ID: 458961
Cookbook: browseurl.jbs
Time: 23:07:25
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

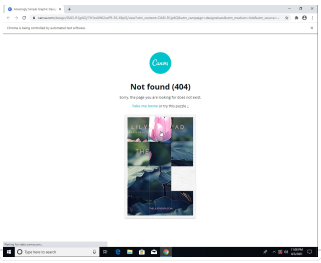
Windows Analysis Report https://www.canva.com/desig…

Overview

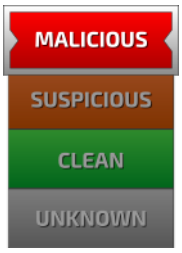
General Information

Sample URL:	https://www.canva.com/design/DAEl-R1jp6Q/7tYJcxXWl2osP9-56-X6pQ/view?utm_co...R1jp6Q&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink
Analysis ID:	458961
Infos:	

Most interesting Screenshot:



Detection

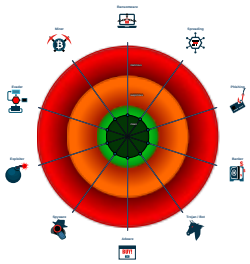


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6624 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.canva.com/design/DAEl-R1jp6Q/7tYJcxXWl2osP9-56-X6pQ/view?utm_content=DAEl-R1jp6Q&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6788 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1508,7393693506506586080,11924844796807865969,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1768 /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

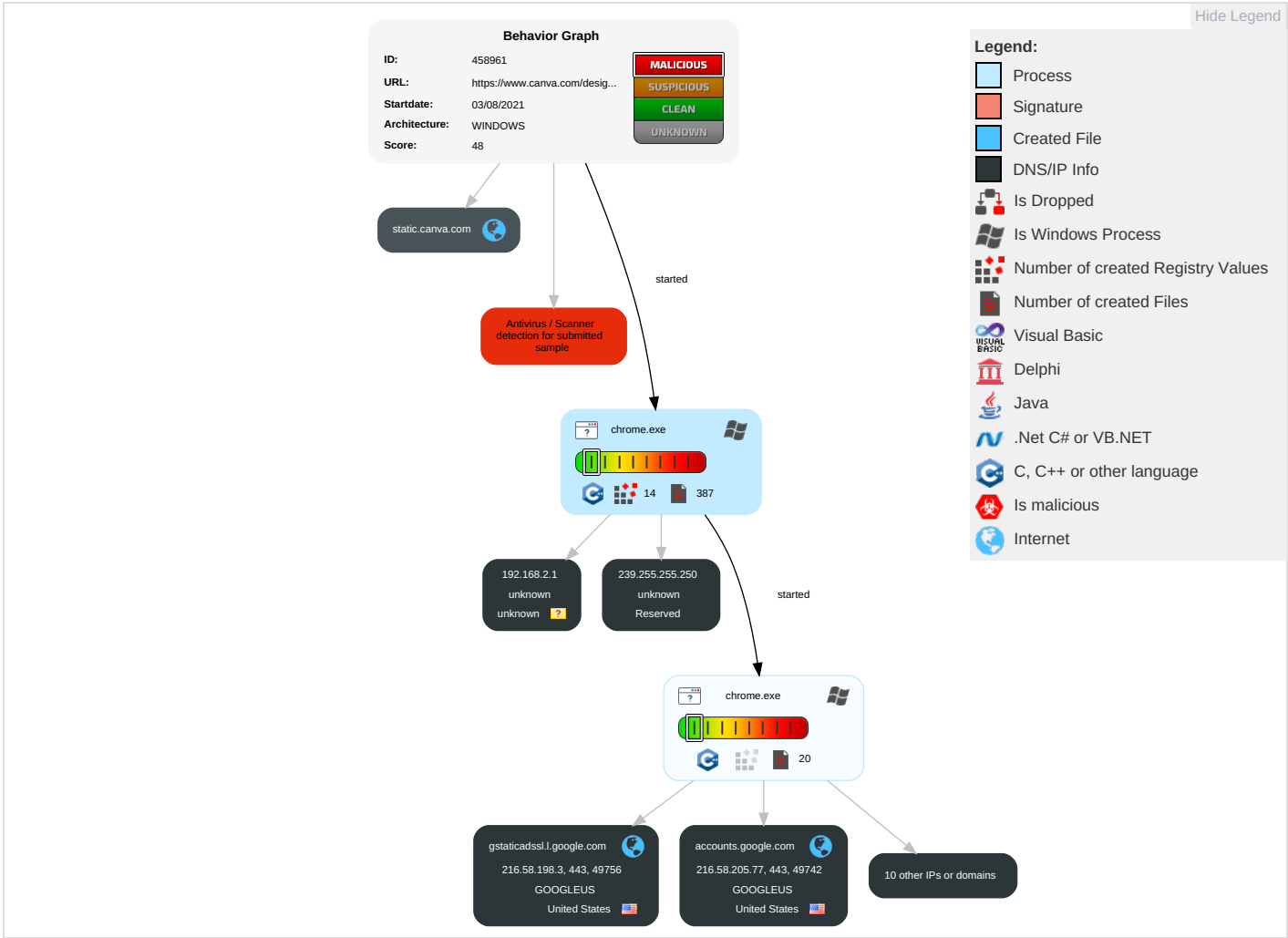
AV Detection:

Antivirus / Scanner detection for submitted sample

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

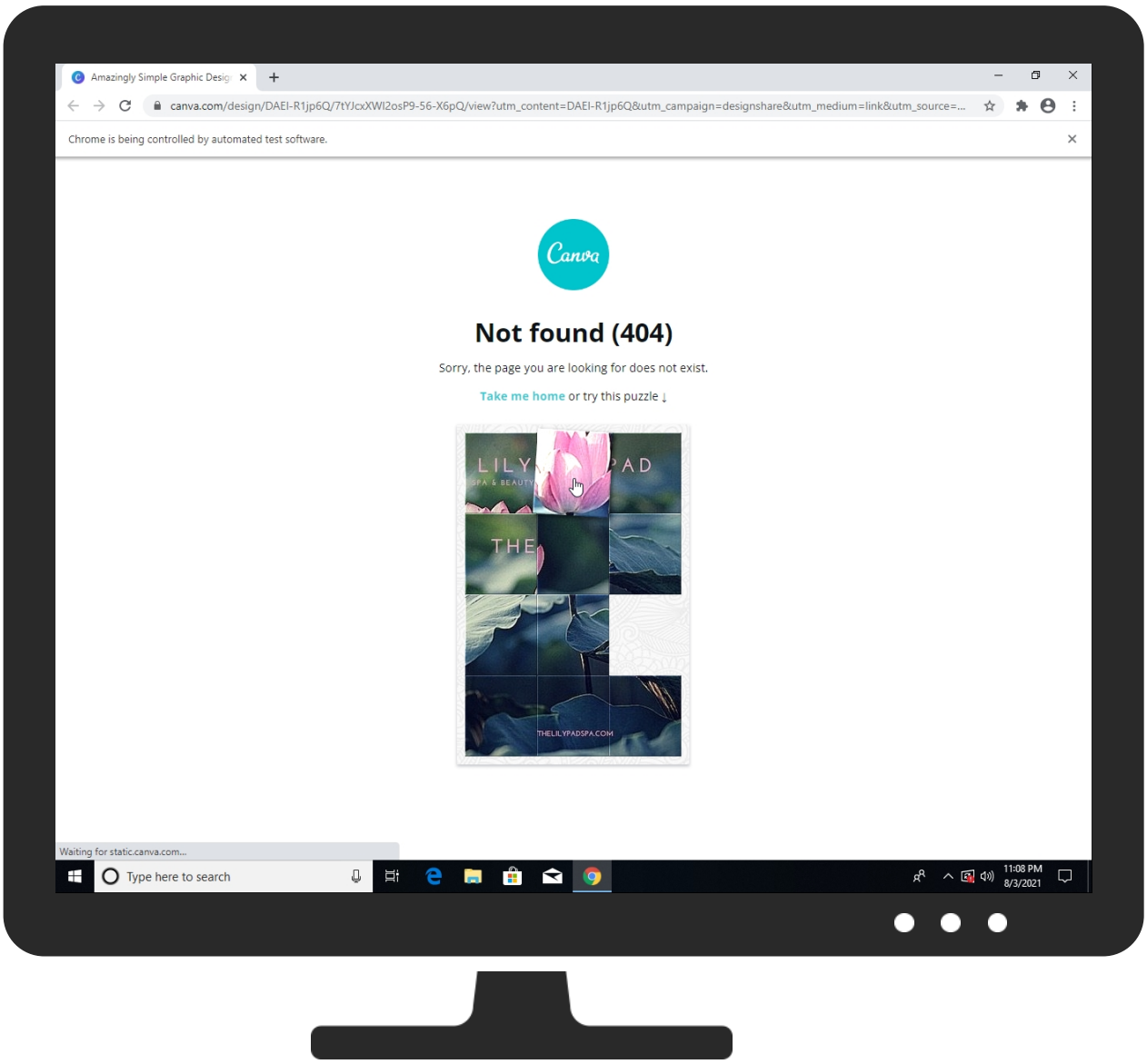
Behavior Graph



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://https://www.canva.com/design/DAEI-R1jp6Q/7tYJcxXWl2osP9-56-X6pQ/view?utm_content=DAEI-R1jp6Q&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	1%	Virustotal		Browse
http://https://www.canva.com/design/DAEI-R1jp6Q/7tYJcxXWl2osP9-56-X6pQ/view?utm_content=DAEI-R1jp6Q&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	0%	Avira URL Cloud	safe	
http://https://www.canva.com/design/DAEI-R1jp6Q/7tYJcxXWl2osP9-56-X6pQ/view?utm_content=DAEI-R1jp6Q&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	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
static.cloudflareinsights.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://static.cloudflareinsights.com/beacon.min.js	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	216.58.198.3	true	false		high
a.nel.cloudflare.com	35.190.80.1	true	false		high
static.cloudflareinsights.com	104.16.94.65	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	216.58.205.77	true	false		high
static.canva.com	104.17.114.17	true	false		high
cl.canva.com	104.17.115.17	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
www.canva.com	104.17.115.17	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.canva.com/design/DAEl-R1jp6Q/7tYJcxXWl2osP9-56-X6pQ/view?utm_content=DAEl-R1jp6Q&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	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
104.17.115.17	cl.canva.com	United States		13335	CLOUDFLARENETUS	false
104.17.114.17	static.canva.com	United States		13335	CLOUDFLARENETUS	false
216.58.198.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
104.16.94.65	static.cloudflareinsights.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458961
Start date:	03.08.2021
Start time:	23:07:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.canva.com/design/DAEl-R1jp6Q/7tYJcxXWl2osP9-56-X6pQ/view?utm_content=DAEl-R1jp6Q&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink
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:	7
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:	mal48.win@28/200@9/11
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

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\0d5a6a19-9bef-46df-a3f5-68cd76013007.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7493235200352872
Encrypted:	false
SSDEEP:	384:7f6JZns+LfoVUN9ruvBr3CVr+Hv6G+BrsPVxxSrzPirQ5mIDMrFF1COv/FNM1dUZ:WO5tC3eewe79zXQH7WfKRf9hV
MD5:	6CAB5FD028151F513DD781C4260024FA
SHA1:	112FB2E6AF9A822C857A05A30A8F4286D9E75CD8
SHA-256:	6CC176BBC13DD92973C838DC137EB8346278BF24994370595E7B3E724C306598
SHA-512:	C0A605670C256CF8F33D0B29B3C94C6768DD48163FF978156D53BDEEA69E3C24939A62FCBC5224D50FFF40959B431D3F16D4B34C854C1116BE545C6B5EBF11A
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....A8.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\3c15b633-f88a-4b73-be51-23868c220e8d.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):	6.079653179585909
Encrypted:	false
SSDEEP:	3072:KLDGaYTJQE+mugy9+QV1T7IRwdfLSNPnFcbXafIB0u1GOJmA3iuRJ:6yxaV+QfT7GSmhFaqfIlUOoSiuRJ
MD5:	88E803F77C180EDF5E08385454B5D050
SHA1:	4F1577D53BF672097D618CFE876A2974947ED039
SHA-256:	11C0A104FA34936DDD98710A68E70808CF34C70A21FD5B4ED07747D1718FDFEE
SHA-512:	5E077EC4C18AC47025CD543DB3D5A5957103251F52357C9C5E632F2B264AB7F95DA393CEDF75EA8AC1F32A3CA856C520BC691A0661EBB51A3054D1C163005B4
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":1.628024893400754e+12,"network":1.628024895e+12,"ticks":6625838171.0,"uncertainty":4772732.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+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\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\32fca649-82ef-4bb7-9d5d-c624b2ed6d19.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):	5761
Entropy (8bit):	5.172221333090952
Encrypted:	false
SSDEEP:	96:nWLRZ9smwlIKIMn5k0JCKL8RkX1xbOTlVuHn:nWLX9TWI8h4KokX5
MD5:	3FFBC0DAFA27F861964761B5B00E794D
SHA1:	AB74D14002E6A72C279D96F135A93DB98CFB150B
SHA-256:	945714D3172B826570F6DBBCBF031109A5CDD55628AD7C8ABAAB4B8613AB93F5
SHA-512:	C0C22E28B943C3E0D3B3A1C590A20C1798872438086A47D7AC7E71D83A0BF2DF17A06E36544FC5CD74439CA7F3527892F1CFEDE312CB584B03547996BB7E91F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272498490627659","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\5f59b313-14ee-4101-b6f2-2625e8f7f9aa.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):	5761
Entropy (8bit):	5.172221333090952
Encrypted:	false
SSDEEP:	96:nWLRZ9smwlIKIMn5k0JCKL8RkX1xbOTlVuHn:nWLX9TWI8h4KokX5
MD5:	3FFBC0DAFA27F861964761B5B00E794D
SHA1:	AB74D14002E6A72C279D96F135A93DB98CFB150B
SHA-256:	945714D3172B826570F6DBBCBF031109A5CDD55628AD7C8ABAAB4B8613AB93F5
SHA-512:	C0C22E28B943C3E0D3B3A1C590A20C1798872438086A47D7AC7E71D83A0BF2DF17A06E36544FC5CD74439CA7F3527892F1CFEDE312CB584B03547996BB7E91F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272498490627659","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\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.121813344763734
Encrypted:	false
SSDEEP:	6:mHuq2Pwkn23iKKdK9RXXTZIFUtpQWUHZZmwPQWUHzkwOwkn23iKKdK9RXX5LJ:fvYf5Kk7XT2FUtpDUHZ/PDUHz5Jf5KkT
MD5:	2C8696A60FEBA04B398AD6D6C0306E13
SHA1:	2B57CFC834845BA9BC15BE59D0BD3B1893FA1C0D
SHA-256:	F1330423EE8BE9C2D0E32A43CDDE75860F4BC622823D1427C6861CB808611D74
SHA-512:	3D9821401311587C5F3332721C6AD1C551DB61015DEAF25B69FC754D8757B015640FD2ED08AFADDB6817A8D1164C03133AE4CC4B30E34D873BA60C28A565F2D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.298 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-23:08:16.300 1a30 Recovering log #3.2021/08/03-23:08:16.300 1a30 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\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.121813344763734
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
SSDEEP:	6:mHuq2Pwkn23iKKdK9RXXTZIFUtpQWUHZZmwPQWUHzkwOwkn23iKKdK9RXX5LJ:fvYf5Kk7XT2FUtpDUHZ/PDUHz5Jf5KkT
MD5:	2C8696A60FEBA04B398AD6D6C0306E13
SHA1:	2B57CFC834845BA9BC15BE59D0BD3B1893FA1C0D
SHA-256:	F1330423EE8BE9C2D0E32A43CDDE75860F4BC622823D1427C6861CB808611D74
SHA-512:	3D9821401311587C5F3332721C6AD1C551DB61015DEAF25B69FC754D8757B015640FD2ED08AFADDB6817A8D1164C03133AE4CC4B30E34D873BA60C28A565F2D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.298 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-23:08:16.300 1a30 Recovering log #3.2021/08/03-23:08:16.300 1a30 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):	5.1394106957500485
Encrypted:	false
SSDEEP:	6:mHLdOq2Pwkn23iKKdKyDZIFUtpQJYZmwPQJAkwOwkn23iKKdKyJLJ:QOvYf5Kk02FUtp//Pt5Jf5KkWJ
MD5:	772272CDA7FA8E8E816FDF8CBBFB673D
SHA1:	522D358874BC284DC93B8852CD1DC7AF1BD23573
SHA-256:	204B8B58CD00BC977C87782F9880A24675EF0F0103C2BC33263806A00F7C196E
SHA-512:	84868099C3BA908FB0213C8F6A57FB9886AE9FD0DB3211CCC284AE3B435D5D1DEBEC623F99E17FE3755CA087E1A0A8BBB669CBA304A71AB58CCD7EB7C3262BAF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.289 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-23:08:16.293 1a30 Recovering log #3.2021/08/03-23:08:16.293 1a30 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\BudgetDatabase\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.1394106957500485
Encrypted:	false
SSDEEP:	6:mHLdOq2Pwkn23iKKdKyDZIFUtpQJYZmwPQJAkwOwkn23iKKdKyJLJ:QOvYf5Kk02FUtp//Pt5Jf5KkWJ
MD5:	772272CDA7FA8E8E816FDF8CBBFB673D
SHA1:	522D358874BC284DC93B8852CD1DC7AF1BD23573
SHA-256:	204B8B58CD00BC977C87782F9880A24675EF0F0103C2BC33263806A00F7C196E
SHA-512:	84868099C3BA908FB0213C8F6A57FB9886AE9FD0DB3211CCC284AE3B435D5D1DEBEC623F99E17FE3755CA087E1A0A8BBB669CBA304A71AB58CCD7EB7C3262BAF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.289 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-23:08:16.293 1a30 Recovering log #3.2021/08/03-23:08:16.293 1a30 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\56e67e1a4a50be0f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.428804165772863
Encrypted:	false
SSDEEP:	3:m+le6zt6v8RzYkwLTLTikBGKE+xtMNLuFvDCLTEQCatlHCi9UG0UitxDH//sYghb:m48EYk+TFs+xCNeQJSWUGO/YPK6t
MD5:	F1835047CFD68AA350B1CC21B036A0F4
SHA1:	701FDF703A5F3F12BEA68A897011B9D879F3E0BE
SHA-256:	E560352886BBFAC585240E27629D834050ED7B9686C9149967C00790FC929285
SHA-512:	4E206C99EA3FB2448DC26A368C33ECE85CE65BB80E7BE3387E3CA88BF3B345219CD9E3CE6E6C65C8E5ADC9696C45560134656CE4C631282EEB7DD82522143E1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\56e67e1a4a50be0f_0	
Preview:	0\r..m.....N....(....._keyhttps://static.canva.com/static/lib/cl/cl-0.4.3.min.js .https://canva.com/..^D'/.....y]w..eBZ[.Q[.$.87..".]Z.."m`...A..Eo.....M6_.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6e7f394632e47430_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.49211758457332
Encrypted:	false
SSDEEP:	6:miUPYk+TFsOg16gDr9SZGI2ZHGyPahZK6t:ub+TuOa67GLvap
MD5:	CD9AABCD09EBAE15DA3A38C042A51958
SHA1:	05F26AAA75769961FF100FDE5F13E11C0DA8DE9C
SHA-256:	A8CBA91423A997F47E461BF252E112C8FC62F9E56190C21A885456C613D2A69A
SHA-512:	12AD053C730A9F483C885185DDF77F40E202B29D3C46638ED3E53BE8E3CE6985EDDD8B33C4EBEC435004E5EC78E58697489450E593B5F63E7437F7FBFBD2D86 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....E...._keyhttps://static.canva.com/static/lib/segment-snippet-4.1.0.min.js .https://canva.com/7..^D'/.....<.....<yz..l'.8.C)iU.b....8..(.....RP..A..Eo.....X..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8bf0835732d01051_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.523389652894842
Encrypted:	false
SSDEEP:	6:mPXXYk+TFskmfLPWNtSP0yx/IT/ufm4NgJhK6t:CD+TuTzWNy09/lN
MD5:	3CF0198E2541B543329FD67C893C7AE0
SHA1:	464256BF35207DCAC34F1BE85424ACEC9631CFAF
SHA-256:	31B4451CC8DD767D41515C67820CEAADA74CE962A299D8776FFC4C5A8BE9018D
SHA-512:	F76438F005DAE0F7110F7683AFC9332C3E7F6AFF6B8954C47861898B0A830692A761BEE91FD9930198B13A48E644E5FB7AEEC88442874708EDB71576B94B913F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...m..Y...._keyhttps://static.canva.com/static/lib/jquery-1.8.3.min.2.js .https://canva.com/._^D'/.....;.....md.Z...T...l.{%^.....(.:..A..Eo.....B.(.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8e98f4b7848fbe37_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.482462164085635
Encrypted:	false
SSDEEP:	3:m+ljXls8RzYkwLeLJKtHhdLLxHWFvDCLTE9ep9tlHCCvROiS3lgw7H5mOz/lpK5M:mKnYk+6KHH6uSqRir4ybK6t
MD5:	3A1835E63A1195BE815E47BCB684136B
SHA1:	BBD920A3434A83DFDDF63D9BF411B5308F9D1313
SHA-256:	2785E503BB739A73E6A77EFDF86AC1105A374B2124EF1A6B02AD8EE6C55F9E44
SHA-512:	93AB0285C8B37A3A20A624F6E78305532BA01279E79336007D20178B07F1FEDE35A3584FB358CBD70721CEF984F752043C9AFEAAC7FF1538F8E47F03CE25D479
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K.....1...._keyhttps://static.cloudflareinsights.com/beacon.min.js .https://canva.com/..^D'/.....4.....3.`O..X.LC..3.b...L"..A..Eo.....u.....A..Eo..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99de76cda7e7f6ae_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.452211396882697
Encrypted:	false
SSDEEP:	6:msHTqEYk+TFs/BmAaVSHlWYHP4mlbK6t:BzD+Tu/BmAa/WYvzN

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99de76cda7e7f6ae_0	
MD5:	9580C79ED9ED5445FE41C5B2E9A152BA
SHA1:	3320982C1D0656CE95B269C3159BE5BC7E527498
SHA-256:	6751FE758FE04FC35C71DAF8D678F31C64D1B1EF01DA0DE22C698854000857A9
SHA-512:	6CA199A475A0A26DC437A45E10BAFE8C4E7E240D9FBE4877914F3DAB83F728D295060FC2A4A0A3F207EB9BED5DBD0853675E6CD107F43917BC3C3C91F4866BF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...G.@6...._keyhttps://static.canva.com/static/lib/underscore-1.8.3.min.js .https://canva.com/.I.^D'/.....b./Fd..D{....w.....s^..yS.A..Eo.....'.v.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a56ee0ddb5db651b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.405583251755372
Encrypted:	false
SSDEEP:	6:mzlXYk+TFs00IMaHSZtaqBfz/PzhmDK6t:Mz+TuVIvspz/PzI
MD5:	5AAAEDC379629DF68E017A21E797EC95
SHA1:	38D30D072E0D17BD1AC3F7246B21AD903296C9D6
SHA-256:	88E4FFAF74684458A0EDFE124735E78D766107FA7BE8AB98FF59FC10D6D98535
SHA-512:	60B8F23E337AA760EC32EC1D8EBD1C469EA74C229A332B1279751ABA45756BEA5CE6CD4745467A8D5F91DACBB11130E41BB5F774F89AC3C6279BF63D7CCE7BEB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...L.!-...._keyhttps://static.canva.com/static/lib/bluebird-2.3.11.min.js .https://canva.com/>..^D'/...../.....e..h!%.K.....>>..1md..A..Eo.....'C.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dc3751d27b8cbd66_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.6300151185611265
Encrypted:	false
SSDEEP:	6:mVtXYk+TF0VEJVUWfJaeXaSXgHA9/XlthK6t:qz+T9PoeZgHgl1
MD5:	726282D7DA2EE4BFC81D900584AA161E
SHA1:	AF9A0885EEE32E95EAF7E1405AFDA2045B555E63
SHA-256:	3ACB33BA60DE62041E99195391FD9E0DC9F8201A69920CFC9880B7B71E33527A
SHA-512:	39CF05974E78FA19C26D7A67DBF9A4728C8B507155805710D71523B1430432566470AF5588C5944D1F8CAC225839E518C0A092924E566D4F36FD5797DF44AADF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...>..&...._keyhttps://static.canva.com/static/r/20210803-02/js/23BzzNosJDRE06_zR1W5uA.js .https://canva.com/k..^D'/.....C.%..I..j..c.K..Q..K ../.4....A..Eo.....A..Eo.....

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):	408
Entropy (8bit):	5.006558182837582
Encrypted:	false
SSDEEP:	3:XFXTZnlHlgVtelr7p23Kl7hrQMhhC+/o27U+AQ2A5C+z9IptllFzfyu7/lOptlo:83A43KllJh1rAccTxzPawAfyDnB
MD5:	6FD45A89AD74B79CB9B523FF2D489669
SHA1:	EC5BEAB9C24947097A6F3380ED6CB7ABE67E9BB5
SHA-256:	1F0248ECCA466A90B4F6A96E2F5E3B38D8E7810C4ED8567FFECEDBA647354B3B
SHA-512:	9F30D349CE0EAC0B92797677E3A3F217E35065870E7D80F73434124F3C924E341CBF9E618A47C3D9B7841E56AE41EFF82A6B24F55238970DD98E01DD94AC402B
Malicious:	false
Reputation:	low
Preview:	.....K.oy retne.....PJ.~.V...^D'/.....7.....^D'/.....f..{.Q7....^D'/.....v....^D'/.....Q..2W.....^D'/.....e...n....^D'/.....^}.Np....4&../.....0t.2F9.n...^D'/.....-..0..x..4&../...../...3...&../.....I....uW...&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../..... ^D'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.006558182837582
Encrypted:	false
SSDEEP:	3:XFXTZnlHlgVtelr7p23Kl7hrQMhhC+/o27U+AQ2A5C+z9lptlllFzfyu7/lOptlo:83A43KllJh1rAccTxzPawAfyDnB
MD5:	6FD45A89AD74B79CB9B523FF2D489669
SHA1:	EC5BEAB9C24947097A6F3380ED6CB7ABE67E9BB5
SHA-256:	1F0248ECCA466A90B4F6A96E2F5E3B38D8E7810C4ED8567FFECEDBA647354B3B
SHA-512:	9F30D349CE0EAC0B92797677E3A3F217E35065870E7D80F73434124F3C924E341CBF9E618A47C3D9B7841E56AE41EFF82A6B24F55238970DD98E01DD94AC402B
Malicious:	false
Reputation:	low
Preview:	......K.oy retne.....PJ.~.V...^D'/.....7.....^D'/.....f..{.Q7....^D'/.....v....^D'/.....Q..2W.....^D'/.....e...n....^D'/.....^}.Np....4&../.....0t.2F9.n...^D'/ .....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../..... ^D'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	1.9240349685252378
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7U05H5mwi+pE1pLFKtS9x37RDiYg76m:dNwI6+AGuiYU
MD5:	1D0332886C7D41BE7A7A172AB31C25D2
SHA1:	5BE3500AA81B658EB4FA70D80C6F38AFE5536B35
SHA-256:	9331A3D598561DAFCC5A169DDF8F84AE18D13B9AB4B56EE959C4EEF9B3774EC2
SHA-512:	22CBCD2895D9CCF813C53DEC5C8501438AB1827264515121C0341E244AE763776C2CC3D1916624AB42460EA3874AC49D977C9FAD489CF8DC0CF0573D346370
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):	12836
Entropy (8bit):	0.9732816643636266
Encrypted:	false
SSDEEP:	24:xe9H6pf1H1oNrqLbJLbXaFpEO5bNmISHn06UwD8:xbfvoNrq5LLOpEO5J/Kn7U08
MD5:	587EC07634E82326348FA46BE8B551E4
SHA1:	FC6FF884DCF7468B7C37349FA20CB89CE4AB68A7
SHA-256:	9A5DB6E5207894C0C7CA06DF2FEC960B931EFFD69436D82CB36288B08661A326
SHA-512:	AA6E57A57C619019CC62A77C9381944964CF008BD6466A8C1BF78C23C5C56A88ED50EE7D841A4363F5AB577B03A7951B3CA145C97FD33223FC73797EB875806
Malicious:	false
Reputation:	low
Preview:	....

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):	1477
Entropy (8bit):	4.121054567117228
Encrypted:	false
SSDEEP:	24:34SIQlrlJ44nRhUuV1gPsnLSl3zB+AkZ6HWBvW3HD+pIk4nRhUuWlLlL:34exlnRpXQsLW1+/6HJjLznRpiRL
MD5:	B3EF434EFC08D9D715F2BA0144C010B2
SHA1:	65DBC5B4DC48F4A2A667E60BFB9E2EF324C434B0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
SHA-256:	ACF126AFEE0D9C61D03749D6B24018911C670D2825E90B154155113FE5737785
SHA-512:	A7C8B61950D90B0AF8D2510EAE364822199C314C6CA666228AB4CEDE4ED0B64683601DA111649C113163B4ECFA4372150EC47D14B907CB40DCAA3838F750DDI 9
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...39318eda_dca5_4a99_981f_6581e616bd4f..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....A..<.....https://www.canva.com/design/DAEl-R1jp6Q/7tYJcxXWl2osP9-56- X6pQ/view?utm_content=DAEl-R1jp6Q&utm_campaign=designshare&utm_medium=link&utm_source=publishshare link.....h.....`..... .....J.....h.t.t.p.s.:././.w.w.w...c.a.n.v.a...c.o.m./.d.e.s.i.g.n./.D.A.E.l.-.R.1.j.p.6.Q./.7.t.Y.J.c.x.X.W.l.2.o.s.P.9.-.5.6.- .X.6.p.Q./.v.i.e.w.?.u.t.m._.c.o.n.t.e.n.t.=.D.A.E.l.-.R.1.j.p.6.Q.&.u.t.m._.c.a.m.p.a.i.g.n.=.d.e.s.i.g.n.s.h.a.r.e.&.u.t.m._.m.e.d.i.u.m.=.l.i.n.k.&.u.t.m._.s.o.u.r.c.e.=.p.u.b.l.i.s.h .s.h.a.r.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.142951972228125
Encrypted:	false
SSDEEP:	6:mBRLS+q2Pwkn23iKKdK8aPrqIFUtpWlZmwPWX63VkwOwkn23iKKdK8amLJ:mk+vYf5KkL3FUtpWl/PWXmV5Jf5KkQJ
MD5:	DCEF2C4103B7A0E7426342932CE08246
SHA1:	5AFC3CBBA0A30D3A15A35D9C415FA9F0BBCAF648
SHA-256:	CF4D8904323975F75BD9766244A84E0C30CC50912008C7DBCED5DE2CADEF0924
SHA-512:	984B9BE2BDEF3DC1A666963CE29E973714500CBB10A3886E4B86C0766A606E69FFF054006CE7F0B8C26E4BF10D988F5478CED51C4A603072C728C3C59BE136A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.633 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-2 3:08:10.634 1a2c Recovering log #3.2021/08/03-23:08:10.635 1a2c 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):	5.142951972228125
Encrypted:	false
SSDEEP:	6:mBRLS+q2Pwkn23iKKdK8aPrqIFUtpWlZmwPWX63VkwOwkn23iKKdK8amLJ:mk+vYf5KkL3FUtpWl/PWXmV5Jf5KkQJ
MD5:	DCEF2C4103B7A0E7426342932CE08246
SHA1:	5AFC3CBBA0A30D3A15A35D9C415FA9F0BBCAF648
SHA-256:	CF4D8904323975F75BD9766244A84E0C30CC50912008C7DBCED5DE2CADEF0924
SHA-512:	984B9BE2BDEF3DC1A666963CE29E973714500CBB10A3886E4B86C0766A606E69FFF054006CE7F0B8C26E4BF10D988F5478CED51C4A603072C728C3C59BE136A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.633 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-23:08:10.634 1a2c Recovering log #3.2021/08/03-23:08:10.635 1a2c 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
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.....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):	5.127441414884562
Encrypted:	false
SSDEEP:	6:mDi70yq2Pwkn23iKKdK8NIFUtpUiuz1ZmwPUiLRkwOwkn23iKKdK8+eLJ:npvYf5KkpFUtpiz1/PB5Jf5KkqJ
MD5:	0EB026B4A80428C858227C36F9FEEA84
SHA1:	9BE013DDE2508E507C1D6F16AAC28E039897FDD3
SHA-256:	BB14B16D51776BC778926E03D952A568F3C0FBBD8039DCEFAE7635C41A3DB1AC
SHA-512:	E613E04C142438140DF77692A75C75CDF63F4B7D5CA9A6285085B7FB751C1101693444800B1B706EBDD01344FC4BED7243CE824DBDF6B0188E15255B497E03F3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:12.702 1aa4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-23:08:12.704 1aa4 Recovering log #3.2021/08/03-23:08:12.707 1aa4 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:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/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:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","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):	22528
Entropy (8bit):	2.047275582732791
Encrypted:	false
SSDEEP:	48:XBmw6fUiRLnRpJvtnRp08r8wBj1wdrlRWBCoN0hRdslhWntdwLXKvkj7T9:XBCnR7RpJvBRp0KZjGTBhiktdwwkfT9
MD5:	AC62EB0B8FE7C31EB65F01A4E0B2F4F1
SHA1:	E10B7383A71240348D9641A60E794CA2984CB029
SHA-256:	5F41C40869D6177EA8F159E2BEE2DDC0A3208FDE2BC338357F653E24E06E2BE4
SHA-512:	5113705588C411640E05506A4F179FB16E493092145479E27E346B4869B67FE695E748E3B6281EAE2F8DDC3EB36DF6C29F574CA5789DB6B1080591E1E53DFED7
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):	19028
Entropy (8bit):	0.7403777880648093
Encrypted:	false
SSDEEP:	24:qKA6lcyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6UwE0CasQpu2:dcCBmw6fUXV2
MD5:	EC743517C744EFD443A3FEAEDD8CB8D8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
SHA1:	DB1C0B7AAFBDB439554ECE6D9AC2A59B65350553
SHA-256:	0E3722CA3A51497B46CA71174C0799026EE66C3CAFB27F9E2F38DBBBFE597CBA
SHA-512:	CB722CAE8F68CB9C246F986BBB62A00255AD0D578D3FA03805C93ABB74019C7573438E3E9130B99D141DBC4DD214B4A3C48EF74FC0ED785461EDAFD21E7CF4C6
Malicious:	false
Reputation:	low
Preview:	.....#I..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.219100920287011
Encrypted:	false
SSDEEP:	6:mHkIq2Pwkn23iKKdK25+Xqx8chI+IFUtpQPWhZmwPQPW7kwOwkn23iKKdK25+Xqp:UvYf5KkTXfchI3FUtpOS/POe5Jf5KkTM
MD5:	11ED46CAC6798462D27AF7ADFD63CBCF
SHA1:	555297988E2203FE51032ADFB792C231A556F2A5
SHA-256:	FB3EA3466182D1B5571BDA6BC26375D01C1C7930E69E33FB8C8ADF5B8F8F15C4
SHA-512:	7C136028D3B619E1AE4ACE92F1D76F9F59B23D52EA058F54D1C818301463A5D5F7F8955C9A5FC5FB86433CD445FCF3B79FF6A9D040D6268052BA9C45EF684C8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.277 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-23:08:16.279 1a30 Recovering log #3.2021/08/03-23:08:16.279 1a30 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\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.219100920287011
Encrypted:	false
SSDEEP:	6:mHkIq2Pwkn23iKKdK25+Xqx8chI+IFUtpQPWhZmwPQPW7kwOwkn23iKKdK25+Xqp:UvYf5KkTXfchI3FUtpOS/POe5Jf5KkTM
MD5:	11ED46CAC6798462D27AF7ADFD63CBCF
SHA1:	555297988E2203FE51032ADFB792C231A556F2A5
SHA-256:	FB3EA3466182D1B5571BDA6BC26375D01C1C7930E69E33FB8C8ADF5B8F8F15C4
SHA-512:	7C136028D3B619E1AE4ACE92F1D76F9F59B23D52EA058F54D1C818301463A5D5F7F8955C9A5FC5FB86433CD445FCF3B79FF6A9D040D6268052BA9C45EF684C8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.277 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-23:08:16.279 1a30 Recovering log #3.2021/08/03-23:08:16.279 1a30 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):	5.145839065546361
Encrypted:	false
SSDEEP:	6:mHDOq2Pwkn23iKKdK25+XuoIFUtpQpFZZmwPQFKkwOwkn23iKKdK25+XuxWLJ:iOvYf5KkTXYFUtp4/PSK5Jf5KkTXHJ
MD5:	14738518DA6F03584D833C8A030A6305
SHA1:	BF5C7992B5A628CA0CE168E09647661916519FAD
SHA-256:	A68616AA8786BA513DCBBFFF5C9D63FF140B4758D10D9AB04D9E2B54AADB6BD3
SHA-512:	CDFE987BA2354567FC4EE1A21E75EC056F2A96C115D55C745DE377911DE8ECFB0B1187D6F271A96995DB0CC34BE780F5D7D8E27C234162E62B6DEEA8E63346E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.261 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-23:08:16.267 1a30 Recovering log #3.2021/08/03-23:08:16.268 1a30 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\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.145839065546361
Encrypted:	false
SSDEEP:	6:mHDOq2Pwkn23iKKdK25+XuoIFUtpQpFZZmwPQFKkwOwkn23iKKdK25+XuxWLJ:iOvYf5KkTXYFUtp4/PSK5Jf5KkTXHJ
MD5:	14738518DA6F03584D833C8A030A6305
SHA1:	BF5C7992B5A628CA0CE168E09647661916519FAD
SHA-256:	A68616AA8786BA513DCBBFFF5C9D63FF140B4758D10D9AB04D9E2B54AADB6BD3
SHA-512:	CDFE987BA2354567FC4EE1A21E75EC056F2A96C115D55C745DE377911DE8ECFB0B1187D6F271A96995DB0CC34BE780F5D7D8E27C234162E62B6DEEA8E63346E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.261 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-23:08:16.267 1a30 Recovering log #3.2021/08/03-23:08:16.268 1a30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.160019812062262
Encrypted:	false
SSDEEP:	6:mHIq2Pwkn23iKKdKWT5g1IdqIFUtpQniZZmwPQyUESFkwOwkn23iKKdKWT5g1I3e:RvYf5Kkg5gSRFUtpBZ/PlSF5Jf5Kkg5i
MD5:	20F2B0433BCEECD153700EAD5E808F61
SHA1:	7E4CB3FB1F4E3606299FCA3C55D869B02F43865E
SHA-256:	84C68185EEDC7FDE310DF3DEDBA0CD48DE98D5043CC9FBCE65D1D02E26C541C0
SHA-512:	304F9FD8DDF852E1E30BD7454C241A1BAF82B06FB64DC5D51099B9CFAF78DA08548B8E0BC6F5B1F713F6F27F3D7B27BD8E51A9DD13C98B9A24BC3E1D1DCE2C8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.238 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-23:08:16.240 1a30 Recovering log #3.2021/08/03-23:08:16.241 1a30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.160019812062262
Encrypted:	false
SSDEEP:	6:mHIq2Pwkn23iKKdKWT5g1IdqIFUtpQniZZmwPQyUESFkwOwkn23iKKdKWT5g1I3e:RvYf5Kkg5gSRFUtpBZ/PlSF5Jf5Kkg5i
MD5:	20F2B0433BCEECD153700EAD5E808F61

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
SHA1:	7E4CB3FB1F4E3606299FCA3C55D869B02F43865E
SHA-256:	84C68185EEDC7FDE310DF3DEDBA0CD48DE98D5043CC9FBCE65D1D02E26C541C0
SHA-512:	304F9FD8DDF852E1E30BD7454C241A1BAF82B06FB64DC5D51099B9CFAF78DA08548B8E0BC6F5B1F713F6F27F3D7B27BD8E51A9DD13C98B9A24BC3E1D1DCE2C8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.238 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-23:08:16.240 1a30 Recovering log #3.2021/08/03-23:08:16.241 1a30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session0 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1477
Entropy (8bit):	4.121054567117228
Encrypted:	false
SSDEEP:	24:34SIQlrlJ44nRhUuV1gPsnLSl3zB+AkZ6HWBvW3HD+pIk4nRhUuWlLlL:34exlnRpXQsLW1+/6HJjLznRpiRL
MD5:	B3EF434EFC08D9D715F2BA0144C010B2
SHA1:	65DBC5B4DC48F4A2A667E60BFB9E2EF324C434B0
SHA-256:	ACF126AFEE0D9C61D03749D6B24018911C670D2825E90B154155113FE5737785
SHA-512:	A7C8B61950D90B0AF8D2510EAE364822199C314C6CA666228AB4CEDE4ED0B64683601DA111649C113163B4ECFA4372150EC47D14B907CB40DCAA3838F750DD9
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...39318eda_dca5_4a99_981f_6581e616bd4f.....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....A..<.....https://www.canva.com/design/DAEl-R1jp6Q/7tYJcxXWl2osP9-56-X6pQ/view?utm_content=DAEl-R1jp6Q&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink.....h.....`.....J.....h.t.t.p.s.:././.w.w.w...c.a.n.v.a...c.o.m./.d.e.s.i.g.n./.D.A.E.l.-.R.1.j.p.6.Q./.7.t.Y.J.c.x.X.W.l.2.o.s.P.9.-.5.6.-.X.6.p.Q./.v.i.e.w.?.u.t.m._.c.o.n.t.e.n.t.=.D.A.E.l.-.R.1.j.p.6.Q.&.u.t.m._.c.a.m.p.a.i.g.n.=.d.e.s.i.g.n.s.h.a.r.e.&.u.t.m._.m.e.d.i.u.m.=.l.i.n.k.&.u.t.m._.s.o.u.r.c.e.=.p.u.b.l.i.s.h.s.h.a.r.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last TabsOC (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\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3860
Entropy (8bit):	5.5997729135943874
Encrypted:	false
SSDEEP:	48:UZ7AWXOCS5Gtha7dMI8db3yCabQSefgGjNrS0U9RdiN93:GNLLa7dMDdb3yCabQ5fgGxrS0F
MD5:	3044E15FF85B13E7DCD1E7E193573EF3
SHA1:	864E5A4063EA08207A2850E1CE603F910499FB83
SHA-256:	0DFB57641DEC269E11DDACFD056E75D3B19AA27DE1B7F52EBAC32E9BE8CB79DC
SHA-512:	15B0EAC9BD8C6712E6C3694EA44F1DFE2D0AB7911148D80F20148DB221AAD2D843303FEBFB4B7230EC5B9340F00B26CD660EE0CB1D8B80C91607C30D77A26D2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Preview:	.p{....*.....META:https://www.canva.com.....(_https://www.canva.com..ajs_anonymous_id'."7a374aa8-47d7-4585-ab14-4226448bfe25".$_https://www.canva.com..ajs_group_id..null.,_https://www.canva.com..ajs_group_properties..{}.#_https://www.canva.com..ajs_user_id..null.'_https://www.canva.com..ajs_user_traits..{}.._https://www.canva.com..debug..undefined.J_https://www.canva.com..segmentio.a9d48755-3dba-454b-bd88-08949c8b3caf.ack..1628024899892.Q_https://www.canva.com..segmentio.a9d48755-3dba-454b-bd88-08949c8b3caf.inProgress..{}.L_https://www.canva.com..segmentio.a9d48755-3dba-454b-bd88-08949c8b3caf.queue..[].Q_https://www.canva.com..segmentio.a9d48755-3dba-454b-bd88-08949c8b3caf.reclaimEnd..null.S_https://www.canva.com..segmentio.a9d48755-3dba-454b-bd88-08949c8b3caf.reclaimStart..null.<_https://www.canva.com..70b0ce3f-6536-4d02-8279-3f0d769a5698.#_https://www.canva.com..__storejs__.k.{...8.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_ch

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):	5.1217414530838585
Encrypted:	false
SSDEEP:	6:mBgUEN+q2Pwkn23iKKdK8a2jMGIFUtpWcZmwPWFNVkwOwkn23iKKdK8a2jMmLJ:mgUEIvYf5Kk8EFUtpWc/PWN5Jf5Kk8bJ
MD5:	1F4E44EFFD916C9382F03F7F2C60E528
SHA1:	21BAA1571A627E96DA33807AAE76D57D73C8C48E
SHA-256:	7A469D5AB5BD6181724B8033FBEDF382BDF21B57282D9EF6BE540BEEAF80BD88
SHA-512:	82E6C71B02F8309F9E48D98AA6FBE989B021FA00CD1507F5BF27908CCBCDACC8FE847E9292A3C73A00BB997AA1BB24C32C7BD6602962DBCA0F526E6D54F9AF77
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.427 1ab8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:08:10.430 1ab8 Recovering log #3.2021/08/03-23:08:10.431 1ab8 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):	332
Entropy (8bit):	5.1217414530838585
Encrypted:	false
SSDEEP:	6:mBgUEN+q2Pwkn23iKKdK8a2jMGIFUtpWcZmwPWFNVkwOwkn23iKKdK8a2jMmLJ:mgUEIvYf5Kk8EFUtpWc/PWN5Jf5Kk8bJ
MD5:	1F4E44EFFD916C9382F03F7F2C60E528
SHA1:	21BAA1571A627E96DA33807AAE76D57D73C8C48E
SHA-256:	7A469D5AB5BD6181724B8033FBEDF382BDF21B57282D9EF6BE540BEEAF80BD88
SHA-512:	82E6C71B02F8309F9E48D98AA6FBE989B021FA00CD1507F5BF27908CCBCDACC8FE847E9292A3C73A00BB997AA1BB24C32C7BD6602962DBCA0F526E6D54F9AF77
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.427 1ab8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:08:10.430 1ab8 Recovering log #3.2021/08/03-23:08:10.431 1ab8 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 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):	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):	334
Entropy (8bit):	5.146204386404425
Encrypted:	false
SSDEEP:	6:mBQfyq2Pwkn23iKKdKgXz4rRIFUtpWC1ZmwPWO+RkwOwkn23iKKdKgXz4q8LJ:m/vYf5KkgXiuFUtpWC1/PWl5Jf5KkgXS
MD5:	C5010BACC3288B5B2DE51ACBB163986F
SHA1:	98A0146A082F13D0EDCAB3D448A4FC1B78C06B28
SHA-256:	7AC60F819426BA8C41BA03D88B7F5F45C5CF619375A295202B180328652A6FB4
SHA-512:	5EBAA1B9AA04EC8F1FC039918D9D6F15B17E61E5F52D369628C71B5ED4453782DC94C50CA27B84B3F98AB1734F509ADBA03BF41EEAFDED32D7F711AB26DAC54
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.660 1aa4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-23:08:10.662 1aa4 Recovering log #3.2021/08/03-23:08:10.663 1aa4 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.146204386404425
Encrypted:	false
SSDEEP:	6:mBQfyq2Pwkn23iKKdKgXz4rRIFUtpWC1ZmwPWO+RkwOwkn23iKKdKgXz4q8LJ:m/vYf5KkgXiuFUtpWC1/PWl5Jf5KkgXS
MD5:	C5010BACC3288B5B2DE51ACBB163986F
SHA1:	98A0146A082F13D0EDCAB3D448A4FC1B78C06B28
SHA-256:	7AC60F819426BA8C41BA03D88B7F5F45C5CF619375A295202B180328652A6FB4
SHA-512:	5EBAA1B9AA04EC8F1FC039918D9D6F15B17E61E5F52D369628C71B5ED4453782DC94C50CA27B84B3F98AB1734F509ADBA03BF41EEAFDED32D7F711AB26DAC54
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.660 1aa4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-23:08:10.662 1aa4 Recovering log #3.2021/08/03-23:08:10.663 1aa4 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):	5761
Entropy (8bit):	5.172221333090952
Encrypted:	false
SSDEEP:	96:nWLRZ9smwlIKIMn5k0JCKL8RkX1xbOTlVuHn:nWLX9TWI8h4KokX5
MD5:	3FFBC0DAFA27F861964761B5B00E794D
SHA1:	AB74D14002E6A72C279D96F135A93DB98CFB150B
SHA-256:	945714D3172B826570F6DBBCBF031109A5CDD55628AD7C8ABAAB4B8613AB93F5
SHA-512:	C0C22E28B943C3E0D3B3A1C590A20C1798872438086A47D7AC7E71D83A0BF2DF17A06E36544FC5CD74439CA7F3527892F1CFEDE312CB584B03547996BB7E91F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272498490627659","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\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	28672
Entropy (8bit):	1.285010816594928
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
SSDEEP:	96:wIElwQF8mpcSb0l0sFDn+CxwfxzIlmvaQ:wIElwQF8mpcSU0mDve6mCQ
MD5:	F47C6A89B3DD7A87BFC96E2DB36ECFF5
SHA1:	FBE428431F6D27B962E3E2A1F45CEC40F7A21889
SHA-256:	817CF0FF4FEA5BF72405E88F56E1B92952DF3B7F5D8A7A849E155F7EFC875C6F
SHA-512:	1A933C7BFAA9D2B872685857A8BE9A1BFA91E35B2732BE156EB929E2893578985B0569313B06EC6D820AB9BB1FD428A4EBFF8CBD4CE7E5E7D4C82FCB972C28F4
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6287059557733143
Encrypted:	false
SSDEEP:	48:68qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUN4:68hIElwQF8mpcS+
MD5:	14068C856A050F0BFED5C1ACC4AFDB0E
SHA1:	EDB88E9778B4FF243F03BF963BCEE6E249A67A06
SHA-256:	F48979D642FC5227B964A26CE2DC596D68D02355CEE31556CC7075B49F48BB30
SHA-512:	4A9714D7ECEC0E902989FD35C08B80C63A480670F658D4826F91FF46BC516BE1ABDEE2951B96FD741479AC5C300C4C10D952D5DE6441B560BB1C31C1D64E43
Malicious:	false
Reputation:	low
Preview:	

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):	22600
Entropy (8bit):	5.536649153467188
Encrypted:	false
SSDEEP:	384:fubtGLlEwXh1kXqKf/pUZNCgVLH2HfD0rUXHGQnZ0l548:5LlXh1kXqKf/pUZNCgVLH2HforU3GQn8
MD5:	081DD7E245C121C86ACEA4C2F3BD2002
SHA1:	26C698D1667E95D8DCF00559FB4695B3C4EAC111
SHA-256:	1C4E90B423E0409B1C9A7D7E98B1755D0FAF413325A9AB401039579D08EA5535
SHA-512:	C1B30A7D4CCE040F0A68BF6AD5CB8E895E0D8D24E1764FAA932F51663904C752146F907C8D3DF0F01D222074A2031CC7A7088D29EF9DF9BDC217BF5CF4218AE
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":"13272498490361007","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\Secure Preferenceswe (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):	22602
Entropy (8bit):	5.536658263462912
Encrypted:	false
SSDEEP:	384:fubt/LlEwXh1kXqKf/pUZNCgVLH2HfD0rUXHGTnZWZ2543:CLlXh1kXqKf/pUZNCgVLH2HforU3GTnO
MD5:	13EAD9467F27511A71F3CA1875A260E1
SHA1:	ED5523F3C4837503AF8F14DEC723AC833030FFE6
SHA-256:	C9FB29E57340574909DF7EC3C08827EBC489EDBB06528141817FB8F2AF4D8A6C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferenceswe (copy)	
SHA-512:	237E401327DA1FC470C569BAA11B82E3B813EFDEB44426E106D08E9CD23CB4985E1B3B964B6D4384BFE7AA107B3A98170B1F133A5529B626877739725DB02D8E
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":"13272498490361007","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\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):	5.10906002807382
Encrypted:	false
SSDEEP:	6:mBvE1q2Pwkn23iKKdKrQMxIFUtpWwFZZmwPWwFzkwOwkn23iKKdKrQMFLJ:mvWvYf5KkCFUtpWwX/PWwF5Jf5KktJ
MD5:	D1C270AB3D1DE7E6BF532E61A971E52B
SHA1:	8065FF0FB06E1F9F19BFC5641F2BB84785968DD9
SHA-256:	1C9EF726166F48FB5CE97612CB13786C5C5022019A74D5736CEB8E795EF59A42
SHA-512:	EA5F8369BC1E48B7D2703D6243796048B7A7C1640A582AE9C80D463454303B756DB7A75344E0AFD766EA35517AD696D4DA85AC1190E44878234B0F48C0994B16
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.582 1a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-23:08:10.583 1a54 Recovering log #3.2021/08/03-23:08:10.583 1a54 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\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):	5.10906002807382
Encrypted:	false
SSDEEP:	6:mBvE1q2Pwkn23iKKdKrQMxIFUtpWwFZZmwPWwFzkwOwkn23iKKdKrQMFLJ:mvWvYf5KkCFUtpWwX/PWwF5Jf5KktJ
MD5:	D1C270AB3D1DE7E6BF532E61A971E52B
SHA1:	8065FF0FB06E1F9F19BFC5641F2BB84785968DD9
SHA-256:	1C9EF726166F48FB5CE97612CB13786C5C5022019A74D5736CEB8E795EF59A42
SHA-512:	EA5F8369BC1E48B7D2703D6243796048B7A7C1640A582AE9C80D463454303B756DB7A75344E0AFD766EA35517AD696D4DA85AC1190E44878234B0F48C0994B16
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.582 1a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-23:08:10.583 1a54 Recovering log #3.2021/08/03-23:08:10.583 1a54 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):	5.104405055683685
Encrypted:	false
SSDEEP:	6:mBP634q2Pwkn23iKKdK7Uh2ghZIFUtpWaF3JZmwPWpZDkwOwkn23iKKdK7Uh2gnd:mC34vYf5KkIhHh2FUtpWaNJ/PWpZD5JA
MD5:	BF373C903E2079797E2859DD27BBDB45
SHA1:	AD153CADCD2E5CDAD38A78719048D161CA5072C5
SHA-256:	FE04966363E9089871C33CB8AF7D218B1CA28B60163A484886975A113A093C3F
SHA-512:	7C004A7136E87B66723B7FFF429903AD64435F97C84FFD53A1A7BB20B1C759BB46CBC0CC21F6C50E4695E35E64AAAF31CA97DB088E9B7C50879A3B35DBA910(5
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.403 1a60 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-23:08:10.418 1a60 Recovering log #3.2021/08/03-23:08:10.419 1a60 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):	5.104405055683685
Encrypted:	false
SSDEEP:	6:mBP634q2Pwkn23iKKdK7Uh2ghZIFUtpWaF3JZmwPWpZDkwOwkn23iKKdK7Uh2gnd:mC34vYf5KkIhHh2FUtpWaNJ/PWpZD5JA
MD5:	BF373C903E2079797E2859DD27BBDB45
SHA1:	AD153CADCD2E5CDAD38A78719048D161CA5072C5
SHA-256:	FE04966363E9089871C33CB8AF7D218B1CA28B60163A484886975A113A093C3F
SHA-512:	7C004A7136E87B66723B7FFF429903AD64435F97C84FFD53A1A7BB20B1C759BB46CBC0CC21F6C50E4695E35E64AAAF31CA97DB088E9B7C50879A3B35DBA910(5
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.403 1a60 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-23:08:10.418 1a60 Recovering log #3.2021/08/03-23:08:10.419 1a60 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\6eabefa4-0769-4c0c-85c5-f1faea145afe.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"}],"isol ation":[],"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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\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):	5.2101683599752056
Encrypted:	false
SSDEEP:	6:mBIlyq2Pwkn23iKKdKusNpV/2jMGIFUtpWuUj11ZmwPWuUjjRkwOwkn23iKKdKux:mIIvYf5KkFFUtpWuo1/PWua5Jf5KkOJ
MD5:	FA4215D57F497B6652FDD287EB7B2A42
SHA1:	B774601E0A1CF5794EE57B118BC0D7C3A41BD24C
SHA-256:	DEB0EC2D4F26B5EA6285676A7265A3470DE15EBE36A6FAAA668B1C4FB5903D76
SHA-512:	5B2A212254A70B6942A4756E2B9BD2C873DF9651FED03E59C259A5E93698C0FCC05EF186A9AB3DC5266B0FD81CCB575E4781B34B258C65FCB33D49AD5F3D39 3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.604 1aa4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:08:10.605 1aa4 Recovering log #3.2021/08/03-23:08:10.605 1aa4 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):	5.2101683599752056
Encrypted:	false
SSDEEP:	6:mBIlyq2Pwkn23iKKdKusNpV/2jMGIFUtpWuUj11ZmwPWuUjjRkwOwkn23iKKdKux:mIIvYf5KkFFUtpWuo1/PWua5Jf5KkOJ
MD5:	FA4215D57F497B6652FDD287EB7B2A42
SHA1:	B774601E0A1CF5794EE57B118BC0D7C3A41BD24C
SHA-256:	DEB0EC2D4F26B5EA6285676A7265A3470DE15EBE36A6FAAA668B1C4FB5903D76
SHA-512:	5B2A212254A70B6942A4756E2B9BD2C873DF9651FED03E59C259A5E93698C0FCC05EF186A9AB3DC5266B0FD81CCB575E4781B34B258C65FCB33D49AD5F3D39 3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.604 1aa4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:08:10.605 1aa4 Recovering log #3.2021/08/03-23:08:10.605 1aa4 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 Stateod (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"}],"isol ation":[],"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):	5.241642809283434
Encrypted:	false
SSDEEP:	6:mBJF4+q2Pwkn23iKKdKusNpqz4rRIFUtpWmZmwPWO83VkwOwkn23iKKdKusNpqzW:mM+vYf5KkmiuFUtpWm/PWlV5Jf5Kkm2J
MD5:	96FAEDC6E2B8843F4AC09FE745C1DB57
SHA1:	9131ABC8B066EDDE4F18300693D6D046E425DAE2
SHA-256:	4B45A8C6419DDCC3FE86B5370B6809577AE05F021E5769BA499835F6E5FB3CD4
SHA-512:	938F787980EEDEA48760D9B7438D8D335D134DE8C148A746D46A125FAA9CBD5873F1BEF50A061C7F420410723142FC98240D606EF0CD091B2EA5CF4961764E3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.659 1abc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-23:08:10.662 1abc Recovering log #3.2021/08/03-23:08:10.663 1abc 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):	5.241642809283434
Encrypted:	false
SSDEEP:	6:mBJF4+q2Pwkn23iKKdKusNpqz4rRIFUtpWmZmwPWO83VkwOwkn23iKKdKusNpqzW:mM+vYf5KkmiuFUtpWm/PWlV5Jf5Kkm2J
MD5:	96FAEDC6E2B8843F4AC09FE745C1DB57
SHA1:	9131ABC8B066EDDE4F18300693D6D046E425DAE2
SHA-256:	4B45A8C6419DDCC3FE86B5370B6809577AE05F021E5769BA499835F6E5FB3CD4
SHA-512:	938F787980EEDEA48760D9B7438D8D335D134DE8C148A746D46A125FAA9CBD5873F1BEF50A061C7F420410723142FC98240D606EF0CD091B2EA5CF4961764E3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.659 1abc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-23:08:10.662 1abc Recovering log #3.2021/08/03-23:08:10.663 1abc Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.204611306481455
Encrypted:	false
SSDEEP:	6:mbN+q2Pwkn23iKKdKusNpZQMxIFUtpDvZmwPEvVkwOwkn23iKKdKusNpZQMFLJ:kIvYf5KkMFUtpz/PE95Jf5KkTJ
MD5:	53E719B39849CB169DBD034EF7FAF280
SHA1:	93BA99FAAE37014C764333FA5F2A721CDA69818E
SHA-256:	0B6C72F809CC2BE81E048E37FF641EF49CCEF5B719AFE507A8ACAAD855AA48DE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
SHA-512:	941D6EFD64639DD1772A5F381E015D5974F71B4CF3985477C6B5A6B85B752B57D222AEB247F07855FAB2CA467CE3B9DD32A3C18240E02D09685B3876A59316B0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:26.686 1aa8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-23:08:26.687 1aa8 Recovering log #3.2021/08/03-23:08:26.688 1aa8 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):	418
Entropy (8bit):	5.204611306481455
Encrypted:	false
SSDEEP:	6:mbN+q2Pwkn23iKKdKusNpZQMxIFUtpDvZmwPEvVkwOwkn23iKKdKusNpZQMFLJ:kIvYf5KkMFUtpz/PE95Jf5KkTJ
MD5:	53E719B39849CB169DBD034EF7FAF280
SHA1:	93BA99FAAE37014C764333FA5F2A721CDA69818E
SHA-256:	0B6C72F809CC2BE81E048E37FF641EF49CCEF5B719AFE507A8ACAAD855AA48DE
SHA-512:	941D6EFD64639DD1772A5F381E015D5974F71B4CF3985477C6B5A6B85B752B57D222AEB247F07855FAB2CA467CE3B9DD32A3C18240E02D09685B3876A59316B0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:26.686 1aa8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-23:08:26.687 1aa8 Recovering log #3.2021/08/03-23:08:26.688 1aa8 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\nmmhkkegccagdldgiimedpiccmgmieda\def\2b7b6dad-c7da-4f46-afd4-a7fca5b369ba.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
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.2247543711258855
Encrypted:	false
SSDEEP:	12:VvYf5KkkGHArBFUtp7/PlFU9z5Jf5KkkGHAryJ:5Yf5KkkGgPgLF4Jf5KkkGga
MD5:	55032CCFBCBA68054C8CD847189B66FA
SHA1:	0C09FCC415AAC3917904606882E71D2414E1CD67
SHA-256:	C96B12C1C57070FF34D3BB031E50659AC1EFE30DFE864E4252A3441772CC7D4D
SHA-512:	80853BA3ED05AA9B0EC08162467E5337CCC3DD825ACAFD06632318123449C03CB249D3707315892ADDFF904A7E0E5FBC1190BB0AA8BD246100ABDEFF946CED8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.786 1a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:08:16.787 1a54 Recovering log #3.2021/08/03-23:08:16.788 1a54 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\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):	5.2247543711258855
Encrypted:	false
SSDEEP:	12:VvYf5KkkGHArBFUtp7/PlFU9z5Jf5KkkGHAryJ:5Yf5KkkGgPgLF4Jf5KkkGga
MD5:	55032CCFBCBA68054C8CD847189B66FA
SHA1:	0C09FCC415AAC3917904606882E71D2414E1CD67
SHA-256:	C96B12C1C57070FF34D3BB031E50659AC1EFE30DFE864E4252A3441772CC7D4D
SHA-512:	80853BA3ED05AA9B0EC08162467E5337CCC3DD825ACAFD06632318123449C03CB249D3707315892ADDFF904A7E0E5FBC1190BB0AA8BD246100ABDEFF946CED8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.786 1a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:08:16.787 1a54 Recovering log #3.2021/08/03-23:08:16.788 1a54 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\Network Persistent Stateod (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):	4.9616384877719995
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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.160152949462705
Encrypted:	false
SSDEEP:	12:Aj+vYf5KkkGHArqiuFUtpUu0X/P5V5Jf5KkkGHArq2J:AAYf5KkkGgCgk5Jf5KkkGg7
MD5:	33DCF0CBE6D7871972B63B0F2151087E
SHA1:	2C36E4C1A6D5AC27C0F97020D1ECC945D50EA804

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
SHA-256:	E9DBB8E3B0C76DD69D677BD7A2EAC36933670AAF37AC6704633E9F8AA3E76B8F
SHA-512:	0418048B69A73A81A2E4369BD2FC76CFAE9A475C8805C66C2A5E1F79FEB445EC88432C46638AFCD9B4C3A30D731C7C9D41564DEA91AE06C657AFDF190D947E6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.802 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:08:16.806 1aac Recovering log #3.2021/08/03-23:08:16.807 1aac 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\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):	5.160152949462705
Encrypted:	false
SSDEEP:	12:Aj+vYf5KkkGHArqiuFUtpUu0X/P5V5Jf5KkkGHArq2J:AAYf5KkkGgCgk5Jf5KkkGg7
MD5:	33DCF0CBE6D7871972B63B0F2151087E
SHA1:	2C36E4C1A6D5AC27C0F97020D1ECC945D50EA804
SHA-256:	E9DBB8E3B0C76DD69D677BD7A2EAC36933670AAF37AC6704633E9F8AA3E76B8F
SHA-512:	0418048B69A73A81A2E4369BD2FC76CFAE9A475C8805C66C2A5E1F79FEB445EC88432C46638AFCD9B4C3A30D731C7C9D41564DEA91AE06C657AFDF190D947E6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.802 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:08:16.806 1aac Recovering log #3.2021/08/03-23:08:16.807 1aac 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:	B0A7B1940428590566387677 4A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.14468811800813
Encrypted:	false
SSDEEP:	12:CIOvYf5KkkGHArAFUtpyLZ/Py+5Jf5KkkGHArfJ:ClYf5KkkGgkg4ooJf5KkkGgV
MD5:	0F04D35E87FB92AFB98D83FAB1A63A5E
SHA1:	D6FC7F22B0FBE4DB4EC8936496D7E2A6971ECCB3
SHA-256:	5500450A405AF27E2EB296484B893DFBEE716457A293A6ACAF9562532FEED307
SHA-512:	27980D38654E38887A65E23F290BCB2647EDE8B20E3DB293C6E5A3A300EEA0939ADE8F61867346DE8EE84FAE3B5A02D8EB29F0D9084E6D80739D4F8FF5B9719
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:32.055 1aa8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-23:08:32.056 1aa8 Recovering log #3.2021/08/03-23:08:32.057 1aa8 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\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.14468811800813
Encrypted:	false
SSDEEP:	12:ClOvYf5KkkGHArAFUtpyLZ/Py+5Jf5KkkGHArfJ:ClYf5KkkGgkg4ooJf5KkkGgV
MD5:	0F04D35E87FB92AFB98D83FAB1A63A5E
SHA1:	D6FC7F22B0FBE4DB4EC8936496D7E2A6971ECCB3
SHA-256:	5500450A405AF27E2EB296484B893DFBEE716457A293A6ACAF9562532FEED307
SHA-512:	27980D38654E38887A65E23F290BCB2647EDE8B20E3DB293C6E5A3A300EEA0939ADE8F61867346DE8EE84FAE3B5A02D8EB29F0D9084E6D80739D4F8FF5B9719
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:32.055 1aa8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/03-23:08:32.056 1aa8 Recovering log #3.2021/08/03-23:08:32.057 1aa8 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:	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):	5.195468798357102
Encrypted:	false
SSDEEP:	6:mBaD+q2Pwkn23iKKdKpIFUtpWZAWZmwPWqVVkwOwkn23iKKdKa/WLJ:me+vYf5KkmFUtpWZAW/PW8V5Jf5KkaUJ
MD5:	5AABC8B1E746DF837F210095100F08A4
SHA1:	B80F72F049BE1390D730016188AA0EBE4655B747
SHA-256:	AC028988CFA2CBC9F63712C159E08B69BCECCC9FEAEB445BAB3589334E061DC6
SHA-512:	F8AC1863EE4A13C99BB3C7B8FA6F2F63078F647FF311C27C63C3805C534B0D13858C2FD8D784ED588C55DCC402454C74942ADCE586B02970ABEAA248C8EAAE 4
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.405 1a5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-23:08:10.426 1a5c Recovering log #3.2021/08/03-23:08:10.429 1a5c 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):	5.195468798357102
Encrypted:	false
SSDEEP:	6:mBaD+q2Pwkn23iKKdKpIFUtpWZAWZmwPWqVVkwOwkn23iKKdKa/WLJ:me+vYf5KkmFUtpWZAW/PW8V5Jf5KkaUJ
MD5:	5AABC8B1E746DF837F210095100F08A4
SHA1:	B80F72F049BE1390D730016188AA0EBE4655B747
SHA-256:	AC028988CFA2CBC9F63712C159E08B69BCECCC9FEAEB445BAB3589334E061DC6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old (copy)	
SHA-512:	F8AC1863EE4A13C99BB3C7B8FA6F2F63078F647FF311C27C63C3805C534B0D13858C2FD8D784ED588C55DCC402454C74942ADCE586B02970ABEAA248C8EAAE4
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:10.405 1a5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-23:08:10.426 1a5c Recovering log #3.2021/08/03-23:08:10.429 1a5c 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):	5.278889456726711
Encrypted:	false
SSDEEP:	6:msypM+q2Pwkn23iKKdKks8Y5JKKhdIFUtpvJQZmwPvJTMVkwOwkn23iKKdKks8Yx:d+vYf5KkkOrsFUtpG/PCV5Jf5KkkOrzJ
MD5:	39C30C5504270DAA1397FD6B004F707C
SHA1:	B773AB15BCF1408973767280F87E0E4A5AF750CB
SHA-256:	77CACFF88ED6CB71660A3DF278C1842E93D93B55930EC2E79B51C61CD328E2E6
SHA-512:	A65AB0B1B62A42FA2C3FB48E4A6A50B4A4055A78BF51F7B11CDF782B2DCF50056E608236FA1240B053047B44D0382B6BAFEEA525CDFB6392254C3C49F852AC06
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:17.859 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-23:08:17.861 1aac Recovering log #3.2021/08/03-23:08:17.861 1aac Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.olds (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.278889456726711
Encrypted:	false
SSDEEP:	6:msypM+q2Pwkn23iKKdKks8Y5JKKhdIFUtpvJQZmwPvJTMVkwOwkn23iKKdKks8Yx:d+vYf5KkkOrsFUtpG/PCV5Jf5KkkOrzJ
MD5:	39C30C5504270DAA1397FD6B004F707C
SHA1:	B773AB15BCF1408973767280F87E0E4A5AF750CB
SHA-256:	77CACFF88ED6CB71660A3DF278C1842E93D93B55930EC2E79B51C61CD328E2E6
SHA-512:	A65AB0B1B62A42FA2C3FB48E4A6A50B4A4055A78BF51F7B11CDF782B2DCF50056E608236FA1240B053047B44D0382B6BAFEEA525CDFB6392254C3C49F852AC06
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:17.859 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-23:08:17.861 1aac Recovering log #3.2021/08/03-23:08:17.861 1aac Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/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):	1540
Entropy (8bit):	5.59963922368973
Encrypted:	false
SSDEEP:	48:Y0t+U+U9m6UUhyhUEr7FKU+9qPeUekUeJwUYPUeP:f+U+U97UUQhUErJKUJPeU3UHUYPUg
MD5:	298F7694E634423EEAFFC04994F83482
SHA1:	D21C5F631B78DA6FD4B90BE5C827777D9AB8945E
SHA-256:	4EAD7B8182DB94144BE6F43DAC2EFDE05710692C16150C4AAC43A24C89BE064F
SHA-512:	5533C1CEA8DB71AF1DB382BE7A91620DA506ECF029E748913E5718EDE63C8B1F91C0405767FF30699D9490DF19B075D62EEA239CF23E18DAB322E9AE4282957
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Preview:	{"expect_ct":[],"sts":[{"expiry":1659560896.055214,"host":"DEYqY3fY1uk+rWZFaOylMBhnZNdkY4A9bQ0Ct+WSQy0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628024896.055219},{"expiry":1659560895.956745,"host":"HIplQqWMs6ZxBLdnO3HzMXf8AYhhbIad/Qg77wu6W6Q=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628024895.95675},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659560895.24134,"host":"W7TETmXWC1BCKJyizGYquiWJjlWwM5BiHT4qzLOSu7g=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628024895.241344},{"expiry":1659560895.474665,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628024895.474668},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a5f5c538-0be9-4615-af46-693daeeade15.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\ad05ab0c-4d15-4ffe-a2ef-8e8a734520a3.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):	22600
Entropy (8bit):	5.536649153467188
Encrypted:	false
SSDEEP:	384:fubtGLlEwXh1kXqKf/pUZNCgVLH2HfD0rUXHGQnZ0l548:5LlXh1kXqKf/pUZNCgVLH2HforU3GQn8
MD5:	081DD7E245C121C86ACEA4C2F3BD2002
SHA1:	26C698D1667E95D8DCF00559FB4695B3C4EAC111
SHA-256:	1C4E90B423E0409B1C9A7D7E98B1755D0FAF413325A9AB401039579D08EA5535
SHA-512:	C1B30A7D4CCE040F0A68BF6AD5CB8E895E0D8D24E1764FAA932F51663904C752146F907C8D3DF0F01D222074A2031CC7A7088D29EF9DF9BDC217BF5CF4218AE
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":"13272498490361007","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\d7e666ce-745c-4ee3-b23d-d599523309b5.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):	22602
Entropy (8bit):	5.536658263462912
Encrypted:	false
SSDEEP:	384:fubt/lIEwXh1kXqKf/pUZNCgVLH2HfD0rUXHGTnZWZ2543:CLlXh1kXqKf/pUZNCgVLH2HforU3GTnO
MD5:	13EAD9467F27511A71F3CA1875A260E1
SHA1:	ED5523F3C4837503AF8F14DEC723AC833030FFE6
SHA-256:	C9FB29E57340574909DF7EC3C08827EBC489EDBB06528141817FB8F2AF4D8A6C
SHA-512:	237E401327DA1FC470C569BAA11B82E3B813EFDEB44426E106D08E9CD23CB4985E1B3B964B6D4384BFE7AA107B3A98170B1F133A5529B626877739725DB02D8D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d7e666ce-745c-4ee3-b23d-d599523309b5.tmp	
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":"13272498490361007","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\CURRENT (copy)	
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):	4.378004740620742
Encrypted:	false
SSDEEP:	3:tUK6kKLNUcHvJZmwv3IkKLUhFhH1V8sIkKLVFrH1WGv:mHy2vJZmwPQAhFhVVvQfVtv
MD5:	6FDD2BB2611A20B7845C7EAE64687073
SHA1:	99E47914083A310CF7B6C7D907E954429E8BDF6F
SHA-256:	EE796D90F3AA8D338ACF26C68B666D649446FF9EE2179238E87D828A767798AE
SHA-512:	AF164FD44BF4565AB1F869FBE80375181C2E74653AAD9DC87CAF19CCA4CFA5E901B24AD2A1BBD680B65D50FA1CAF9D153C16A739F3D51CB1FBDF94751D03028
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.028 19b0 Recovering log #3.2021/08/03-23:08:16.100 19b0 Delete type=0 #3.2021/08/03-23:08:16.101 19b0 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old. (copy)	
Entropy (8bit):	4.378004740620742
Encrypted:	false
SSDEEP:	3:tUK6kKLNUcHvJZmwv3IkKLUhFhH1V8sIkKLVFrH1WGv:mHy2vJZmwPQAhFhVVvQfVtv
MD5:	6FDD2BB2611A20B7845C7EAE64687073
SHA1:	99E47914083A310CF7B6C7D907E954429E8BDF6F
SHA-256:	EE796D90F3AA8D338ACF26C68B666D649446FF9EE2179238E87D828A767798AE
SHA-512:	AF164FD44BF4565AB1F869FBE80375181C2E74653AAD9DC87CAF19CCA4CFA5E901B24AD2A1BBD680B65D50FA1CAF9D153C16A739F3D51CB1FBDF94751D030 28
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.028 19b0 Recovering log #3.2021/08/03-23:08:16.100 19b0 Delete type=0 #3.2021/08/03-23:08:16.101 19b0 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
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e56da246-8455-4edd-b13a-53955359f1ac.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":[{"adverti sed_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","s upports_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\f6f164b0-095e-40fd-a079-f867cab90773.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):	1540
Entropy (8bit):	5.59963922368973
Encrypted:	false
SSDEEP:	48:Y0t+U+U9m6UUhyhUEr7FKU+9qPeUekUeJwUYPUeP:f+U+U97UUQhUErJKUJPeU3UHUYPUg
MD5:	298F7694E634423EEAFFC04994F83482
SHA1:	D21C5F631B78DA6FD4B90BE5C827777D9AB8945E
SHA-256:	4EAD7B8182DB94144BE6F43DAC2EFDE05710692C16150C4AAC43A24C89BE064F
SHA-512:	5533C1CEA8DB71AF1DB382BE7A91620DA506ECF029E748913E5718EDE63C8B1F91C0405767FF30699D9490DF19B075D62EEA239CF23E18DAB322E9AE4282957
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f6f164b0-095e-40fd-a079-f867cab90773.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1659560896.055214,"host":"DEYqY3fY1uk+rWZFaOylMBhnZNdkY4A9bQ0Ct+WSQy0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628024896.055219},{"expiry":1659560895.956745,"host":"HIplQqWMs6ZxBLdnO3HzMXf8AYhhbIad/Qg77wu6W6Q=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628024895.95675},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659560895.24134,"host":"W7TETmXWC1BCKJyizGYquiWJjlWwM5BiHT4qzLOSu7g=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628024895.241344},{"expiry":1659560895.474665,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628024895.474668},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_obser

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):	5.141124092703655
Encrypted:	false
SSDEEP:	6:mHL+q2Pwkn23iKKdKfrzAdIFUtpQKZmwPQZVkwOwkn23iKKdKfrzILJ:u+vYf5Kk9FUtpz/PoV5Jf5Kk2J
MD5:	830963C6FF69D2A40BCDB5E32D477374
SHA1:	022113428C9D630184B3B176D3C58ACF479CB506
SHA-256:	7EB4F5E8A280BC97BE8A64D5E748C97B140D745831C58C23DBEAF59D7D7BDD06
SHA-512:	82A1D63A0EA0E8733CE101D07DA4C667CAED1085B66D19081F175F2B91AE054A455E4B763620216D89FF06152AFA9F87A56F0D7A274EAFF71C4B761FD50FC46
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.311 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-23:08:16.312 1a2c Recovering log #3.2021/08/03-23:08:16.313 1a2c 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\Default\shared_proto_db\metadata\LOG.oldE (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.141124092703655
Encrypted:	false
SSDEEP:	6:mHL+q2Pwkn23iKKdKfrzAdIFUtpQKZmwPQZVkwOwkn23iKKdKfrzILJ:u+vYf5Kk9FUtpz/PoV5Jf5Kk2J
MD5:	830963C6FF69D2A40BCDB5E32D477374
SHA1:	022113428C9D630184B3B176D3C58ACF479CB506
SHA-256:	7EB4F5E8A280BC97BE8A64D5E748C97B140D745831C58C23DBEAF59D7D7BDD06
SHA-512:	82A1D63A0EA0E8733CE101D07DA4C667CAED1085B66D19081F175F2B91AE054A455E4B763620216D89FF06152AFA9F87A56F0D7A274EAFF71C4B761FD50FC46
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:08:16.311 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-23:08:16.312 1a2c Recovering log #3.2021/08/03-23:08:16.313 1a2c 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:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
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):	6.079653179585909
Encrypted:	false
SSDEEP:	3072:KLDGaYTJQE+mugy9+QV1T7IRwdfLSNPnFcbXafIB0u1GOJmA3iuRJ:6yxaV+QfT7GSmhFaqfIlUOoSiuRJ
MD5:	88E803F77C180EDF5E08385454B5D050
SHA1:	4F1577D53BF672097D618CFE876A2974947ED039
SHA-256:	11C0A104FA34936DDD98710A68E70808CF34C70A21FD5B4ED07747D1718FDFEE
SHA-512:	5E077EC4C18AC47025CD543DB3D5A5957103251F52357C9C5E632F2B264AB7F95DA393CEDF75EA8AC1F32A3CA856C520BC691A0661EBB51A3054D1C163005B4
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":1.628024893400754e+12,"network":1.628024895e+12,"ticks":6625838171.0,"uncertainty":4772732.0}},"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":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateTM (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):	6.079653179585909
Encrypted:	false
SSDEEP:	3072:KLDGaYTJQE+mugy9+QV1T7IRwdfLSNPnFcbXafIB0u1GOJmA3iuRJ:6yxaV+QfT7GSmhFaqfIlUOoSiuRJ
MD5:	88E803F77C180EDF5E08385454B5D050
SHA1:	4F1577D53BF672097D618CFE876A2974947ED039
SHA-256:	11C0A104FA34936DDD98710A68E70808CF34C70A21FD5B4ED07747D1718FDFEE
SHA-512:	5E077EC4C18AC47025CD543DB3D5A5957103251F52357C9C5E632F2B264AB7F95DA393CEDF75EA8AC1F32A3CA856C520BC691A0661EBB51A3054D1C163005B4
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":1.628024893400754e+12,"network":1.628024895e+12,"ticks":6625838171.0,"uncertainty":4772732.0}},"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":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7493235200352872
Encrypted:	false
SSDEEP:	384:7f6JZns+LfoVUN9ruvBr3CVr+Hv6G+BrsPVxxSrzPirQ5mIDMrFF1COv/FNM1dUZ:WO5tC3eewe79zXQH7WfKRf9hV
MD5:	6CAB5FD028151F513DD781C4260024FA
SHA1:	112FB2E6AF9A822C857A05A30A8F4286D9E75CD8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
SHA-256:	6CC176BBC13DD92973C838DC137EB8346278BF24994370595E7B3E724C306598
SHA-512:	C0A605670C256CF8F33D0B29B3C94C6768DD48163FF978156D53BDEEA69E3C24939A62FCBC5224D50FFF40959B431D3F16D4B34C854C1116BE545C6B5EBF11A
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....A8.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\e05e02b6-f162-4417-af40-57678a30a893.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):	6.079653179585909
Encrypted:	false
SSDEEP:	3072:KLDGaYTJQE+mugy9+QV1T7IRwdfLSNPnFcbXafIB0u1GOJmA3iuRJ:6yxaV+QfT7GSmhFaqfIlUOoSiuRJ
MD5:	88E803F77C180EDF5E08385454B5D050
SHA1:	4F1577D53BF672097D618CFE876A2974947ED039
SHA-256:	11C0A104FA34936DDD98710A68E70808CF34C70A21FD5B4ED07747D1718FDFEE
SHA-512:	5E077EC4C18AC47025CD543DB3D5A5957103251F52357C9C5E632F2B264AB7F95DA393CEDF75EA8AC1F32A3CA856C520BC691A0661EBB51A3054D1C163005B4
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":1.628024893400754e+12,"network":1.628024895e+12,"ticks":6625838171.0,"uncertainty":4772732.0}},"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":{"

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 3, 2021 23:08:15.279104948 CEST	192.168.2.4	8.8.8.8	0xa9b4	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.282893896 CEST	192.168.2.4	8.8.8.8	0x2f5f	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.286760092 CEST	192.168.2.4	8.8.8.8	0x9fb0	Standard query (0)	www.canva.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.688633919 CEST	192.168.2.4	8.8.8.8	0xb1c9	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 23:08:15.744865894 CEST	192.168.2.4	8.8.8.8	0x8457	Standard query (0)	static.canva.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.964791059 CEST	192.168.2.4	8.8.8.8	0x96f8	Standard query (0)	static.clo udflareins ights.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:16.306284904 CEST	192.168.2.4	8.8.8.8	0x35dd	Standard query (0)	cl.canva.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:16.659713984 CEST	192.168.2.4	8.8.8.8	0x3e57	Standard query (0)	clients2.g oogleuserc ontent.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:17.129482985 CEST	192.168.2.4	8.8.8.8	0x5cc9	Standard query (0)	static.canva.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 23:08:15.316447020 CEST	8.8.8.8	192.168.2.4	0xa9b4	No error (0)	clients2.g oogle.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:08:15.316447020 CEST	8.8.8.8	192.168.2.4	0xa9b4	No error (0)	clients.l. google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.318512917 CEST	8.8.8.8	192.168.2.4	0x2f5f	No error (0)	accounts.g oogle.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.326798916 CEST	8.8.8.8	192.168.2.4	0x9fb0	No error (0)	www.canva.com		104.17.115.17	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.326798916 CEST	8.8.8.8	192.168.2.4	0x9fb0	No error (0)	www.canva.com		104.17.114.17	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.722465992 CEST	8.8.8.8	192.168.2.4	0xb1c9	No error (0)	a.nel.clou dflare.com		35.190.80.1	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.781574965 CEST	8.8.8.8	192.168.2.4	0x8457	No error (0)	static.canva.com		104.17.114.17	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.781574965 CEST	8.8.8.8	192.168.2.4	0x8457	No error (0)	static.canva.com		104.17.115.17	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:15.974370956 CEST	8.8.8.8	192.168.2.4	0xa662	No error (0)	gstaticads sl.l.google.com		216.58.198.3	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:16.001749992 CEST	8.8.8.8	192.168.2.4	0x96f8	No error (0)	static.clo udflareins ights.com		104.16.94.65	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:16.001749992 CEST	8.8.8.8	192.168.2.4	0x96f8	No error (0)	static.clo udflareins ights.com		104.16.95.65	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:16.344451904 CEST	8.8.8.8	192.168.2.4	0x35dd	No error (0)	cl.canva.com		104.17.115.17	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:16.344451904 CEST	8.8.8.8	192.168.2.4	0x35dd	No error (0)	cl.canva.com		104.17.114.17	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:16.693238020 CEST	8.8.8.8	192.168.2.4	0x3e57	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.googleuserc rcontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:08:16.693238020 CEST	8.8.8.8	192.168.2.4	0x3e57	No error (0)	googlehost ed.l.googl euserconte nt.com		216.58.208.129	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:17.167716980 CEST	8.8.8.8	192.168.2.4	0x5cc9	No error (0)	static.canva.com		104.17.115.17	A (IP address)	IN (0x0001)
Aug 3, 2021 23:08:17.167716980 CEST	8.8.8.8	192.168.2.4	0x5cc9	No error (0)	static.canva.com		104.17.114.17	A (IP address)	IN (0x0001)

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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 23:08:17.302154064 CEST	104.17.115.17	443	192.168.2.4	49766	CN=canva.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Sep 08 02:00:00 CEST 2020	Wed Sep 08 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6624 Parent PID: 4424

General

Start time:	23:08:09
Start date:	03/08/2021
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 'https://www.canva.com/design/DAEl-R1jp6Q/7tYJcxXWl2osP9-56-X6pQ/view?utm_content=DAEl-R1jp6Q&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink'
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: 6788 Parent PID: 6624

General

Start time:	23:08:10
Start date:	03/08/2021
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=1508,7393693506506586080,11924844796807865969,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1768 /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

Registry Activities

Show Windows behavior

Disassembly