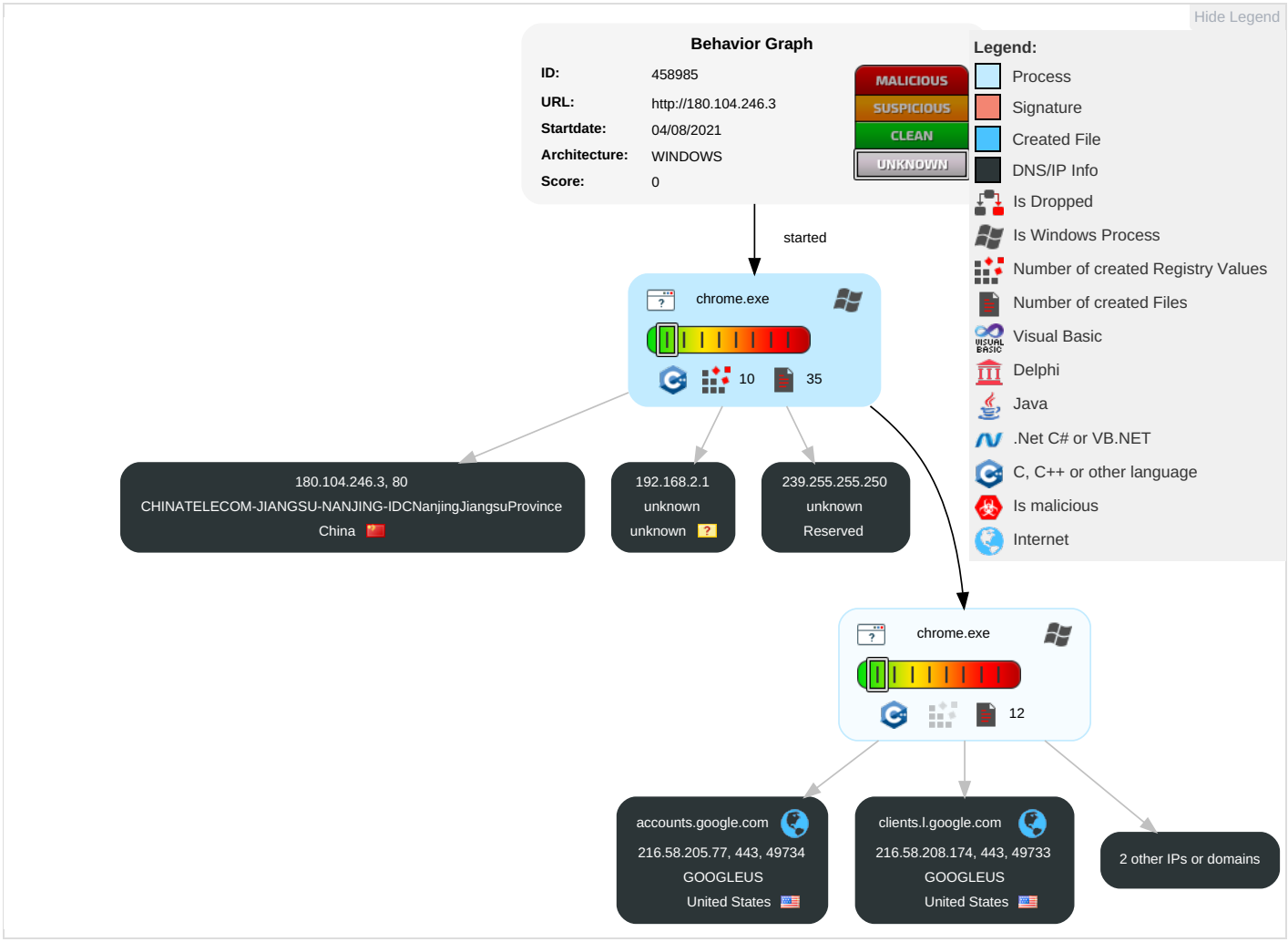
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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	Modify System Partitior
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
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 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

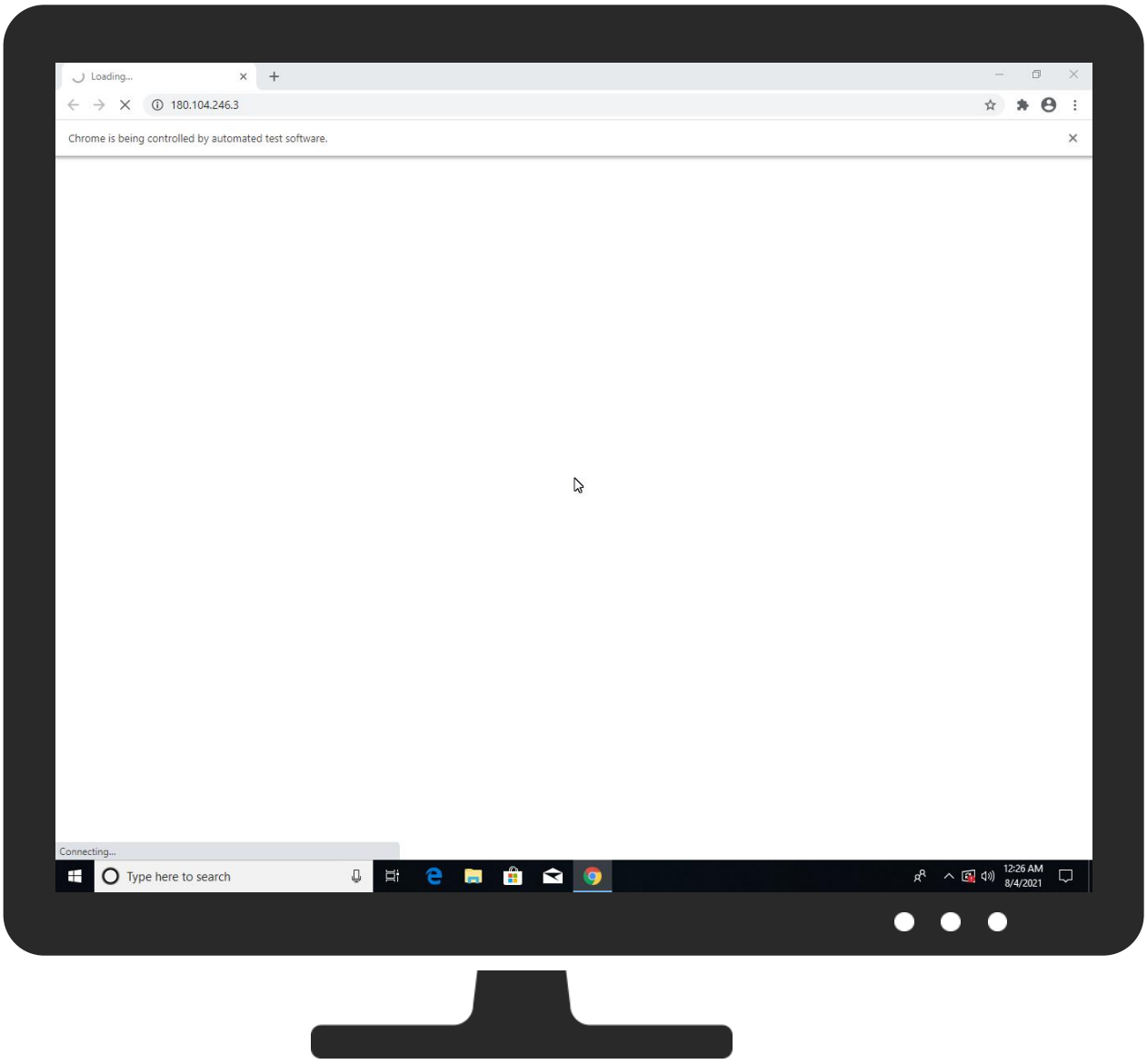
Behavior Graph



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://180.104.246.3	2%	Virustotal		Browse
http://180.104.246.3	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://180.104.246.3/d=	0%	Avira URL Cloud	safe	
http://180.104.246.3/	2%	Virustotal		Browse
http://180.104.246.3/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.205.77	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
clients2.google.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
180.104.246.3	unknown	China		137702	CHINATELECOM-JIANGSU-NANJING-IDCNanjingJiangsuProvince	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458985
Start date:	04.08.2021
Start time:	00:25:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://180.104.246.3
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:	5

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:	UNKNOWN
Classification:	unknown0.win@15/48@2/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All
Errors:	• URL not reachable

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\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

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

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\1bbf3729-8856-4e9b-8809-e8e87da9ea7c.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):	16745
Entropy (8bit):	5.57739365965048
Encrypted:	false
SSDEEP:	384:5IltjLlNHXh1kXqKf/pUZNCgVLH2HfDGrUNblxy24ZS:+LlRh1kXqKf/pUZNCgVLH2HfirUlDdT
MD5:	E2E54AA9428A7FBED439D192E8D00B39
SHA1:	2D3356F0FF1E8C94F72DC16ED204AE81E0C33E88
SHA-256:	9C40CCBBE59B7C79AAF15F80FE9D09FDF3A84C6D2574EDE7EF69AD0956D0BFF7
SHA-512:	45D2ACAF73D41B7E7E0A174119D47C819A5B595A94033089B3D0B4C4DD7F8E856413658F6D1C9501F6E2848A03E6AEC92F64ECA544DD85F773B3D1BB555C8D6
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":"13272503167929384","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\1cd1e788-cc40-44e6-8b38-5a19f1e3e3bf.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):	1041
Entropy (8bit):	5.570356141115493
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeiXzkq/HeUe8zUe37wUnsRUeiQ:Ym6UUhyKUeiYqPeUekUerwUnQUeP
MD5:	C3A0B164E6D735C90F6179D77DA4CBC9
SHA1:	92724A117984CA61DF462C09F8FA3E068FDE7FCE
SHA-256:	814458BBCC78CFA7F313B1193F6539088BA246B52DC9052FA9071D0E7BCFF548
SHA-512:	3BD5F6B553801AA806A7CE650C53BB434793A21B2D828A7044D01EEB075E7ADF694B5C3BFAB642A234959CD0FFC4D04285A8E16F32C169BC5A1917F8883E6B4
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":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"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":1659565571.043354,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628029571.043357},{"expiry":1632986995.164829,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3c5bf8c7-bbb1-4be0-8d6b-c51ecef0730a.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):	4891
Entropy (8bit):	4.934509471016479
Encrypted:	false
SSDEEP:	48:YcLSMkKSChkliLqAOqqTlYGlQKHoTw0brf4MqM8C1Nfct/9BhUJo3KhmeSnpNGzm:nmELkt9pIKIt5k0JCKL8bbOTlVuHn
MD5:	19D6FDDF4509F98F8C2478E6E5114618
SHA1:	7FDDC818683744EEB8A5233555B301189A82B3A0
SHA-256:	9BBA6DAB792E66580B2F3AFFF504528F932151B86E54561D7AB098175805E374
SHA-512:	2169A1EC820C1F1B637925D57CDA59CC733A36453EAB9FABB5ED5C0C2158BC6379CE556C16B84B087C70DB4ED42E162A9EAA4883EF29F98ADC99A1784FEE072D
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3c5bf8c7-bbb1-4be0-8d6b-c51ecef0730a.tmp	
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272503168209277","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":{"default_browser_infobar_last_declined":"13245924607060180","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_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4059da12-cecd-4fe2-bf2f-0b9c84f887ad.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:	modified
Size (bytes):	16746
Entropy (8bit):	5.577504372855019
Encrypted:	false
SSDEEP:	384:5Ilt2LlNHXh1kXqKf/pUZNCgVLH2HfDGrUYblxy245HP:tLlRh1kXqKf/pUZNCgVLH2HfirUkDdKv
MD5:	6DD7F24AAE4B78791F410B1263223644
SHA1:	52962DCFEC89C11213B859E316A5667C98CD0BC0
SHA-256:	C47477075C89CDB60F48DD472E050F5D8DFCAB704324AD59C61241120AB565C8
SHA-512:	AAB7D35B8A06FD78363C1D96EB066F25E8CD8B5D0ACCA12836C88B8874EC136CCEB4BC32F24A783D1492C002EBE256CCDCD21088E8DD5346CA853D8D6CEC3C1
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":"13272503167929384","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\609f01de-31a8-4d6c-8920-8961dceb5737.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":"13248516607334226","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\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	917
Entropy (8bit):	3.0063490614512056
Encrypted:	false
SSDEEP:	12:3olydJh+HPE1PlpxlpNVOrYlptlpyItbtmQUtZlV:34SXlrlJXlLlQ6tml
MD5:	8B656E7A7FEC9EC34F93791370B0AB69
SHA1:	F40B89F3E9E50854DB9B602CCB48DA6E91830262
SHA-256:	9C5A82077CFA251A5FCFD9B7157C9C432DD342D515BD7962D48F6D8C3D660128
SHA-512:	8B59E5B363832DF3B3A7A1BD33521F1D7537DC2F0BFAD4A3B168D02782C95229FA6A2DBDEB35F86E12D6A19D96EB5AC749F5DF83D7E835CFB18633E1E319D9B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Preview:	SNSS.....!.....1.,.....$...fb9b82ce_d3ec_4a6e_a9e5_b5ae7c486746.....H..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....http://180.104.246.3/.... ...|...x.....p.....h.....`.....{-.....{-.....2.....h.t.t.p.:./.1.8.0...1.0.4...2.4.6...3./..... .....8.....0.....8..... .....http://180.104.246.3/.....d=.vE'/.....

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):	126
Entropy (8bit):	4.569580985472087
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC54:qT5z/t2qoEwhXeLKI
MD5:	F9672B4DD4FE52E26F179EAF35E69B22
SHA1:	DE3C80E35851DFAD51E1FD0F35E90EC5C223B739
SHA-256:	11F36B4E7449BA10E1E24571A5DE3A67918F8B971A2B2B43FFC549492C00DEC5
SHA-512:	898A55D8F35DA209FA85E9F94654CFA12859D411740394BBA1A909FA77109B0FB6F36D5E7B4AFA7F8CCBF6BE407E01421229E7EC241906A9ECCCAE852622609I
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.132065469485546
Encrypted:	false
SSDEEP:	6:mkO+q2Pwkn23iKKdK8aPrqIFUtp9s5ZmwP9aVkwOwkn23iKKdK8amLJ:N/vYf5KkL3FUtp9s5/P9S5Jf5KkQJ
MD5:	D6EA64D6470143BA7F469A7CD296D85C
SHA1:	024A8CC3619C808B71007CFCE9D250A700DA0C06
SHA-256:	7C2A599949BF93E41CF3BA5DBB3327DF21CD0659373AD5BA8C2EE65DADEC9F83
SHA-512:	B8DE0C6E929F77EF94650BF2F1AC9C134C8B275B8A0C272275341D1645011AE37FEAEC15D0B9E38133EF046138B4A71EACEACE3E1577FEA4D2B9FA9CF430C5AA
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:08.215 1028 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-00:26:08.217 1028 Recovering log #3.2021/08/04-00:26:08.219 1028 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 Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.132065469485546
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
SSDEEP:	6:mkO+q2Pwkn23iKKdK8aPrqIFUtp9s5ZmwP9aVkwOwkn23iKKdK8amLJ:N/vYf5KkL3FUtp9s5/P9S5Jf5KkQJ
MD5:	D6EA64D6470143BA7F469A7CD296D85C
SHA1:	024A8CC3619C808B71007CFCE9D250A700DA0C06
SHA-256:	7C2A599949BF93E41CF3BA5DBB3327DF21CD0659373AD5BA8C2EE65DADEC9F83
SHA-512:	B8DE0C6E929F77EF94650BF2F1AC9C134C8B275B8A0C272275341D1645011AE37FEAEC15D0B9E38133EF046138B4A71EACEACE3E1577FEA4D2B9FA9CF430C5AA
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:08.215 1028 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-00:26:08.217 1028 Recovering log #3.2021/08/04-00:26:08.219 1028 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):	456
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWW
MD5:	F23D2DF21A39AA8D814CADE6C37856C8
SHA1:	233E65707015A53F83A0D53DB03A4AF8FAB21EA6
SHA-256:	C5CE9AAF8FFDCB8A00463A7BF24001885E0A792F110C8DB74A1E2F4392CB0E31
SHA-512:	A7B50B8CAFBA80F6BACA44B260F8379852C4176F3DD57168812F3B4B811D2FF340F09F8CE625CC2ADECAB2851CC33725CB729548A3DA98B041387C795207791
Malicious:	false
Reputation:	low
Preview:	.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):	5.102941715562696
Encrypted:	false
SSDEEP:	6:mkyv+q2Pwkn23iKKdK8NIFUtp9yf5ZmwP9yNItVkwOwkn23iKKdK8+eLJ:N9vYf5KkpFUtp9y/P9H5Jf5KkqJ
MD5:	314CD82CFE880DC516C39F6297336176
SHA1:	3EE2B5FEF32036E253BE4E59EB12F16E111640CF
SHA-256:	DC28C189EFAB6D7E9DE6C9F3888F1971C3C32096FFB06750A37C104B75466C30
SHA-512:	0C9218B2DA6973D326E0399FA5CDE7FBA03A83D9988E56D353899C8B6A0025CC6BEF34C0FB978FA35DCCEA083527D2006F47C5F2A59A14DEAE55C7C3EF6B8E69
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:10.400 16a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-00:26:10.402 16a8 Recovering log #3.2021/08/04-00:26:10.403 16a8 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\Extension State\LOG.old_ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.102941715562696
Encrypted:	false
SSDEEP:	6:mkyv+q2Pwkn23iKKdK8NIFUtp9yf5ZmwP9yNItVkwOwkn23iKKdK8+eLJ:N9vYf5KkpFUtp9y/P9H5Jf5KkqJ
MD5:	314CD82CFE880DC516C39F6297336176
SHA1:	3EE2B5FEF32036E253BE4E59EB12F16E111640CF
SHA-256:	DC28C189EFAB6D7E9DE6C9F3888F1971C3C32096FFB06750A37C104B75466C30
SHA-512:	0C9218B2DA6973D326E0399FA5CDE7FBA03A83D9988E56D353899C8B6A0025CC6BEF34C0FB978FA35DCCEA083527D2006F47C5F2A59A14DEAE55C7C3EF6B8E69
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old_ (copy)	
Preview:	2021/08/04-00:26:10.400 16a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-00:26:10.402 16a8 Recovering log #3.2021/08/04-00:26:10.403 16a8 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\Last Session4 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	917
Entropy (8bit):	3.0063490614512056
Encrypted:	false
SSDEEP:	12:3olydJh+HPE1PlpxlpNVOrYlptlpyItbtmQUtZlV:34SXlrlJXlLlQ6tml
MD5:	8B656E7A7FEC9EC34F93791370B0AB69
SHA1:	F40B89F3E9E50854DB9B602CCB48DA6E91830262
SHA-256:	9C5A82077CFA251A5FCFD9B7157C9C432DD342D515BD7962D48F6D8C3D660128
SHA-512:	8B59E5B363832DF3B3A7A1BD33521F1D7537DC2F0BFAD4A3B168D02782C95229FA6A2DBDEB35F86E12D6A19D96EB5AC749F5DF83D7E835CFB18633E1E319D9B
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...fb9b82ce_d3ec_4a6e_a9e5_b5ae7c486746.....H.....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....http://180.104.246.3/....`...|...x.....p.....h.....`.....{-.....{-.....2.....h.t.t.p.:././.1.8.0...1.0.4...2.4.6...3./.....8.....0.....8..... .....http://180.104.246.3/.....d=.vE'/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabsta (copy)	
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\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.17143346852765
Encrypted:	false
SSDEEP:	6:mk+at+q2Pwkn23iKKdK8a2jMGIFUtp9+nKZmwP9+yQtVkwOwkn23iKKdK8a2jMmd:N+jvYf5Kk8EFUtp9+nK/P9+yQT5Jf5KV
MD5:	B9C045201046BD658503F60F29E1A988
SHA1:	3ED46DAE73CEC4F0072FE6A4DD4300726E6E9F04
SHA-256:	79EF4ECD5AFA342764C3C1B2CE502CD1297C5F995E4044B27DCAEDE7741A8AE5
SHA-512:	15E0C3F2C90EA8C1E9E4AF8A15A876926AA76A78643567619BEE82A7BA40DA572DF4DA4D3E0768BA02DBFBC8F1C4459D66D9EEC45800F598CBF04894B037EB78
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:07.987 328 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:26:07.990 328 Recovering log #3.2021/08/04-00:26:07.991 328 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\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
Entropy (8bit):	5.17143346852765
Encrypted:	false
SSDEEP:	6:mk+at+q2Pwkn23iKKdK8a2jMGIFUtp9+nKZmwP9+yQtVkwOwkn23iKKdK8a2jMmd:N+jvYf5Kk8EFUtp9+nK/P9+yQT5Jf5KV
MD5:	B9C045201046BD658503F60F29E1A988
SHA1:	3ED46DAE73CEC4F0072FE6A4DD4300726E6E9F04
SHA-256:	79EF4ECD5AFA342764C3C1B2CE502CD1297C5F995E4044B27DCAEDE7741A8AE5
SHA-512:	15E0C3F2C90EA8C1E9E4AF8A15A876926AA76A78643567619BEE82A7BA40DA572DF4DA4D3E0768BA02DBFBC8F1C4459D66D9EEC45800F598CBF04894B037EB78
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:07.987 328 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:26:07.990 328 Recovering log #3.2021/08/04-00:26:07.991 328 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State37 (copy)	
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":"13248516607334226","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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.176430266974875
Encrypted:	false
SSDEEP:	6:mkuIq2Pwkn23iKKdKgXz4rRIFUtp9DNJZmwP9DNDkwOwkn23iKKdKgXz4q8LJ:NnvYf5KkgXiuFUtp95J/P95D5Jf5Kkgi
MD5:	CAFF5C60D3BDF4DFEC10F7E98479F449
SHA1:	17A86CB1A1C337157C65B9ED29D6361283372819
SHA-256:	70BFC0D38E81B99E46722F84A806EB2BF7341764108BFB4B079F5548380F0D25
SHA-512:	156405AE4656298C3D8B857D33D9A00A6010BEFAA2C415715B70F69496C172377D9A65921798299F5CF18528FE450A28D179B0416D68C46C4132A502C8DD4DFC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:08.236 c34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-00:26:08.237 c34 Recovering log #3.2021/08/04-00:26:08.237 c34 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\Platform Notifications\LOG.oldun (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.176430266974875
Encrypted:	false
SSDEEP:	6:mkuIq2Pwkn23iKKdKgXz4rRIFUtp9DNJZmwP9DNDkwOwkn23iKKdKgXz4q8LJ:NnvYf5KkgXiuFUtp95J/P95D5Jf5Kkgi
MD5:	CAFF5C60D3BDF4DFEC10F7E98479F449
SHA1:	17A86CB1A1C337157C65B9ED29D6361283372819
SHA-256:	70BFC0D38E81B99E46722F84A806EB2BF7341764108BFB4B079F5548380F0D25
SHA-512:	156405AE4656298C3D8B857D33D9A00A6010BEFAA2C415715B70F69496C172377D9A65921798299F5CF18528FE450A28D179B0416D68C46C4132A502C8DD4DFC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.oldun (copy)	
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:08.236 c34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-00:26:08.237 c34 Recovering log #3.2021/08/04-00:26:08.237 c34 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\Preferences.. (copy)	
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):	4891
Entropy (8bit):	4.934509471016479
Encrypted:	false
SSDEEP:	48:YcLSMkKSChkliLqAOqqTlYGlQKHoTw0brf4MqM8C1Nfct/9BhUJo3KhmeSnpNGzm:nmELkt9pIKIt5k0JCKL8bbOTlVuHn
MD5:	19D6FDDF4509F98F8C2478E6E5114618
SHA1:	7FDDC818683744EEB8A5233555B301189A82B3A0
SHA-256:	9BBA6DAB792E66580B2F3AFFF504528F932151B86E54561D7AB098175805E374
SHA-512:	2169A1EC820C1F1B637925D57CDA59CC733A36453EAB9FABB5ED5C0C2158BC6379CE556C16B84B087C70DB4ED42E162A9EAA4883EF29F98ADC99A1784FEE07 2D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272503168209277","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":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
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):	16746
Entropy (8bit):	5.577504372855019
Encrypted:	false
SSDEEP:	384:5Ilt2LlNHXh1kXqKf/pUZNCgVLH2HfDGrUYblxy245HP:tLlRh1kXqKf/pUZNCgVLH2HfirUkDdKv
MD5:	6DD7F24AAE4B78791F410B1263223644
SHA1:	52962DCFEC89C11213B859E316A5667C98CD0BC0
SHA-256:	C47477075C89CDB60F48DD472E050F5D8DFCAB704324AD59C61241120AB565C8
SHA-512:	AAB7D35B8A06FD78363C1D96EB066F25E8CD8B5D0ACCA12836C88B8874EC136CCEB4BC32F24A783D1492C002EBE256CCDCD21088E8DD5346CA853D8D6CEC 3C1
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":"13272503167929384","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\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	181ED05FAE6D31CDBFC2680CB632F859
SHA1:	B6391180B7167969686A3986E06D975F4CE67FAD
SHA-256:	62150C5EA1D8CFDE4916440F9662C32F3DCC1207BBC5441536D121EC683607E4
SHA-512:	40D79847C0420FA9395511DAA271B735ABD60CB55983F23DBF9552E56AAE1D915058D6D236D37D433FA7B16567957DB2C515BDB61B9032003914FF34EFA26BB5
Malicious:	false
Reputation:	low
Preview:	..&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):	5.110202234371212
Encrypted:	false
SSDEEP:	6:mkzA+q2Pwkn23iKKdKrQMxIFUtp9ZZmwP9SVkwOwkn23iKKdKrQMFLJ:NRvYf5KkCFUtp9Z/P9q5Jf5KktJ
MD5:	9755134141DC3ABE3B2B901BDCA33CE1
SHA1:	927883B145A5F8D58C2CB52552F61FB5DC89C8B1
SHA-256:	7990695859ADF41464CE061ED3BD2820BD451E84DB4DDFDF0B1B28A819DD8597
SHA-512:	0CC751AEB53A19D0611B2B5884138BB539911E39A007C55C411F537747636BF9BB8580D2B9E47495319121D1B8A57DC4544CD8D1BCB4ABED283A5F3F92CD585
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:08.151 16a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-0 0:26:08.152 16a8 Recovering log #3.2021/08/04-00:26:08.153 16a8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.110202234371212
Encrypted:	false
SSDEEP:	6:mkzA+q2Pwkn23iKKdKrQMxIFUtp9ZZmwP9SVkwOwkn23iKKdKrQMFLJ:NRvYf5KkCFUtp9Z/P9q5Jf5KktJ
MD5:	9755134141DC3ABE3B2B901BDCA33CE1
SHA1:	927883B145A5F8D58C2CB52552F61FB5DC89C8B1
SHA-256:	7990695859ADF41464CE061ED3BD2820BD451E84DB4DDFDF0B1B28A819DD8597
SHA-512:	0CC751AEB53A19D0611B2B5884138BB539911E39A007C55C411F537747636BF9BB8580D2B9E47495319121D1B8A57DC4544CD8D1BCB4ABED283A5F3F92CD585
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:08.151 16a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-0 0:26:08.152 16a8 Recovering log #3.2021/08/04-00:26:08.153 16a8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/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):	5.189455491964851
Encrypted:	false
SSDEEP:	6:mk+EL+q2Pwkn23iKKdK7Uh2ghZIFUtp9+Bv1ZmwP9+H5LVkwOwkn23iKKdK7Uh2w:N+ZvYf5KklhHh2FUtp9+91/P9+Hf5Jfl
MD5:	8AC4429DB5275FFA9051A663C1802207
SHA1:	2494B5D09894C52163E94E6B265ABBEB56864AEE
SHA-256:	36377E95EC8714B57F8B61562CDF1D560C04C13A67DFA5247224FDA3D5DD1FEC
SHA-512:	B1EA0390238F49F24D62E7CAE708620610113C20DAB4E5FA25EFED9BB6A44FDD01C693457107697C1A04AEAB02D14CBC2212F6DE1F44ACB8EA7334CFA4A2A5 4D
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:07.948 1678 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/04-00:26:07.952 1678 Recovering log #3.2021/08/04-00:26:07.954 1678 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.189455491964851
Encrypted:	false
SSDEEP:	6:mk+EL+q2Pwkn23iKKdK7Uh2ghZIFUtp9+Bv1ZmwP9+H5LVkwOwkn23iKKdK7Uh2w:N+ZvYf5KklhHh2FUtp9+91/P9+Hf5Jfl
MD5:	8AC4429DB5275FFA9051A663C1802207
SHA1:	2494B5D09894C52163E94E6B265ABBEB56864AEE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
SHA-256:	36377E95EC8714B57F8B61562CDF1D560C04C13A67DFA5247224FDA3D5DD1FEC
SHA-512:	B1EA0390238F49F24D62E7CAE708620610113C20DAB4E5FA25EFED9BB6A44FDD01C693457107697C1A04AEAB02D14CBC2212F6DE1F44ACB8EA7334CFA4A2A5 4D
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:07.948 1678 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/04-00:26:07.952 1678 Recovering log #3.2021/08/04-00:26:07.954 1678 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics 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):	5.176588634483274
Encrypted:	false
SSDEEP:	6:mkgt+q2Pwkn23iKKdKusNpV/2jMGIFUtp9cZmwP9cVkwOwkn23iKKdKusNpV/2jz:NJvYf5KkFFUtp9c/P9c5Jf5KkOJ
MD5:	E48D8A36B6975ED4C934EB287818720B
SHA1:	1C1C8EBCD523F8E72545003E5D7D4557689030F6
SHA-256:	8F1B6B55113A9B43F04AE183E3F808D36C76DAF1BE4A908F3585B504CB26A96A
SHA-512:	CDE75D26FDC3B902F300403B208BC411F6A1A1618FBCBE39718C744A3AD3920FDD54FD3E8C0EBC2BD7A09C0242C621BCD6BD19C5A7F7D1DEB281643A8CFB 412
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:08.198 1028 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:26:08.200 1028 Recovering log #3.2021/08/04-00:26:08.200 1028 Reusing old log C:\Users\user\A ppData\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\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.176588634483274
Encrypted:	false
SSDEEP:	6:mkgt+q2Pwkn23iKKdKusNpV/2jMGIFUtp9cZmwP9cVkwOwkn23iKKdKusNpV/2jz:NJvYf5KkFFUtp9c/P9c5Jf5KkOJ
MD5:	E48D8A36B6975ED4C934EB287818720B
SHA1:	1C1C8EBCD523F8E72545003E5D7D4557689030F6
SHA-256:	8F1B6B55113A9B43F04AE183E3F808D36C76DAF1BE4A908F3585B504CB26A96A
SHA-512:	CDE75D26FDC3B902F300403B208BC411F6A1A1618FBCBE39718C744A3AD3920FDD54FD3E8C0EBC2BD7A09C0242C621BCD6BD19C5A7F7D1DEB281643A8CFB 412
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:08.198 1028 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:26:08.200 1028 Recovering log #3.2021/08/04-00:26:08.200 1028 Reusing old log C:\Users\user\A ppData\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\Network Persistent State.. (copy)	
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\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):	5.237886813543177
Encrypted:	false
SSDEEP:	12:NOXOvYf5KkmiuFUtp97/P9K15Jf5Kkm2J:NFYf5KkSg3JKnJf5Kkr
MD5:	8669C7390004ABF01EDAF270016AEA33
SHA1:	3CA02A196B5CC482842294163F0C3521CB576CA1
SHA-256:	BB13A87C185CCE5FF17086E35E88FCD8184464B56C7B5F3B7306691381BF0F45
SHA-512:	DABC07E193663A070ACE18C5EA26B284AB496B41775662645EE21334CD492F96AD45ABC34AEA30E91D93676D3EA64D37C90F10D3633B73F761359209884BEED
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:08.241 16a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/04-00:26:08.244 16a8 Recovering log #3.2021/08/04-00:26:08.245 16a8 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.237886813543177
Encrypted:	false
SSDEEP:	12:NOXOvYf5KkmiuFUtp97/P9K15Jf5Kkm2J:NFYf5KkSg3JKnJf5Kkr
MD5:	8669C7390004ABF01EDAF270016AEA33
SHA1:	3CA02A196B5CC482842294163F0C3521CB576CA1
SHA-256:	BB13A87C185CCE5FF17086E35E88FCD8184464B56C7B5F3B7306691381BF0F45
SHA-512:	DABC07E193663A070ACE18C5EA26B284AB496B41775662645EE21334CD492F96AD45ABC34AEA30E91D93676D3EA64D37C90F10D3633B73F761359209884BEED
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:08.241 16a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/04-00:26:08.244 16a8 Recovering log #3.2021/08/04-00:26:08.245 16a8 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):	415
Entropy (8bit):	5.223752238164854
Encrypted:	false
SSDEEP:	6:mkczIq2Pwkn23iKKdKusNpZQMxIFUtp9ciJZmwP9c/FkwOwkn23iKKdKusNpZQMT:NTvYf5KkMFUtp9FJ/P9c5Jf5KkTJ
MD5:	6EB5191EFBE36BA9B42F8C58F24F9CF9
SHA1:	95DBAD2BCF496E29E2B4C22ACFFCD96FF20E35C6
SHA-256:	1930A2721FEB5964376DA3BE43E410AC0B1E92D42CEC8A6AAEA04BCA5A76C3A4
SHA-512:	E0500FDD75049C73CBEDD7989FABFC82A158207A27125F7300CB3E2A8C05B5C589ED2D00997989FB8FB20BF8ED8AF627877E811291F322438CCA280D950D0D
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:24.344 c34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/04-00:26:24.345 c34 Recovering log #3.2021/08/04-00:26:24.346 c34 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\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.223752238164854
Encrypted:	false
SSDEEP:	6:mkczIq2Pwkn23iKKdKusNpZQMxIFUtp9ciJZmwP9c/FkwOwkn23iKKdKusNpZQMT:NTvYf5KkMFUtp9FJ/P9c5Jf5KkTJ
MD5:	6EB5191EFBE36BA9B42F8C58F24F9CF9
SHA1:	95DBAD2BCF496E29E2B4C22ACFFCD96FF20E35C6
SHA-256:	1930A2721FEB5964376DA3BE43E410AC0B1E92D42CEC8A6AAEA04BCA5A76C3A4
SHA-512:	E0500FDD75049C73CBEDD7989FABFC82A158207A27125F7300CB3E2A8C05B5C589ED2D00997989FB8FB20BF8ED8AF627877E811291F322438CCA280D950D0D
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:24.344 c34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/04-00:26:24.345 c34 Recovering log #3.2021/08/04-00:26:24.346 c34 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\d782c689-3ce9-4c14-9742-00c6796b20e3.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:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
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\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
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):	5.235488113379457
Encrypted:	false
SSDEEP:	6:mk+V84q2Pwkn23iKKdKpIFUtp9+xJZmwP9+1BvDkwOwkn23iKKdKa/WLJ:N+VrvYf5KkmFUtp9+b/P9+1Z5Jf5KkaQ
MD5:	335DABE14E6A7B92049AEB938EC86CC6
SHA1:	36B7B2BCA6BC35893FDA3EB424A9FB277F5E5188
SHA-256:	A370FC02DB6C71C30D053E09B6915FAD0CA70BE6D35677E1293710E2CE7B3A90
SHA-512:	13F9A1F8329EB3B33C10B56D91D4413F76DB48CE1C68CE0E92F61DF87BF8E20B7E0A80A267AEBCD1D39529480FBF335D6DA1FDDA1DD8264642F511768A6BFB 9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:07.947 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-00:26:07.951 16d0 Recovering log #3.2021/08/04-00:26:07.953 16d0 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 Data\LevelDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.235488113379457
Encrypted:	false
SSDEEP:	6:mk+V84q2Pwkn23iKKdKpIFUtp9+xJZmwP9+1BvDkwOwkn23iKKdKa/WLJ:N+VrvYf5KkmFUtp9+b/P9+1Z5Jf5KkaQ
MD5:	335DABE14E6A7B92049AEB938EC86CC6
SHA1:	36B7B2BCA6BC35893FDA3EB424A9FB277F5E5188
SHA-256:	A370FC02DB6C71C30D053E09B6915FAD0CA70BE6D35677E1293710E2CE7B3A90
SHA-512:	13F9A1F8329EB3B33C10B56D91D4413F76DB48CE1C68CE0E92F61DF87BF8E20B7E0A80A267AEBCD1D39529480FBF335D6DA1FDDA1DD8264642F511768A6BFB 9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:26:07.947 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-00:26:07.951 16d0 Recovering log #3.2021/08/04-00:26:07.953 16d0 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\TransportSecurity (copy)	
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):	1041
Entropy (8bit):	5.570356141115493
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeiXzkq/HeUe8zUe37wUnsRUeiQ:Ym6UUhyKUeiYqPeUekUerwUnQUeP
MD5:	C3A0B164E6D735C90F6179D77DA4CBC9
SHA1:	92724A117984CA61DF462C09F8FA3E068FDE7FCE
SHA-256:	814458BBCC78CFA7F313B1193F6539088BA246B52DC9052FA9071D0E7BCFF548
SHA-512:	3BD5F6B553801AA806A7CE650C53BB434793A21B2D828A7044D01EEB075E7ADF694B5C3BFAB642A234959CD0FFC4D04285A8E16F32C169BC5A1917F8883E6B4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"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":1659565571.043354,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628029571.043357},{"expiry":1632986995.164829,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cd923072-bc1b-44ef-80fc-ccf156900767.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\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\Local State (copy)	
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):	174471
Entropy (8bit):	6.079652144521575
Encrypted:	false
SSDEEP:	3072:LscGaYTJQE+mugy9+QV1T7IRwdfLSNPxFcbXafIB0u1GOJmA3iuRU:AdxaV+QfT7GSmhfaqfIlUOoSiuRU
MD5:	1A31EB578E94727BF23B4EB576C1257C
SHA1:	83A0AB21A0BE3D50B76209964F0B95C0453C440D
SHA-256:	B24B40841F14926CC1E44FF36F0834BA1C300E522A0B41C67D728AAE5D7F765E
SHA-512:	B76A1E554B6EF64DBA5413A65C009A199BBF5B18D8D0BC5972ECECAAAFCD6544D89801B455E6F715BC3DC19267DABD5CAE955E65CE8B7E273809CED2090EB472
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":1.628029570820718e+12,"network":1.628029572e+12,"ticks":4587593015.0,"uncertainty":4364222.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\ad01a795-7ec4-4a44-860d-94ceee977de4.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):	174471
Entropy (8bit):	6.079652144521575
Encrypted:	false
SSDEEP:	3072:LscGaYTJQE+mugy9+QV1T7IRwdfLSNPxFcbXafIB0u1GOJmA3iuRU:AdxaV+QfT7GSmhfaqfIlUOoSiuRU
MD5:	1A31EB578E94727BF23B4EB576C1257C
SHA1:	83A0AB21A0BE3D50B76209964F0B95C0453C440D
SHA-256:	B24B40841F14926CC1E44FF36F0834BA1C300E522A0B41C67D728AAE5D7F765E
SHA-512:	B76A1E554B6EF64DBA5413A65C009A199BBF5B18D8D0BC5972ECECAAAFCD6544D89801B455E6F715BC3DC19267DABD5CAE955E65CE8B7E273809CED2090E 472
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_t ime":{"network_time_mapping":{"local":1.628029570820718e+12,"network":1.628029572e+12,"ticks":4587593015.0,"uncertainty":4364222.0}},"os_crypt":{"encrypted_key" :"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOi LGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrw RgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password _manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\d1878dbc-1024-4144-ae1c-e30391b71643.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):	174471
Entropy (8bit):	6.079652539158712
Encrypted:	false
SSDEEP:	3072:LNXGaYTJQE+mugy9+QV1T7IRwdfLSNPxFcbXafIB0u1GOJmA3iuRU:RWxaV+QfT7GSmhfaqfIlUOoSiuRU
MD5:	4BA8F515C05E6D785AFE714D246B6994
SHA1:	040E9D3A2E06820CEE081F98F0620E50D2E26B9B
SHA-256:	D67689B55086FAADA089BE30E359DF70371E2788CFE18AD8FE5D1AE55A13003D
SHA-512:	A72CA38A92BAF43AED74E62FC860137CB13186A5EC15B6EAF82EBC47409892E455DD1CAA4E53AEC0887A085C4D14AF3D15BA611F926B4F106185B99F4EF201 7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_t ime":{"network_time_mapping":{"local":1.628029570820718e+12,"network":1.628029572e+12,"ticks":4587593015.0,"uncertainty":4364222.0}},"os_crypt":{"encrypted_key" :"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOi LGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrw RgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password _manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	2334
Entropy (8bit):	4.643712717256279
Encrypted:	false
SSDEEP:	48:Ev969bSNPcctv969bSEUkKFHtUkFSMFxkqrxkO1FkJ8+69bSGM4+69bSCHq09696:w9mSNk09mSP5b3YVmS3JmSr09mSGYKr+
MD5:	D0DA8E264461346DDEC1436537A5D4D4
SHA1:	9500457A0FB023820FF2456EFA5A791229128CF6
SHA-256:	9DE44584ECE3C280451B4CEFD0900DCC56429B8ABD816A1FF800537D5A3536C4
SHA-512:	D722791AB83FB3F0C8ED436FD5EA0E7A69069A3157CE107F083C4C34B1B307C606D2A87C3804A38B82984532B27984524F3EEE5C1A3A47E099A38D421A396622
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET ad6aa63dcaeb559a99aad3d221fb0f023378e8a4927a473125b377b006fe4186 575269c5aa852052f5d5979f6e79493dd baffded06b7c47e88f7872f7e0b534d.SERVER_HANDSHAKE_TRAFFIC_SECRET ad6aa63dcaeb559a99aad3d221fb0f023378e8a4927a473125b377b006fe4186 a 0cb6142c8a7a8a1293d71c5d98edb5ae81941f9734c41f293ef215a052a9ccd.CLIENT_HANDSHAKE_TRAFFIC_SECRET 4c3694dc28806d62bec9dee7076f186563 f5478c76f6b3b6efd7fb14b89e6a07 c6ebc69ad4bf3a8e66d30822b9c5ebe7728f69285042ead044f49fba11f68a4d.SERVER_HANDSHAKE_TRAFFIC_SECRET 4c 3694dc28806d62bec9dee7076f186563f5478c76f6b3b6efd7fb14b89e6a07 f26962b2620e602724022229621cf3d864129b9d9895733299b65ffbb85cf041.CLIENT_TRAFF IC_SECRET_0 4c3694dc28806d62bec9dee7076f186563f5478c76f6b3b6efd7fb14b89e6a07 631fac645123ed1cdf7b2420885af850559c75c5eb557b330a0418495dfc6de c.SERVER_TRAFFIC_SECRET_0 4c3694dc28806d62bec9dee7076f186563f5478c76f6b3b6efd7fb14b89e6a07 18ec3605378c5a16d7c69348c407ecb611f456c bf5824ea8f01dcb1ea5c561c8.EXPORTER_SECRET 4c3694dc28806d62bec9dee7076f

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 4, 2021 00:26:10.870290995 CEST	192.168.2.4	8.8.8.8	0xaaca	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:26:10.871653080 CEST	192.168.2.4	8.8.8.8	0xbca7	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)

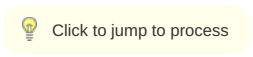
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 00:26:10.912283897 CEST	8.8.8.8	192.168.2.4	0xbca7	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:26:10.912283897 CEST	8.8.8.8	192.168.2.4	0xbca7	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:26:10.913558960 CEST	8.8.8.8	192.168.2.4	0xaaca	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5760 Parent PID: 4176

General

Start time:	00:26:07

Start date:	04/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://180.104.246.3'
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 Show Windows behavior

Registry Activities Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 1848 Parent PID: 5760

General

Start time:	00:26:08
Start date:	04/08/2021
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=1576,17160568527506305237,18363554842373443119,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1712 /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 Show Windows behavior

Disassembly