ID: 458955
Cookbook: browseurl.jbs
Time: 22:33:19
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

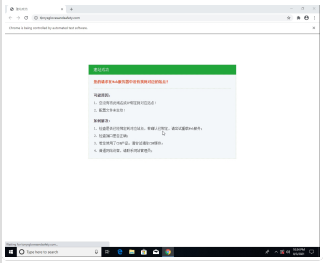
Windows Analysis Report http://tonysglovesandsafety.c…

Overview

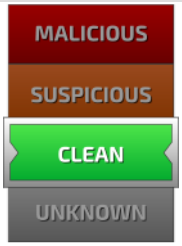
General Information

Sample URL:	http://tonysglovesandsafety.com
Analysis ID:	458955
Infos:	

Most interesting Screenshot:



Detection

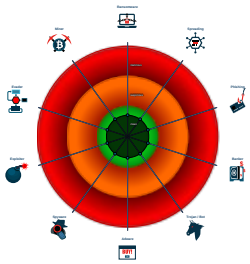


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3544 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://tonysglovesandsafety.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5708 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1568,2662458852142118270,11731089809733117219,131072 --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

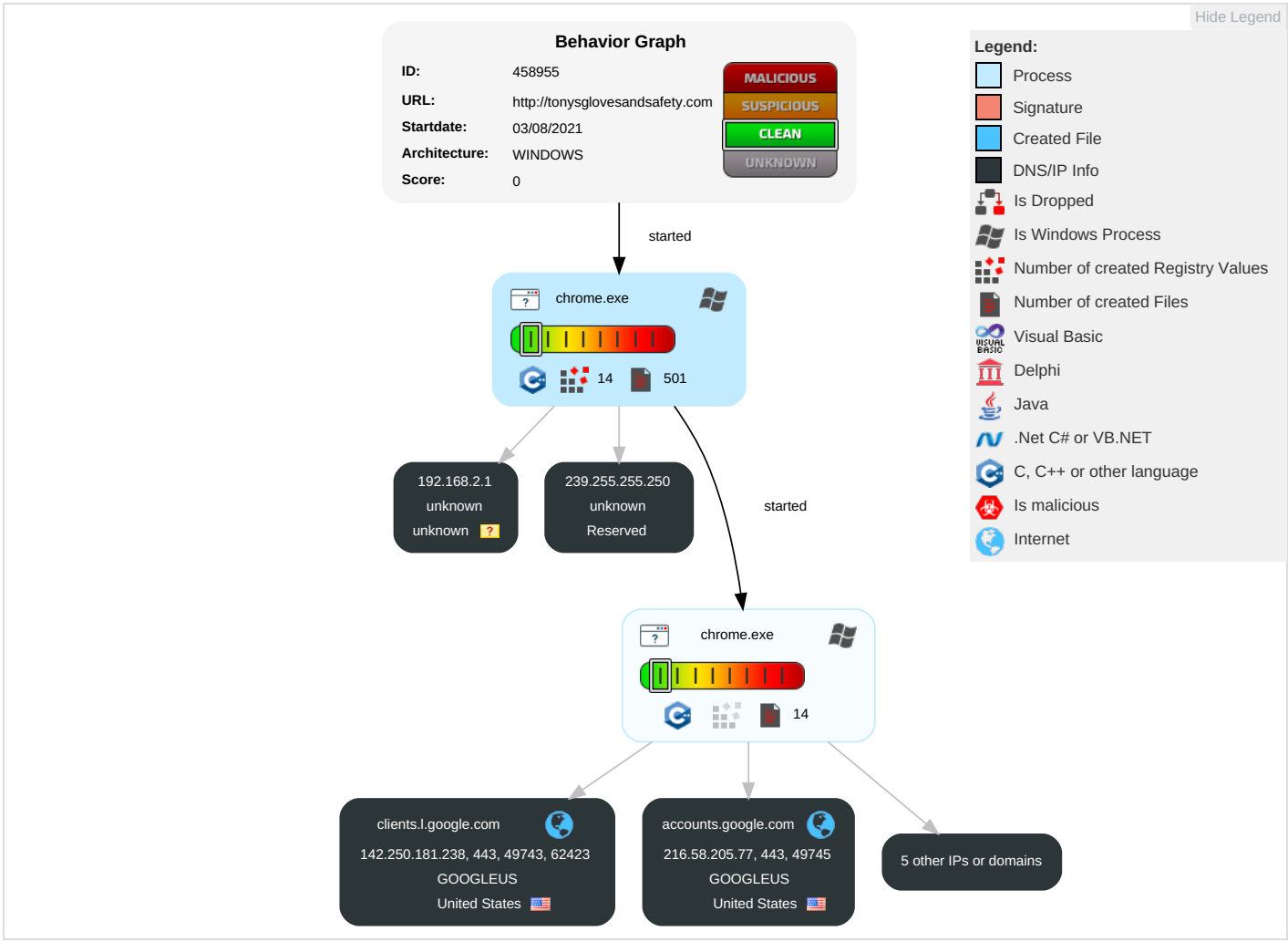
Click to jump to signature section

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

Mitre Att&ck Matrix

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

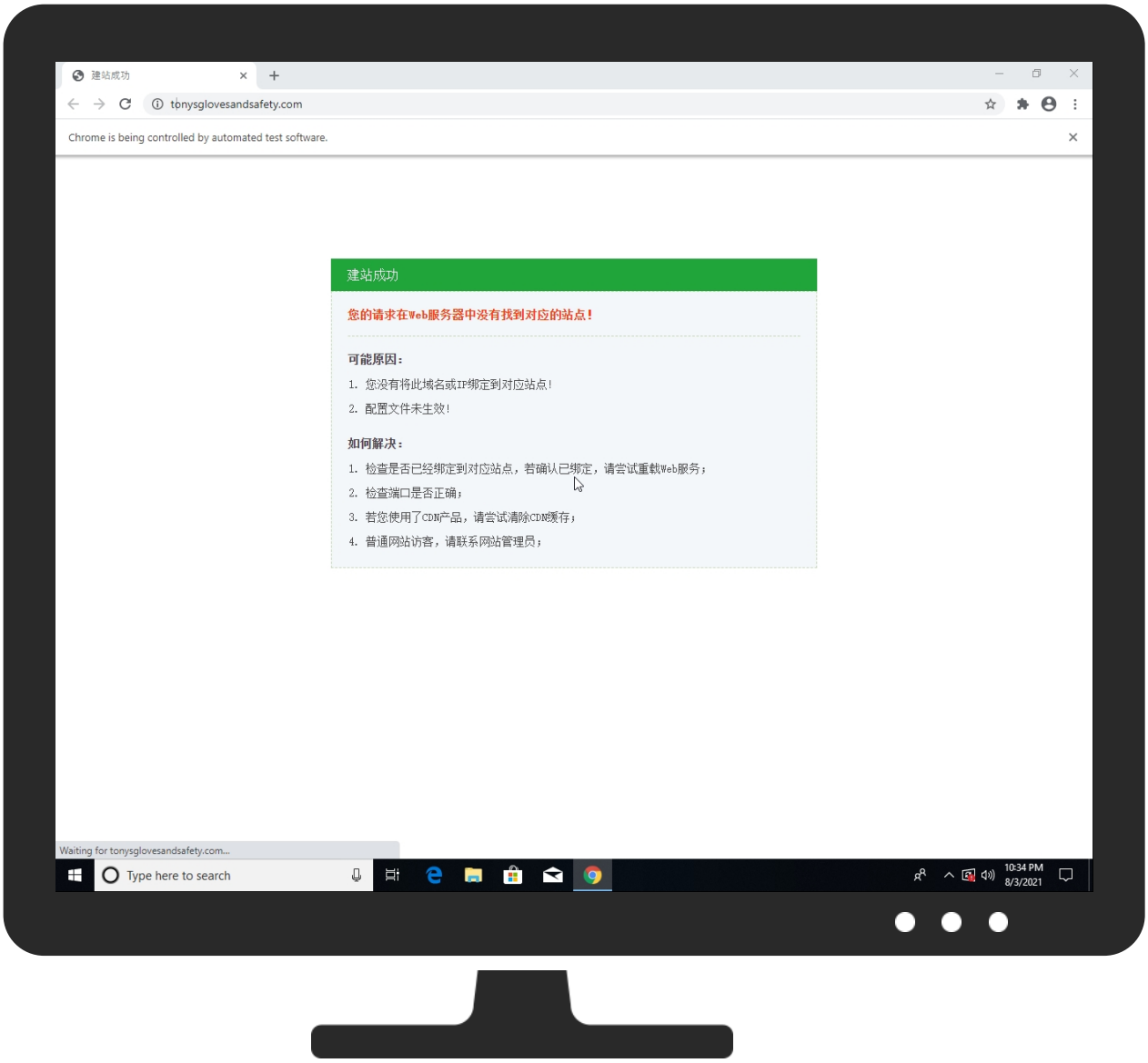
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://tonysglovesandsafety.com/2	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://tonysglovesandsafety.com/favicon.ico	0%	Avira URL Cloud	safe	
http://tonysglovesandsafety.com/?	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tonysglovesandsafety.com	168.206.125.23	true	false		unknown
accounts.google.com	216.58.205.77	true	false		high
clients.l.google.com	142.250.181.238	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://tonysglovesandsafety.com/	false		unknown
http://tonysglovesandsafety.com/	false		unknown
http://tonysglovesandsafety.com/favicon.ico	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.181.238	clients.l.google.com	United States		15169	GOOGLEUS	false
168.206.125.23	tonysglovesandsafety.com	South Africa		137951	CLAYERLIMITED-AS-APClayerLimitedHK	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458955
Start date:	03.08.2021
Start time:	22:33:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 23s

Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://tonysglovesandsafety.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@33/240@4/7
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\04a860ca-2d2b-4fb7-8a02-2a713192acb5.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\04a860ca-2d2b-4fb7-8a02-2a713192acb5.tmp

Entropy (8bit):	6.079642928041353
Encrypted:	false
SSDEEP:	3072:FrBGaYTJQE+mugy9+QV1T7IRwdfLSNPoFcbXafIB0u1GOJmA3iuRG:tsxaV+QfT7GSmh2aqfIlUOoSiuRG
MD5:	F722132E155D13922165AD8D2DE26B9B
SHA1:	8C648D879B96588EA47675FA8888F5A521EC43DA
SHA-256:	F17AF8FEF9994142F7B88FA054FEAE17497B30D24314D35B66574017322F9315
SHA-512:	CE866D85B7C74C5DEA58DB7BF39C99883D8042B7561F05F6B5A1AFC0A343BF6D78A31AF939353D19FBD7503043DA36AECA83FC303BF3B316656BBBED80D5AE52
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":1.628022855165405e+12,"network":1.628022856e+12,"ticks":7447711876.0,"uncertainty":4607845.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\1b3ed700-0c7d-4d8a-ac09-11bb22478882.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	174471
Entropy (8bit):	6.0796433605983475
Encrypted:	false
SSDEEP:	3072:O8JGaYTJQE+mugy9+QV1T7IRwdfLSNPoFcbXafIB0u1GOJmA3iuRG:ZkxaV+QfT7GSmh2aqfIlUOoSiuRG
MD5:	D348135C6C6496596DA943778B44E78C
SHA1:	1CC67804DCF56A5C269243E3556A8058288DBF6F
SHA-256:	2AF611D894D3FC437E49ECC99B23FE7CD8AA097562B0859E11089132FE808914
SHA-512:	8E3FE81A5E92843A732FDC772163577B665C364A95B5CF82066D27BF738AE076CD65C481129F7E3D0170DCA8B622C9088BE8A9AD99784266DF2D66ED14F33E7
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":1.628022855165405e+12,"network":1.628022856e+12,"ticks":7447711876.0,"uncertainty":4607845.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715059030"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\29c2c618-2ec2-43b9-ac83-d32df1380059.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):	6.0796432440602475
Encrypted:	false
SSDEEP:	3072:FddGaYTJQE+mugy9+QV1T7IRwdfLSNPoFcbXafIB0u1GOJmA3iuRG:7YxaV+QfT7GSmh2aqfIlUOoSiuRG
MD5:	D85E5231D4BF0A3BBC08D6B9B0AC3828
SHA1:	FB9D7BBF50844495E78CD07B030A5748FF426ADF
SHA-256:	1818B61AA8F834447A03C0F576D807BDE88C011FAA0B58F14B6900AD76190572
SHA-512:	7A604B856C8B03A97FDE7C1CFBF3C81A66FE364A849F197502A4782CFA46EA3D78C2FB88597E0A49C6EC8492C9494170CAFCCD9193C7A9982A4E86A1605F7E1
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":1.628022855165405e+12,"network":1.628022856e+12,"ticks":7447711876.0,"uncertainty":4607845.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d2ea397-4804-4843-8119-8251a8413536.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d2ea397-4804-4843-8119-8251a8413536.tmp

Entropy (8bit):	3.7496685214888243
Encrypted:	false
SSDEEP:	384:HnVa6E3hgkjedNSrnvGO3VeMxHclGJQrbI6MxVwgIjr7KmHMr4yOeNOY8uNj1STC:XWRRisd1AePEWMc/zG+KEeuhp
MD5:	FAD85C0CA5529EE363FA691AD16A6A77
SHA1:	20E7AEECBC0EBE044D4994482ABF8C0F5AC4F2A6
SHA-256:	C4291EA8827C102F434D3E45AAA84943F2EEF468E0356C658469CDDE0BDFD267
SHA-512:	7A0DC98C4B48C67BE63104E8DAF9210DFCF71892579BC457DB9D912A74E0E57988D2F33924A8720ADEC325AE9480228D476BE5757C03811E0287A08D42556A03
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\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:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C5 9
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\1ad81809-99a1-4796-9707-b60efdd430c2.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):	1041
Entropy (8bit):	5.566473516705512
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeiXzkq/HeUe8zUe3q7wUCUsRUeiQ:Ym6UUhyKUeiYqPeUekUe30wUCUeP
MD5:	EA0869E44DC4A0485D3773666DAF1E42
SHA1:	71286FDA0CDF361729F32135D2F993DEBECAFCC4
SHA-256:	40DFAFE21292DF242879009EA51E592B4D8A2CD38AB495F66A28B5BFA9DFDEA9
SHA-512:	72DACF42913E8233005A7051AD3905DC0653A7E3DD99C41D77F06945A424B14E8E1DB8B579DAE19A2A8182AF8C933EA672181D6B40F57FA476C6CDBD5DEF14 5
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1601450995.029298},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_in clude_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=," mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+ D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1659558856.811314,"host":"8/RrMmQlCD2G sp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628022856.811319},{"expiry":1632986995.164829,"h ost":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5a7da835-071d-4ec2-8487-651201b0a204.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):	5174
Entropy (8bit):	4.965450819023245
Encrypted:	false
SSDEEP:	48:YcVkKSChkliXqAOqqTlYGlQKHoTw0Crf4MqM8C1Nfct/9BhUJo3KhmeSnp4k3JbW:n1LMt9pIKIo5k0JCKL84k31abOTlVuHn
MD5:	258CD192A917865DB5F49C5B612E9C64

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5a7da835-071d-4ec2-8487-651201b0a204.tmp	
SHA1:	4EE7F68B51D44D9AD8CC7B765B3B5B2EC937B1BE
SHA-256:	D67021B34B1930D58A57E829155010A299B8AE00D8E890839D32488E81FE9DA2
SHA-512:	07B4609F68C152A6977A7931B3B08F36B33B6B841D26BEBEEB7FEAFE052144393221FAF9CF08CA37668E958D335FEECB3A9C049BDBB00214C2F0AC2207396C8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272496451438026","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\703f87e1-23e9-48f9-b13d-4f31c31b1d2e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577595807640707
Encrypted:	false
SSDEEP:	384:ZqitdwLlntXk1kXqKf/pUZNCgVLH2HfDcrUKzc4a:8LlJk1kXqKf/pUZNCgVLH2HforU+cl
MD5:	DB477AB1A6BAAD166D356A371A3D51A3
SHA1:	001B94F34448CB97DBF19AEAF6AED487762EF226
SHA-256:	55E04B1C4498987C8F69EA9EBC15978D3C53AD2970307B86BBB50D14243B6C86
SHA-512:	65267713F36737F5D136B2BCE1AFD16C62EEF572A22AFD38230D7C39F92A64C5BA855335C20F6021C6D36E7DDC17CC1F7056E9A3FA8913BA4450DD5599A3791
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":"13272496451041931","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\8b8e4313-ee8e-4e0a-9702-2ff363b8f33d.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):	5771
Entropy (8bit):	5.176057858089573
Encrypted:	false
SSDEEP:	96:n1LgU9oNO5VJusmaffIKIo5k0JCKL84k31abOTlVuHn:n1Lt9wgeHaffIeh4K7k3s
MD5:	BF021DC24E58D4DAF4ACA96768FB97EA
SHA1:	1E39358BA935F65E54861964D2DFD94ECACB8AF6
SHA-256:	69FD44F5C5D558E8D9DE6C1EF88995C73AC16C4EDC273CFD165E66DCC785D38D
SHA-512:	5349BFCEC571EFF9C8E5310688CCD0A2CF7C7F216F90DA174F54CA9D73D95E0631AE8DD03EFA54708090C85C7F13AAF0FAF1A8F33302C3BAF8823377FE256E C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272496451438026","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\914b7ce8-5e1d-4b37-9465-37d03d7390b6.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:6Fe0i0sIlyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\914b7ce8-5e1d-4b37-9465-37d03d7390b6.tmp	
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\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.24693175698276
Encrypted:	false
SSDEEP:	6:mRoSR+q2Pwkn23iKKdK9RXXTZIFUtpSoTZmwPhNtVkwOwkn23iKKdK9RXX5LJ:i1cvYf5Kk7XT2FUtpS+/P/T5Jf5Kk7XH
MD5:	50915082C1131B6FCCB5C973B7884C24
SHA1:	FBC059EC92574CE005DD9BAB3C2687B785CF1CBE
SHA-256:	242D3E596FBC4523F3D89D5D96F7ECAF943465E90538E0DD1573D72E64602B08
SHA-512:	B44837DA34E7AC818C4D760E72801C2B308AB1074C7E876709ED67716D35404BB0C6AFAA0E6930D487BE6C518DB79EADDBD008AEC14975FC1A97455A005721 9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.985 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-22:34:23.995 17d8 Recovering log #3.2021/08/03-22:34:24.008 17d8 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.olds: (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.24693175698276
Encrypted:	false
SSDEEP:	6:mRoSR+q2Pwkn23iKKdK9RXXTZIFUtpSoTZmwPhNtVkwOwkn23iKKdK9RXX5LJ:i1cvYf5Kk7XT2FUtpS+/P/T5Jf5Kk7XH
MD5:	50915082C1131B6FCCB5C973B7884C24
SHA1:	FBC059EC92574CE005DD9BAB3C2687B785CF1CBE
SHA-256:	242D3E596FBC4523F3D89D5D96F7ECAF943465E90538E0DD1573D72E64602B08
SHA-512:	B44837DA34E7AC818C4D760E72801C2B308AB1074C7E876709ED67716D35404BB0C6AFAA0E6930D487BE6C518DB79EADDBD008AEC14975FC1A97455A005721 9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.985 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-22:34:23.995 17d8 Recovering log #3.2021/08/03-22:34:24.008 17d8 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):	5.233802180483107
Encrypted:	false
SSDEEP:	6:mRojN+q2Pwkn23iKKdKyDZIFUtpSoO7ZmwPSoZHVkwOwkn23iKKdKyJLJ:iAIvYf5Kk02FUtpSj7/PSw5Jf5KkWJ
MD5:	B9CBF11A24B7C1B473733CE1D24870FC
SHA1:	BF93BB668939366284B7929B560D1D51610C9846
SHA-256:	54B8B6A559730A96B21D330FCFE3D8893AC8F630D0BD8DAA761743020478A0F3
SHA-512:	0339975FB56F94E9F09AEE356399D6F4A6330115DC73A058D939C97A9748447F843DA3A8EC65BBBC72DD6B0E5497F2028C48F68D4E3B75E7111E85C0883951C9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.944 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-22:34:23.952 17d8 Recovering log #3.2021/08/03-22:34:23.953 17d8 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.oldDB (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.233802180483107
Encrypted:	false
SSDEEP:	6:mRojN+q2Pwkn23iKKdKyDZIFUtpSoO7ZmwPSoZHVkwOwkn23iKKdKyJLJ:iAIvYf5Kk02FUtpSj7/PSw5Jf5KkWJ
MD5:	B9CBF11A24B7C1B473733CE1D24870FC
SHA1:	BF93BB668939366284B7929B560D1D51610C9846
SHA-256:	54B8B6A559730A96B21D330FCFE3D8893AC8F630D0BD8DAA761743020478A0F3
SHA-512:	0339975FB56F94E9F09AEE356399D6F4A6330115DC73A058D939C97A9748447F843DA3A8EC65BBBC72DD6B0E5497F2028C48F68D4E3B75E7111E85C0883951C9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.944 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-22:34:23.952 17d8 Recovering log #3.2021/08/03-22:34:23.953 17d8 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\Cookies	
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):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
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):	0.9737413195934403
Encrypted:	false
SSDEEP:	24:h3e9H6pf1H1oNhqLbJLbXaFpEO5bNmISHn06Uw6M8:h3bfvoNhq5LLOpEO5J/Kn7UC8
MD5:	AEE43DE99D425378AA33695E1A2F5628
SHA1:	B7D3BB13C4B1348E38F611BBC611897AC1840F49
SHA-256:	6883F053D7819E2C904FDF5779657508273AB67846779DCB27236F2EAB33FF4F
SHA-512:	B9949AE1DAB334B8CA41514F38E3AD5373137963F6B051BDCEF24F648F5D5CA5CC2DA1C32BEC49FCC74772CBB53835C72324ECECCE7FE8D8D71F8E7E895A156
Malicious:	false
Reputation:	low
Preview:	.....9..... ....

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):	949
Entropy (8bit):	3.2488925165397444
Encrypted:	false
SSDEEP:	12:3olydJhzIgEYOEPlpxlpNVOr1XsAHIDLiBhWZcc5lptlpl:34S1NsylrlJUczSHKlLlL

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
MD5:	3B9601A2638285AE0FB5C035E2FF7424
SHA1:	3C43FDBE791365C527F3156F4E9E023E6A5EEE92
SHA-256:	35096CEB1F5160856D9EDCE638C129F126870143EFC8D1A09698A6A11B03BAAA
SHA-512:	8BD13980EBE3AA9D327A99BFEDA5F5C6ACB010C5B69BBBF0F19D74C775E642F293355F694B8039B21C71A4CEEB6C404D689248650B7721FC0FDAD6F8034CCD64
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...2bd33470_156d_4f3c_b99b_7000b8849e3a.....w.....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....1.,..... ...http://tonysglovesandsafety.com/.....h.....`.....V.....V.....H... ...h.t.t.p.:././.t.o.n.y.s.g.l.o.v.e.s.a.n.d.s.a.f.e.t.y...c.o.m./.....8.....0.....8..... ....http://tonysglovesandsafety.com/....?{..C'/..... .....

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):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....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):	5.183336207475393
Encrypted:	false
SSDEEP:	6:mMoVq2Pwkn23iKKdK8aPrqIFUtp1h0gZmwP1zARSIkwOwkn23iKKdK8amLJ:loVvYf5KkL3FUtp1yg/P1z3I5Jf5KkQJ
MD5:	9CFC29BBA58F4805EA287B33E092B4E0
SHA1:	3B174D608527A5C364BF8AEF487EEFC78DB04743
SHA-256:	244DB1ABC2973ECF786E50541D77B687CB70A2900BE3F80CA1B6917B52B56096
SHA-512:	A2CF0E882C4604C1DAD8DEE661A5589FD9229A8A4935E80898BB2A02B90DA19B164B2176C7EEE73AF5EB6413B07105F23A0BD6322EA190F8F02671CCE369FC1F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.444 1254 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-22:34:11.446 1254 Recovering log #3.2021/08/03-22:34:11.447 1254 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):	5.183336207475393
Encrypted:	false
SSDEEP:	6:mMoVq2Pwkn23iKKdK8aPrqIFUtp1h0gZmwP1zARSIkwOwkn23iKKdK8amLJ:loVvYf5KkL3FUtp1yg/P1z3I5Jf5KkQJ
MD5:	9CFC29BBA58F4805EA287B33E092B4E0
SHA1:	3B174D608527A5C364BF8AEF487EEFC78DB04743
SHA-256:	244DB1ABC2973ECF786E50541D77B687CB70A2900BE3F80CA1B6917B52B56096
SHA-512:	A2CF0E882C4604C1DAD8DEE661A5589FD9229A8A4935E80898BB2A02B90DA19B164B2176C7EEE73AF5EB6413B07105F23A0BD6322EA190F8F02671CCE369FC1 F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.444 1254 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-22:34:11.446 1254 Recovering log #3.2021/08/03-22:34:11.447 1254 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):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4 C
Malicious:	false
Reputation:	low
Preview:	.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):	5.170079501676875
Encrypted:	false
SSDEEP:	6:mS1Uq4q2Pwkn23iKKdK8NIFUtpZwJZmwPZXDkwOwkn23iKKdK8+eLJ:bH4vYf5KkpFUtpCJ/PZD5Jf5KkqJ
MD5:	3FF6F38A7595E7B0A5583E94A3DB8800
SHA1:	F02B99B3F0E5F962C8E3F968D3118ACF57DB8F2E
SHA-256:	FF608DE01ACD18505376FD4B10B64BEF83A980333C9DC8940C40A4747E837C8A
SHA-512:	A5617B62E49CED0F4E189FB984B97D6090AB3961135F8320FE0D8F7166F8CD9F26F0378B458770696D654A3F0BBA8354B8F297E4962714503A0F07960F5836F4
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:15.208 1724 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-22:34:15.210 1724 Recovering log #3.2021/08/03-22:34:15.211 1724 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.olde (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.170079501676875
Encrypted:	false
SSDEEP:	6:mS1Uq4q2Pwkn23iKKdK8NIFUtpZwJZmwPZXDkwOwkn23iKKdK8+eLJ:bH4vYf5KkpFUtpCJ/PZD5Jf5KkqJ
MD5:	3FF6F38A7595E7B0A5583E94A3DB8800

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.olde (copy)	
SHA1:	F02B99B3F0E5F962C8E3F968D3118ACF57DB8F2E
SHA-256:	FF608DE01ACD18505376FD4B10B64BEF83A980333C9DC8940C40A4747E837C8A
SHA-512:	A5617B62E49CED0F4E189FB984B97D6090AB3961135F8320FE0D8F7166F8CD9F26F0378B458770696D654A3F0BBA8354B8F297E4962714503A0F07960F5836F4
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:15.208 1724 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-22:34:15.210 1724 Recovering log #3.2021/08/03-22:34:15.211 1724 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
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+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_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):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
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+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
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=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.2650330889678765
Encrypted:	false
SSDEEP:	6:mRzvH+q2Pwkn23iKKdK25+Xqx8chI+IFUtpSzzeZmwPSpLVkwOwkn23iKKdK25+M:iyvYf5KkTXfchI3FUtpS/e/PSpR5Jf5G
MD5:	8F00D1FCA76D0B867D8312922F1101DF
SHA1:	0DB27BD74D46AA004B457A841787AD0DCCEEFE8A
SHA-256:	F98DFC32AEAE9FC3F91968DF3C573523919F9CC11F48CC31B9B43768AAF44CF1
SHA-512:	CC1FC0FABBB771802C287D32E7B8DC6D2A56C927862476F82DA65380A587BF847D60661C475FC44F9749A6420346A72BAB85888152B12BB1BDAE745BCD1825B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.880 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-22:34:23.887 17d8 Recovering log #3.2021/08/03-22:34:23.895 17d8 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):	5.2650330889678765
Encrypted:	false
SSDEEP:	6:mRzvH+q2Pwkn23iKKdK25+Xqx8chI+IFUtpSzzeZmwPSpLVkwOwkn23iKKdK25+M:iyvYf5KkTXfchI3FUtpS/e/PSpR5Jf5G
MD5:	8F00D1FCA76D0B867D8312922F1101DF
SHA1:	0DB27BD74D46AA004B457A841787AD0DCCEEFE8A
SHA-256:	F98DFC32AEAE9FC3F91968DF3C573523919F9CC11F48CC31B9B43768AAF44CF1
SHA-512:	CC1FC0FABBB771802C287D32E7B8DC6D2A56C927862476F82DA65380A587BF847D60661C475FC44F9749A6420346A72BAB85888152B12BB1BDAE745BCD1825B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Preview:	2021/08/03-22:34:23.880 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-22:34:23.887 17d8 Recovering log #3.2021/08/03-22:34:23.895 17d8 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):	5.206462391951471
Encrypted:	false
SSDEEP:	6:mRmWdrFN+q2Pwkn23iKKdK25+XuoIFUtpS7NdXZmwPSNVkwOwkn23iKKdK25+Xu6:imWdRIvYf5KkTXYFUtpS5dX/PSz5Jf5X
MD5:	DDD3EF389E9CBC865F095D1EAE07BB47
SHA1:	C62926C305B05D22F062809030FC5BB443A747ED
SHA-256:	88A986D6392EC504256EE7D0B16F5048AC30A33F869927BC4982EBD577894850
SHA-512:	37D529B1D7D20D75F593912A4EA389D16B301D595C28C6B52381B60C8F4D8DD81EA9AF105941D32EBF8C41D8D4924C24C20B0A5AB323610002CE610C8ABBEF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.734 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-22:34:23.800 17d8 Recovering log #3.2021/08/03-22:34:23.815 17d8 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):	5.206462391951471
Encrypted:	false
SSDEEP:	6:mRmWdrFN+q2Pwkn23iKKdK25+XuoIFUtpS7NdXZmwPSNVkwOwkn23iKKdK25+Xu6:imWdRIvYf5KkTXYFUtpS5dX/PSz5Jf5X
MD5:	DDD3EF389E9CBC865F095D1EAE07BB47
SHA1:	C62926C305B05D22F062809030FC5BB443A747ED
SHA-256:	88A986D6392EC504256EE7D0B16F5048AC30A33F869927BC4982EBD577894850
SHA-512:	37D529B1D7D20D75F593912A4EA389D16B301D595C28C6B52381B60C8F4D8DD81EA9AF105941D32EBF8C41D8D4924C24C20B0A5AB323610002CE610C8ABBEF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.734 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-22:34:23.800 17d8 Recovering log #3.2021/08/03-22:34:23.815 17d8 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):	5.25222978593124
Encrypted:	false
SSDEEP:	6:mRdCBt+q2Pwkn23iKKdKWT5g1IdqIFUtpSdV5ZmwPSdLVkwOwkn23iKKdKWT5g1L:idCBovYf5Kkg5gSRFUtpSdV5/PSdR5Jb
MD5:	A4ACCD08A8A54762D23855F8BC17D434
SHA1:	66CEAEA08B262020F2392D168D6DA98E85663394
SHA-256:	44C5D2037E030B65E9ADF6F613C8C691FCE43F396441C32824BB7C00D2DA998C
SHA-512:	C0058DE57BAA1B8F19A28621933D6634BFCB63DA67BA13213A54F8B8E379671883AC32F8164EC987E6C8BAF86ABE0638B6269848E4CF71A732471C2510C5011B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.683 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-22:34:23.688 17d8 Recovering log #3.2021/08/03-22:34:23.693 17d8 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.oldd (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.25222978593124

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.oldd (copy)	
Encrypted:	false
SSDEEP:	6:mRdCBt+q2Pwkn23iKKdKWT5g1IdqIFUtpSdV5ZmwPSdLVkwOwkn23iKKdKWT5g1L:idCBovYf5Kkg5gSRFUtpSdV5/PSdR5Jb
MD5:	A4ACCD08A8A54762D23855F8BC17D434
SHA1:	66CEAEA08B262020F2392D168D6DA98E85663394
SHA-256:	44C5D2037E030B65E9ADF6F613C8C691FCE43F396441C32824BB7C00D2DA998C
SHA-512:	C0058DE57BAA1B8F19A28621933D6634BFCB63DA67BA13213A54F8B8E379671883AC32F8164EC987E6C8BAF86ABE0638B6269848E4CF71A732471C2510C5011B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.683 17d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-22:34:23.688 17d8 Recovering log #3.2021/08/03-22:34:23.693 17d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09865412557404674
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvARpSnVD3oOo/lCxthiZUCGCxC+/er/lNktb/RpN:TL+A/RVD3oNuQCCGI/SC
MD5:	7148D80632E71A0E7280017BF56B8A62
SHA1:	70836B022C2256266DDB8AAD5CF761C227FAC320
SHA-256:	3C0A0064BD82F9C1130FBB86AFECFB6F35C58716C4D3815E358B83B061D63CDD
SHA-512:	E15DCE0455FB6F9DB2447685072B143FF68453B7A07BD5B9C7A754F00B0EB7A6EB922E56BED4422744484D74B4986FE1FAC3493C9ABDCECB4800D94D396B0C1
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.225003968461967
Encrypted:	false
SSDEEP:	12:2uQPIQdzdZkxwXZvGSe+UYpxJ/Cu4dywRBk778B/xgs1z7P33yVDaxcfyu:25PIQdzvkMZG+ZpxJr4kcY78BJgs1zLW
MD5:	D0127C7ECB27753D00876AED25DEEEDA
SHA1:	DCB190189458AEF1DAA4E46E99D667B1BFE6754F
SHA-256:	C9A80394B5A774F250820E2061199E95852A4BF0CFA2446F21772A2FA13D8612
SHA-512:	18F3B9F0C92E7FAAB0E52BC24CCE5068B07DFC50199E4AB710C2526A8BB12932D99AA914618220D1F4597AEA63DF8EABB49D98760896C80824BFCC15AF4392EF
Malicious:	false
Reputation:	low
Preview:	....."5....com..http..tonysglovesandsafety.....*M.....com.....http.....tonysglovesandsafety.....2.....a.....c.....d.....e.....f.....g.....h.....l.....m.....n.....o.....p.....s.....t.....v.....y.....:8.....BT...P..... .....* http://tonysglovesandsafety.com/2....:.....J.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33356
Entropy (8bit):	0.04733536188185292
Encrypted:	false
SSDEEP:	6:JSmpAv/5nnGflnrAfg9bNFlWCj/l1OhKl3n:omWQdUqLBj/h3n
MD5:	7BB0554CF9D3E57C4FCD21887DCA1906
SHA1:	6A75C26684E3C3AF27107FD1449D935E526B4239
SHA-256:	C59B83FE255BEC6D87E1138BE4F593E4B83295E6DF47DA0C602C4C4DAD0BC366
SHA-512:	124DF89D49295DFE3123DD46FA75DA567D86B3B4E47B0307B974B32A962851F71820E990C1D4D073C764317F2D5298698DCC266F2381D7393B015939A943E353
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Preview:	.....f..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	949
Entropy (8bit):	3.2488925165397444
Encrypted:	false
SSDEEP:	12:3olydJhzIgEYOEPlpxlpNVOr1XsAHIDLiBhWZcc5lptlpl:34S1NsylrlJUczSHKlLlL
MD5:	3B9601A2638285AE0FB5C035E2FF7424
SHA1:	3C43FDBE791365C527F3156F4E9E023E6A5EEE92
SHA-256:	35096CEB1F5160856D9EDCE638C129F126870143EFC8D1A09698A6A11B03BAAA
SHA-512:	8BD13980EBE3AA9D327A99BFEDA5F5C6ACB010C5B69BBBF0F19D74C775E642F293355F694B8039B21C71A4CEEB6C404D689248650B7721FC0FDAD6F8034CCD64
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...2bd33470_156d_4f3c_b99b_7000b8849e3a.....w..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....1.,..... ...http://tonysglovesandsafety.com/..... .....h.....`.....V.....V.....H... ...h.t.t.p.:././.t.o.n.y.s.g.l.o.v.e.s.a.n.d.s.a.f.e.t.y...c.o.m./.....8..... 0.....8..... ....http://tonysglovesandsafety.com/....?{..C'/..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabson (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):	2955
Entropy (8bit):	5.476962976394289
Encrypted:	false
SSDEEP:	48:fsXGWrY7a72Ml8dbo7LCbQSefgGLNrS0U9RdiN9nrA:f2r2a72M+dbo7LCbQ5fgG5rS0lrA
MD5:	50D4C6B60C2ACCF6593B6E8B0156E08B
SHA1:	E803E1948C50B0AE42290709ED86BC6DBC12598C
SHA-256:	E8F904B05E1EB6368E612B8D964B9A395CA3FC0518ED48BD02682DBDFA080DA6
SHA-512:	67175B7ABEFA43F6A51A11BCF2931B7BD3BB51E7808125DCA1059A6F3690EBCA3C365178807BFBB29EF0BFD4DB00AC578839A01F589F05E9237123D2A5DEAAEB
Malicious:	false
Reputation:	low
Preview:	.9....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.ldGenerator.cast.RequestIdGenerator..303862000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 22:34:27.65][INFO][mr.Init] MR instance ID: a08b9e75-9906-4b43-b908-305fb21edeee\n","[2021-08-03 22:34:27.65][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 22:34:27.65][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 22:34:27.65][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 22:34:27.65][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 22:34:27.65][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 22:34:27.65][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.116429647342277
Encrypted:	false
SSDEEP:	6:mw+q2Pwkn23iKKdK8a2jMGIFUtpJrZmwPmLVkwOwkn23iKKdK8a2jMmLJ:OvYf5Kk8EFUtpJr/Po5Jf5Kk8bJ
MD5:	A39E79178EAFF42D29DF99D11B4F1982
SHA1:	84B6FA635C57D20D6D421E03F2B6210681CD1C84
SHA-256:	88BDB47D268849A7354ABDD1823FEFC119F2BCF226A7A891ECFE651FB8B7E605
SHA-512:	802CED48D5703DCD31502912AB2522E5B73D1C28446192C12D739ED2AAD037EDA219C574A286D45EB8521433580277B68CB4D752D7270359F449941797CB4A1E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.110 248 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:34:11.112 248 Recovering log #3.2021/08/03-22:34:11.113 248 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.oldTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.116429647342277
Encrypted:	false
SSDEEP:	6:mw+q2Pwkn23iKKdK8a2jMGIFUtpJrZmwPmLVkwOwkn23iKKdK8a2jMmLJ:OvYf5Kk8EFUtpJr/Po5Jf5Kk8bJ
MD5:	A39E79178EAFF42D29DF99D11B4F1982
SHA1:	84B6FA635C57D20D6D421E03F2B6210681CD1C84
SHA-256:	88BDB47D268849A7354ABDD1823FEFC119F2BCF226A7A891ECFE651FB8B7E605
SHA-512:	802CED48D5703DCD31502912AB2522E5B73D1C28446192C12D739ED2AAD037EDA219C574A286D45EB8521433580277B68CB4D752D7270359F449941797CB4A1E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.110 248 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:34:11.112 248 Recovering log #3.2021/08/03-22:34:11.113 248 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):	5.214256088471762
Encrypted:	false
SSDEEP:	6:mAslyq2Pwkn23iKKdKgXz4rRIFUtp5XJ11ZmwP5ohRkwOwkn23iKKdKgXz4q8LJ:p1vYf5KkgXiuFUtp5XJ11/P5U5Jf5Kkt
MD5:	FDA570316E0EF48321C276E7FEDB9F51

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
SHA1:	04065CA9EBEE31F190E58D7586F2D64B17C3FCEF
SHA-256:	8C02C0DE289112A2B4DE243BC170A8B7D06C7BD3EA9A6269AFDB23D61E5D2E0A
SHA-512:	04BC1510681DC1DCF2EF9C58B991FF6B02C452254D9E7736F7491FFF7E256631936D0F567D7A445F0128D6D99A450E3DC7F8500AFDB9C0DBABEDFA8A5A4B96
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.480 1794 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-22:34:11.483 1794 Recovering log #3.2021/08/03-22:34:11.484 1794 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):	5.214256088471762
Encrypted:	false
SSDEEP:	6:mAslyq2Pwkn23iKKdKgXz4rRIFUtp5XJ11ZmwP5ohRkwOwkn23iKKdKgXz4q8LJ:p1vYf5KkgXiuFUtp5XJ11/P5U5Jf5Kkt
MD5:	FDA570316E0EF48321C276E7FEDB9F51
SHA1:	04065CA9EBEE31F190E58D7586F2D64B17C3FCEF
SHA-256:	8C02C0DE289112A2B4DE243BC170A8B7D06C7BD3EA9A6269AFDB23D61E5D2E0A
SHA-512:	04BC1510681DC1DCF2EF9C58B991FF6B02C452254D9E7736F7491FFF7E256631936D0F567D7A445F0128D6D99A450E3DC7F8500AFDB9C0DBABEDFA8A5A4B96
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.480 1794 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-22:34:11.483 1794 Recovering log #3.2021/08/03-22:34:11.484 1794 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):	5771
Entropy (8bit):	5.176057858089573
Encrypted:	false
SSDEEP:	96:n1LgU9oNO5VJusmaffIKIo5k0JCKL84k31abOTlVuHn:n1Lt9wgeHaffIeh4K7k3s
MD5:	BF021DC24E58D4DAF4ACA96768FB97EA
SHA1:	1E39358BA935F65E54861964D2DFD94ECACB8AF6
SHA-256:	69FD44F5C5D558E8D9DE6C1EF88995C73AC16C4EDC273CFD165E66DCC785D38D
SHA-512:	5349BFCEC571EFF9C8E5310688CCD0A2CF7C7F216F90DA174F54CA9D73D95E0631AE8DD03EFA54708090C85C7F13AAF0FAF1A8F33302C3BAF8823377FE256E C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272496451438026","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\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):	22601
Entropy (8bit):	5.536443225339621
Encrypted:	false
SSDEEP:	384:ZqitkwLlntXk1kXqKf/pUZNCgVLH2HfDcrUvHGZnZ6lPc4X:pLlJk1kXqKf/pUZNCgVLH2HforUfGZnc
MD5:	797664830A5544C1EA100D85F15C5F1F
SHA1:	DDCC2272AA71248A0CDA40BB49FF20397134AD1C
SHA-256:	9F4056E0544D87CE2CFD8113A07B0F5153F248F99C5783EB2B96AF38F6E64993
SHA-512:	A3265CAC7BF5F32193A7F84C0F7D8659F332FAC0377CA93A2C118F90991FA1B7AC789BFA2BED1F9A307240B9A5290853B21794C4C68F52E8EC7D9585AC95271
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
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":"13272496451041931","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	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):	5.132254156403785
Encrypted:	false
SSDEEP:	6:m3ZSVq2Pwkn23iKKdKrQMxIFUtpjSgZmwPm0IkwOwkn23iKKdKrQMFLJ:HVvYf5KkCFUtpug/Pm0I5Jf5KktJ
MD5:	2BA75BACC081F0CB9BE591B2FD4A1B14
SHA1:	22A3421CB144904DFBEAE34B86CABC8CD3251F2C
SHA-256:	11EDF33CE11EC7B134CB7C959A2B4E0C961D1E2CA8E692EC22F798532FA16FEC
SHA-512:	54C719AB5EBB30FAE30D7AE08747C1B5B620E4F0971E4E5DAF6EBB6EF28AD9055230C3C604EEE5BDEBF51B8BD437E64F7283A46D54B76ED99FD56D04EEF26F94
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.355 1254 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-22:34:11.383 1254 Recovering log #3.2021/08/03-22:34:11.384 1254 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):	5.132254156403785
Encrypted:	false
SSDEEP:	6:m3ZSVq2Pwkn23iKKdKrQMxIFUtpjSgZmwPm0IkwOwkn23iKKdKrQMFLJ:HVvYf5KkCFUtpug/Pm0I5Jf5KktJ
MD5:	2BA75BACC081F0CB9BE591B2FD4A1B14
SHA1:	22A3421CB144904DFBEAE34B86CABC8CD3251F2C
SHA-256:	11EDF33CE11EC7B134CB7C959A2B4E0C961D1E2CA8E692EC22F798532FA16FEC
SHA-512:	54C719AB5EBB30FAE30D7AE08747C1B5B620E4F0971E4E5DAF6EBB6EF28AD9055230C3C604EEE5BDEBF51B8BD437E64F7283A46D54B76ED99FD56D04EEF26F94
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.355 1254 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-22:34:11.383 1254 Recovering log #3.2021/08/03-22:34:11.384 1254 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.1369470774888555
Encrypted:	false
SSDEEP:	6:myGQyq2Pwkn23iKKdK7Uh2ghZIFUtp7zRG1ZmwP70aYQRkwOwkn23iKKdK7Uh2gd:6VvYf5KkIhHh2FUtpBG1/PQRI5Jf5Kks
MD5:	C4A1221079D17E25D493C12667CF1FC3
SHA1:	AFBC0B8019BFBE5039335183DD33666D586BFBEF
SHA-256:	B93C92466547C854C1073FBCD70E7544D975BA011269F54B2FAC86BEDF1C517E
SHA-512:	B9B71BE8DB6E090386A0A29CE9AC488E4A2420FBC767934B11C77277734A17B79FA4A6D4273F6FF1C4BFBDB30205CD00A4DB4BA123ED6BB03FB6B44DAC687F02
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.064 1630 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-22:34:11.067 1630 Recovering log #3.2021/08/03-22:34:11.068 1630 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	5.1369470774888555
Encrypted:	false
SSDEEP:	6:myGQyq2Pwkn23iKKdK7Uh2ghZIFUtp7zRG1ZmwP70aYQRkwOwkn23iKKdK7Uh2gd:6VvYf5KkIhHh2FUtpBG1/PQRI5Jf5Kks
MD5:	C4A1221079D17E25D493C12667CF1FC3
SHA1:	AFBC0B8019BFBE5039335183DD33666D586BFBEF
SHA-256:	B93C92466547C854C1073FBCD70E7544D975BA011269F54B2FAC86BEDF1C517E
SHA-512:	B9B71BE8DB6E090386A0A29CE9AC488E4A2420FBC767934B11C77277734A17B79FA4A6D4273F6FF1C4BFBDB30205CD00A4DB4BA123ED6BB03FB6B44DAC687F02
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.064 1630 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-22:34:11.067 1630 Recovering log #3.2021/08/03-22:34:11.068 1630 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.207828036986077
Encrypted:	false
SSDEEP:	6:m0dlWM+q2Pwkn23iKKdKusNpV/2jMGIFUtpxvUtz1ZmwPxvUtlWMVkwOwkn23iK4:PlL+vYf5KkFFUtpxq/PxiLV5Jf5KkOJ
MD5:	39192815A2D216E16F5F7938AF6AD950
SHA1:	0929ED1B51B68ED00CEAC4A5D9B8F5438FE7257B
SHA-256:	8592C8F33B4F1F7E2AD140D903181922126F144D7A8B3B95EEC78ABB44791E10

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
SHA-512:	7DD79169F8535A415C9C29A084C7CEDD00ACFF4760F64090C753398E7637C4C875102C3ED1D68BE731B2E57C3AA035DF705A1C1684EE4A0C6BEAC71E9AAA4E D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.397 12ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:34:11.400 12ac Recovering log #3.2021/08/03-22:34:11.400 12ac 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):	5.207828036986077
Encrypted:	false
SSDEEP:	6:m0dlWM+q2Pwkn23iKKdKusNpV/2jMGIFUtpxvUtz1ZmwPxvUtlWMVkwOwkn23iK4:PlL+vYf5KkFFUtpxq/PxiLV5Jf5KkOJ
MD5:	39192815A2D216E16F5F7938AF6AD950
SHA1:	0929ED1B51B68ED00CEAC4A5D9B8F5438FE7257B
SHA-256:	8592C8F33B4F1F7E2AD140D903181922126F144D7A8B3B95EEC78ABB44791E10
SHA-512:	7DD79169F8535A415C9C29A084C7CEDD00ACFF4760F64090C753398E7637C4C875102C3ED1D68BE731B2E57C3AA035DF705A1C1684EE4A0C6BEAC71E9AAA4E D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.397 12ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:34:11.400 12ac Recovering log #3.2021/08/03-22:34:11.400 12ac Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"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):	5.2666138965504175
Encrypted:	false
SSDEEP:	12:f4vYf5KkmiuFUtp5IbJ/P5XqD5Jf5Kkm2J:CYf5KkSgLuXeJf5Kkr
MD5:	DB26C7DF3066EEFF7CB3976850D58A03
SHA1:	CCF21E6664A59FF68D44CEDEEB4B86C10501D595
SHA-256:	44D58AC3E17A073994247751E20C7CF8FA3B5F6549191208684F74FFB701F6C3
SHA-512:	359B573F81E769180BDD4FAC5A0862B31DA437081CAE88ACBE480022F38771D46AF53276516D942EFDC36D3BFFB15893CE6305B7DE2D737A750B083188CFB4D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.477 1724 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-22:34:11.481 1724 Recovering log #3.2021/08/03-22:34:11.483 1724 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):	5.2666138965504175
Encrypted:	false
SSDEEP:	12:f4vYf5KkmiuFUtp5IbJ/P5XqD5Jf5Kkm2J:CYf5KkSgLuXeJf5Kkr
MD5:	DB26C7DF3066EEFF7CB3976850D58A03
SHA1:	CCF21E6664A59FF68D44CEDEEB4B86C10501D595
SHA-256:	44D58AC3E17A073994247751E20C7CF8FA3B5F6549191208684F74FFB701F6C3
SHA-512:	359B573F81E769180BDD4FAC5A0862B31DA437081CAE88ACBE480022F38771D46AF53276516D942EFDC36D3BFFB15893CE6305B7DE2D737A750B083188CFB4D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.477 1724 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-22:34:11.481 1724 Recovering log #3.2021/08/03-22:34:11.483 1724 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):	5.269440679911068
Encrypted:	false
SSDEEP:	6:mb4aM+q2Pwkn23iKKdKusNpZQMxIFUtpYrZmwPYSaMVkwOwkn23iKKdKusNpZQMT:ZH+vYf5KkMFUtpO/PnV5Jf5KkTJ
MD5:	9BBD245485C6E024DE07BD870832B79D
SHA1:	F331BA71604A42E1559030899B3E80994A980FF8
SHA-256:	A7B12F499A46536F36E126F1E21CE50B33D16174C5C5CDFDEFE9F0C3FCBF6601
SHA-512:	EDE2C8E7918C6785BC64817C463712AC8E586B0ADC237B82223CBF45DBE13D4C4F73DDBC0756419BD79888643E9AF8F682048CE6DF5BBA9A0A315418171200A A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:29.456 13ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-22:34:29.457 13ac Recovering log #3.2021/08/03-22:34:29.458 13ac 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):	5.269440679911068
Encrypted:	false
SSDEEP:	6:mb4aM+q2Pwkn23iKKdKusNpZQMxIFUtpYrZmwPYSaMVkwOwkn23iKKdKusNpZQMT:ZH+vYf5KkMFUtpO/PnV5Jf5KkTJ
MD5:	9BBD245485C6E024DE07BD870832B79D
SHA1:	F331BA71604A42E1559030899B3E80994A980FF8
SHA-256:	A7B12F499A46536F36E126F1E21CE50B33D16174C5C5CDFDEFE9F0C3FCBF6601

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old (copy)	
SHA-512:	EDE2C8E7918C6785BC64817C463712AC8E586B0ADC237B82223CBF45DBE13D4C4F73DDBC0756419BD79888643E9AF8F682048CE6DF5BBA9A0A315418171200A A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:29.456 13ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-22:34:29.457 13ac Recovering log #3.2021/08/03-22:34:29.458 13ac 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\ae6ba29c-c83d-46cf-bdb4-73ccf993e989.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\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
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.21797957794646
Encrypted:	false
SSDEEP:	12:2OVvYf5KkkGHArBFUtpGsg/PGAI5Jf5KkkGHAryJ:BYf5KkkGgPgbJf5KkkGga
MD5:	5EBA87F42AD9B9B58C9BED6A67E2CD3B
SHA1:	A5EE7252E3FD6DD98C1B65E26484ACB5F4B1476A
SHA-256:	58683268E975718331BCFCC4171643FFEF0A4CB37B0CF03F9B3B6AA20FCF0B54
SHA-512:	23B09101ADB19511C10480E86B3C12D570AD568E12707F41023D83D9FF89D9A2A7B842B3C6332D5EA66DCD508B3C3181BDB9839E91448D03680FD3CBE8CED28
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:24.500 1658 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:34:24.511 1658 Recovering log #3.2021/08/03-22:34:24.515 1658 Reusing old log C:\Users\user\A ppData\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.21797957794646
Encrypted:	false
SSDEEP:	12:2OVvYf5KkkGHArBFUtpGsg/PGAI5Jf5KkkGHAryJ:BYf5KkkGgPgbJf5KkkGga
MD5:	5EBA87F42AD9B9B58C9BED6A67E2CD3B
SHA1:	A5EE7252E3FD6DD98C1B65E26484ACB5F4B1476A
SHA-256:	58683268E975718331BCFCC4171643FFEF0A4CB37B0CF03F9B3B6AA20FCF0B54
SHA-512:	23B09101ADB19511C10480E86B3C12D570AD568E12707F41023D83D9FF89D9A2A7B842B3C6332D5EA66DCD508B3C3181BDB9839E91448D03680FD3CBE8CED28
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:24.500 1658 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:34:24.511 1658 Recovering log #3.2021/08/03-22:34:24.515 1658 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 State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
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):	5.186999179949324
Encrypted:	false
SSDEEP:	12:2nUG+vYf5KkkGHArqiuFUtpG3/PG7V5Jf5KkkGHArq2J:s8Yf5KkkGgCg3Jf5KkkGg7
MD5:	8F7A86F964D21CFC8935179BF03D2434
SHA1:	5989ADE130D9677D0766ED4C7DFBDCDFBE7FE293
SHA-256:	5BD54C90AA525E8139EEEFEA6C1488B1C1359D43B725D91BCDB4F9E93E863430
SHA-512:	B62109931B6CD2E84074525087DF6FE0F494F2249AE06B47275856FF1CDCCBB41470C32E22364CD199F1197B0C280AF7371F42E4F9F20CC2D627CB7C40D2BFE(
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:24.502 13ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-22:34:24.511 13ac Recovering log #3.2021/08/03-22:34:24.515 13ac 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):	5.186999179949324
Encrypted:	false
SSDEEP:	12:2nUG+vYf5KkkGHArqiuFUtpG3/PG7V5Jf5KkkGHArq2J:s8Yf5KkkGgCg3Jf5KkkGg7
MD5:	8F7A86F964D21CFC8935179BF03D2434
SHA1:	5989ADE130D9677D0766ED4C7DFBDCDFBE7FE293

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
SHA-256:	5BD54C90AA525E8139EEEFEA6C1488B1C1359D43B725D91BCDB4F9E93E863430
SHA-512:	B62109931B6CD2E84074525087DF6FE0F494F2249AE06B47275856FF1CDCCBB41470C32E22364CD199F1197B0C280AF7371F42E4F9F20CC2D627CB7C40D2BFE(
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:24.502 13ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/03-22:34:24.511 13ac Recovering log #3.2021/08/03-22:34:24.515 13ac Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.191906831406681
Encrypted:	false
SSDEEP:	12:+VvYf5KkkGHArAFUtpGQg/PGQI5Jf5KkkGHArfJ:AYf5KkkGgkgTJf5KkkGgV
MD5:	0D02BA9522BA8DD74F9E2CF060B6C0DC
SHA1:	2F3A1A36CE87FCB8DAF7545D9266DC1A310F7067
SHA-256:	6EC722D38DCF663DA6844BABEE8ED5DF3891BCFCEC1F7F36E2634667C454D1B9
SHA-512:	0525223243D65D6871586F595C834294DBBE170055DC4C645D4F746DE11A013620D9D058E5DB514DADEE71556659D5AD1724BFF4E5571521105438D0B168A3EA
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:40.060 1658 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/03-22:34:40.063 1658 Recovering log #3.2021/08/03-22:34:40.063 1658 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.c (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.191906831406681
Encrypted:	false
SSDEEP:	12:+VvYf5KkkGHArAFUtpGQg/PGQI5Jf5KkkGHArfJ:AYf5KkkGgkgTJf5KkkGgV
MD5:	0D02BA9522BA8DD74F9E2CF060B6C0DC
SHA1:	2F3A1A36CE87FCB8DAF7545D9266DC1A310F7067
SHA-256:	6EC722D38DCF663DA6844BABEE8ED5DF3891BCFCEC1F7F36E2634667C454D1B9
SHA-512:	0525223243D65D6871586F595C834294DBBE170055DC4C645D4F746DE11A013620D9D058E5DB514DADEE71556659D5AD1724BFF4E5571521105438D0B168A3EA
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:40.060 1658 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/03-22:34:40.063 1658 Recovering log #3.2021/08/03-22:34:40.063 1658 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\a664b310-06f2-497d-b3de-b0a180802ba3.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\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.173740267123389
Encrypted:	false
SSDEEP:	6:myzyyq2Pwkn23iKKdKpIFUtp7Ur1ZmwP7U9RkwOwkn23iKKdKa/WLJ:yyvYf5KkmFUtps/P8R5Jf5KkaUJ
MD5:	337D150387217907EC840A84E2B5D9E2
SHA1:	68478DC76DE85012E56E50E4AD31D316C275BF59
SHA-256:	54B0AA17B9F6D48FD9123F26E18093C8948505E0763A4A628A8324070AC26A90
SHA-512:	7C4DBC090A8C6062EA17A180EE31FB062292DEB747EACD67616F4A692CBE661E2414B255B6BAE7FB49B6F1D8C5764602A89C1106A0DF6D32F4A31370D05EDDC
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.067 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-22:34:11.069 1010 Recovering log #3.2021/08/03-22:34:11.069 1010 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):	5.173740267123389
Encrypted:	false
SSDEEP:	6:myzyyq2Pwkn23iKKdKpIFUtp7Ur1ZmwP7U9RkwOwkn23iKKdKa/WLJ:yyvYf5KkmFUtps/P8R5Jf5KkaUJ
MD5:	337D150387217907EC840A84E2B5D9E2
SHA1:	68478DC76DE85012E56E50E4AD31D316C275BF59

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old.. (copy)	
SHA-256:	54B0AA17B9F6D48FD9123F26E18093C8948505E0763A4A628A8324070AC26A90
SHA-512:	7C4DBC090A8C6062EA17A180EE31FB062292DEB747EACD67616F4A692CBE661E2414B255B6BAE7FB49B6F1D8C5764602A89C1106A0DF6D32F4A31370D05EDDC
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:11.067 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-22:34:11.069 1010 Recovering log #3.2021/08/03-22:34:11.069 1010 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):	5.318181762944581
Encrypted:	false
SSDEEP:	12:mQXHVvYf5KkkOrsFUtpWeSg/PW6I5Jf5KkkOrzJ:RXZYf5Kk+grOJf5Kkn
MD5:	0804855C648EA95289F577496BADBB7D
SHA1:	3A5EA445C41063E038ADB1EA136A352CA11CFC9F
SHA-256:	7B606A649940EF9D7C0F13C50AE51DDD1A3FDC4C2F7A0964650C9AF086D4AB22
SHA-512:	DED6A62880F7667ED7519C8692702306CAAB51D61CC522F523C53D64C147F7546CE6D16969C425DCB96D27638734AE53AFC049665F712521EC22205A76F641A2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:27.660 1254 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-22:34:27.661 1254 Recovering log #3.2021/08/03-22:34:27.662 1254 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):	5.318181762944581
Encrypted:	false
SSDEEP:	12:mQXHVvYf5KkkOrsFUtpWeSg/PW6I5Jf5KkkOrzJ:RXZYf5Kk+grOJf5Kkn
MD5:	0804855C648EA95289F577496BADBB7D
SHA1:	3A5EA445C41063E038ADB1EA136A352CA11CFC9F
SHA-256:	7B606A649940EF9D7C0F13C50AE51DDD1A3FDC4C2F7A0964650C9AF086D4AB22
SHA-512:	DED6A62880F7667ED7519C8692702306CAAB51D61CC522F523C53D64C147F7546CE6D16969C425DCB96D27638734AE53AFC049665F712521EC22205A76F641A2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:27.660 1254 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-22:34:27.661 1254 Recovering log #3.2021/08/03-22:34:27.662 1254 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.6 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1041
Entropy (8bit):	5.566473516705512
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeiXzkq/HeUe8zUe3q7wUCUsRUeiQ:Ym6UUhyKUeiYqPeUekUe30wUCUeP
MD5:	EA0869E44DC4A0485D3773666DAF1E42
SHA1:	71286FDA0CDF361729F32135D2F993DEBECAFCC4
SHA-256:	40DFAFE21292DF242879009EA51E592B4D8A2CD38AB495F66A28B5BFA9DFDEA9
SHA-512:	72DACF42913E8233005A7051AD3905DC0653A7E3DD99C41D77F06945A424B14E8E1DB8B579DAE19A2A8182AF8C933EA672181D6B40F57FA476C6CDBD5DEF145
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity.6 (copy)	
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1659558856.811314,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628022856.811319},{"expiry":1632986995.164829,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:F0:F0
MD5:	2972BAE71A0676C43FAF88F8AEE7618B
SHA1:	23C4E5BA708AB1C00A55240CD256FA960BFFD585
SHA-256:	9536CCE216809FB963512A7D18691A916CEC29376DE6AE6561D82DCD0820A22E
SHA-512:	C5721175AD772CE8566948BE0BDF88133D390F5CA25E446AB895C812EA3241346000966E2C5EE23F12ECBBD3B609D439DDB490FECE1FD1AE7D292DDDD6EFF40
Malicious:	false
Reputation:	low
Preview:	....a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168B6
Malicious:	false
Reputation:	low
Preview:	F.....r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ac55fecd-dcbd-410d-8291-8435a4e329ea.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\bb94d782-808e-4601-9edc-08eadfcca2b1.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bb94d782-808e-4601-9edc-08eadfcca2b1.tmp	
Size (bytes):	24064
Entropy (8bit):	5.53426091774292
Encrypted:	false
SSDEEP:	384:ZqitkwLlntXk1kXqKf/pUZNCgVLH2HfDcrUSHGJHG2nZ67c4r:pLlJk1kXqKf/pUZNCgVLH2HforUSGtGT
MD5:	BA7C6B0AFA34BB44B31F04EAA3A82571
SHA1:	65008C375A954ADAD8E5879B10680223187A9791
SHA-256:	386F8C3E537095CE8834698DF57B50C456D18DF58EAABC535B7C78CF420A8ED1
SHA-512:	DC190577A8847ADB89ABDC347A947917B2AD2C7DAAE66FE0EC38C9BD46499C65BA89A79141546062CA950650107D07AEE6DC842CB1D0F24E2B10404B0997F5 0
Malicious:	false
Reputation:	low
Preview:	 {"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13272496451041931","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d9c16df9-9102-4dac-b302-c62503af6c23.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):	22601
Entropy (8bit):	5.536443225339621
Encrypted:	false
SSDEEP:	384:ZqitkwLlntXk1kXqKf/pUZNCgVLH2HfDcrUvHGZnZ6lPc4X:pLlJk1kXqKf/pUZNCgVLH2HforUfGZnc
MD5:	797664830A5544C1EA100D85F15C5F1F
SHA1:	DDCC2272AA71248A0CDA40BB49FF20397134AD1C
SHA-256:	9F4056E0544D87CE2CFD8113A07B0F5153F248F99C5783EB2B96AF38F6E64993
SHA-512:	A3265CAC7BF5F32193A7F84C0F7D8659F332FAC0377CA93A2C118F90991FA1B7AC789BFA2BED1F9A307240B9A5290853B21794C4C68F52E8EC7D9585AC95271(
Malicious:	false
Reputation:	low
Preview:	 {"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13272496451041931","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
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):	4.42697286904894
Encrypted:	false
SSDEEP:	3:tUK6ziRydXZmwv3IzlXUdM0V8sIzlXXDu0WGv:mRiQXZmwPSNUdM0VvSNzu0tv
MD5:	A0D7CA7C4F1D8268451CE1802B4B3928
SHA1:	35336572BEC4E64796E8C2CD6C1230816F2BB057
SHA-256:	65424593F87973D0861B9A250214E86991BB957003986B51D38CD5E1CF4DFA24
SHA-512:	415548E84EC42C7788780D74B6A8929798A679041ADC617063EEA5111211E709381F3DC89C540C57074614E4A4D5B4A7D3D8E8285B7CD582813BE6F316604DAE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.350 17d8 Recovering log #3.2021/08/03-22:34:23.421 17d8 Delete type=0 #3.2021/08/03-22:34:23.422 17d8 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.olde (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.42697286904894
Encrypted:	false
SSDEEP:	3:tUK6ziRydXZmwv3IzlXUdM0V8sIzlXXDu0WGv:mRiQXZmwPSNUdM0VvSNzu0tv
MD5:	A0D7CA7C4F1D8268451CE1802B4B3928
SHA1:	35336572BEC4E64796E8C2CD6C1230816F2BB057
SHA-256:	65424593F87973D0861B9A250214E86991BB957003986B51D38CD5E1CF4DFA24
SHA-512:	415548E84EC42C7788780D74B6A8929798A679041ADC617063EEA5111211E709381F3DC89C540C57074614E4A4D5B4A7D3D8E8285B7CD582813BE6F316604DAE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:23.350 17d8 Recovering log #3.2021/08/03-22:34:23.421 17d8 Delete type=0 #3.2021/08/03-22:34:23.422 17d8 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\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Size (bytes):	338
Entropy (8bit):	5.2233602678768465
Encrypted:	false
SSDEEP:	6:mVBCaM+q2Pwkn23iKKdKfrzAdIFUtpWBzZmwPWBQaMVkwOwkn23iKKdKfrzILJ:ms+vYf5Kk9FUtpWp/PWyHV5Jf5Kk2J
MD5:	828731A1D54248D3B3494C815BA5C383
SHA1:	66F9D4B8510093D5574CBD2A3F44496AE00FCC14
SHA-256:	A4E12355194EBB08DE066DE296809527B69597853D09E98F5F701A9C1094E0E9
SHA-512:	F82D0E644172558AA125A4FB6054471DD9ADF9C400EBE77CF9F5B8F2894EB55E3FBED940A34B52066DF4822A14AC1DDB5672DDFFF82563E356718ABABA46E92F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:27.993 13ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-22:34:27.994 13ac Recovering log #3.2021/08/03-22:34:27.995 13ac 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.2233602678768465
Encrypted:	false
SSDEEP:	6:mVBCaM+q2Pwkn23iKKdKfrzAdIFUtpWBzZmwPWBQaMVkwOwkn23iKKdKfrzILJ:ms+vYf5Kk9FUtpWp/PWyHV5Jf5Kk2J
MD5:	828731A1D54248D3B3494C815BA5C383
SHA1:	66F9D4B8510093D5574CBD2A3F44496AE00FCC14
SHA-256:	A4E12355194EBB08DE066DE296809527B69597853D09E98F5F701A9C1094E0E9
SHA-512:	F82D0E644172558AA125A4FB6054471DD9ADF9C400EBE77CF9F5B8F2894EB55E3FBED940A34B52066DF4822A14AC1DDB5672DDFFF82563E356718ABABA46E92F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:34:27.993 13ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-22:34:27.994 13ac Recovering log #3.2021/08/03-22:34:27.995 13ac 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
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local Statee (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):	6.0796433605983475
Encrypted:	false
SSDEEP:	3072:O8JGaYTJQE+mugy9+QV1T7IRwdfLSNPoFcbXafIB0u1GOJmA3iuRG:ZkxaV+QfT7GSmh2aqfIlUOoSiuRG
MD5:	D348135C6C6496596DA943778B44E78C
SHA1:	1CC67804DCF56A5C269243E3556A8058288DBF6F
SHA-256:	2AF611D894D3FC437E49ECC99B23FE7CD8AA097562B0859E11089132FE808914
SHA-512:	8E3FE81A5E92843A732FDC772163577B665C364A95B5CF82066D27BF738AE076CD65C481129F7E3D0170DCA8B622C9088BE8A9AD99784266DF2D66ED14F33E7(
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":1.628022855165405e+12,"network":1.628022856e+12,"ticks":7447711876.0,"uncertainty":4607845.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715059030"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cached (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7496685214888243
Encrypted:	false
SSDEEP:	384:HnVa6E3hgkjedNSrnvGO3VeMxHclGJQrbI6MxVwgIjr7KmHMr4yOeNOY8uNj1STC:XWRRisd1AePEWMc/zG+KEeuhp
MD5:	FAD85C0CA5529EE363FA691AD16A6A77
SHA1:	20E7AEECBC0EBE044D4994482ABF8C0F5AC4F2A6
SHA-256:	C4291EA8827C102F434D3E45AAA84943F2EEF468E0356C658469CDDE0BDFD267
SHA-512:	7A0DC98C4B48C67BE63104E8DAF9210DFCF71892579BC457DB9D912A74E0E57988D2F33924A8720ADEC325AE9480228D476BE5757C03811E0287A08D42556A03
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\Temp\503aa76f-0f8e-4d52-bcd8-f34d619afaef.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\5a50a613-923e-4421-838a-56ee1997027f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\5a50a613-923e-4421-838a-56ee1997027f.tmp	
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...'].....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	3890
Entropy (8bit):	4.64027751484382
Encrypted:	false
SSDEEP:	48:Eo/oOgsto/oP7Bteo498t4roQva1EzdJdrih1Rr8HF/oyCF/ow+Z/oeTn58tnAmn:FgDJgGDvAENiH58lgZglZgMm8y2t5/O
MD5:	E0FC36CB83B2D5F8BBEFD05F0C146BBD
SHA1:	7897453A022DA301CB4C20B3C3321D6F61D0E30D
SHA-256:	3BED8C3C2EBA56AA635CF0E40D39785C4B5DEC35567F98AB66869559908B1635
SHA-512:	AADE2C10001F66087B8CC9E712309CEF42BEF0B9A1E490CA29B1E56BCF9C48B9029674AD07AC744881909ABC321F62D67402B8CC0D238C1C79AB5B01916D159
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET bc55db7201b5a0e55e280d9fb929ed9334c8c2b9f5a41780f2518eada1af7e8a 8a8b42728d8072ff25d2f2141361e8759000fee43db6e33159865c42ad4a8ec1.SERVER_HANDSHAKE_TRAFFIC_SECRET bc55db7201b5a0e55e280d9fb929ed9334c8c2b9f5a41780f2518eada1af7e8a 8858f7a09d39b0fac03846b819beaf250d3960cd953530c8de0342484d5a2dbf.CLIENT_HANDSHAKE_TRAFFIC_SECRET 8246d3ae3b407ec6d29127c6598978678c6a0c1c9b1018aff95642aa8568bb51 e2b38a05bc2c6363a063a5dd20ef4d0049812685e26e4cc721275c8f46c99518.SERVER_HANDSHAKE_TRAFFIC_SECRET 8246d3ae3b407ec6d29127c6598978678c6a0c1c9b1018aff95642aa8568bb51 f69dab3c9f090f4bce21ff0fa71fd6b982356e239473987abf8af9b9e0268595.CLIENT_HANDSHAKE_TRAFFIC_SECRET 2c6d203cb783cc80f029425e8bb76bc2bd153a272737861e3f0868667c10d88c 29659789e700186c48d92f352a687073578d6970e1f8d33c30e452bbb3eeb0b8.SERVER_HANDSHAKE_TRAFFIC_SECRET 2c6d203cb783cc80f029425e8bb76bc2bd153a272737861e3f0868667c10d88c 8e1b0b5cc9be6934002efbc00f63fd7049a556796b0805b20c22ecd60871e0e4.CLIENT_TRAFFIC_SECRET_0 8246

C:\Users\user\AppData\Local\Temp\d7d988f4-0c41-4ee6-a1f9-874e173c9ac0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...'].....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\ea8a5ab0-d0be-4505-97de-a27be02448e0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp\ea8a5ab0-d0be-4505-97de-a27be02448e0.tmp	
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\f2fa7419-eba0-4c67-b38b-9ee5054cdfa6.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:	.

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 22:34:16.395908117 CEST	192.168.2.4	8.8.8.8	0x41c2	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:34:16.401540995 CEST	192.168.2.4	8.8.8.8	0x23d3	Standard query (0)	tonysglovesandsafety.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:34:16.401567936 CEST	192.168.2.4	8.8.8.8	0x46af	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:34:23.412580013 CEST	192.168.2.4	8.8.8.8	0x5c63	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:34:16.421039104 CEST	8.8.8.8	192.168.2.4	0x41c2	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:34:16.421039104 CEST	8.8.8.8	192.168.2.4	0x41c2	No error (0)	clients.l.google.com		142.250.181.238	A (IP address)	IN (0x0001)
Aug 3, 2021 22:34:16.434343100 CEST	8.8.8.8	192.168.2.4	0x46af	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 22:34:16.592801094 CEST	8.8.8.8	192.168.2.4	0x23d3	No error (0)	tonysglovesandsafety.com		168.206.125.23	A (IP address)	IN (0x0001)
Aug 3, 2021 22:34:23.454000950 CEST	8.8.8.8	192.168.2.4	0x5c63	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:34:23.454000950 CEST	8.8.8.8	192.168.2.4	0x5c63	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- tonysglovesandsafety.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49747	168.206.125.23	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:34:16.798115015 CEST	1054	OUT	GET / HTTP/1.1 Host: tonysglovesandsafety.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:34:17.004409075 CEST	1065	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 20:34:16 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 33 31 39 0d 0a 1f 8b 08 00 00 00 00 00 00 03 7d 54 5d 4f da 50 18 be c6 c4 ff 70 c4 ec 66 09 6b 41 c6 14 aa 37 db cd 6e 96 dd ed ba d0 56 9a 15 4a e0 38 65 64 c9 64 13 51 e7 d4 88 46 91 85 31 fc 20 33 16 a7 c9 54 a0 f3 cf 70 4e eb 15 7f 61 e7 b4 e5 43 59 96 5e b4 7d cf f3 3e cf f3 7e b4 dc 98 a0 46 60 3a 21 82 28 8c 29 33 a3 23 5c ef 2e f2 02 7d 8f 89 90 07 91 28 9f 4c 89 70 da 3d 07 25 cf a4 9b c6 a1 0c 15 71 06 35 1b c6 e9 3e ce 6f a2 d5 32 c7 d8 31 72 98 82 69 72 38 3a f2 38 13 e3 93 b3 72 3c c8 86 12 bc 20 c8 f1 59 f2 14 51 15 35 19 1c f7 fb fd 1f 46 47 c2 aa 90 ce 48 6a 1c 7a 52 f2 7b 31 e8 f5 27 16 42 d6 ab c4 c7 64 25 1d 74 23 6d ad ad 6f bb 09 f4 49 8c 97 e3 99 79 59 80 d1 60 80 65 09 d0 21 f7 b2 8f 00 3f 07 d5 10 05 59 1e 32 61 3e f2 76 36 a9 ce c5 85 20 18 f7 b1 fc d3 09 de d1 05 e3 92 24 d9 12 96 22 f0 06 08 53 54 94 67 a3 30 08 fc 94 56 91 e3 a2 e7 5e c4 31 ef 51 44 89 80 7c 14 44 b5 22 c4 a8 18 87 03 6a 1e a7 38 69 42 7a 26 4d 85 80 c3 32 61 d9 0d ab 49 41 4c 06 bd 89 05 20 f0 a9 a8 28 80 f1 48 40 98 0a 07 7a cd a1 cc 56 11 de 8c 0d f6 84 55 08 d5 18 71 39 9c 64 4b d1 7a fc 2c cb da 25 cd 3b 75 84 55 45 08 01 a7 3f 80 25 97 65 1a 74 0b e9 d1 4e 3a a5 40 9f 33 aa ae 22 3d 00 d6 24 1c 4e 4a 49 bc a9 4a 6f a6 0e 2b f0 f9 08 b6 3f 5f 0b 04 14 39 33 d8 c7 09 bb 32 8e e9 ae 06 c7 44 9d 0d a3 2b 40 76 c5 c5 09 f2 3b 10 51 f8 54 6a da 4d 47 4d d7 cc 75 2f 6a cd d6 fd 60 e9 48 d6 10 d0 19 8c cd e0 e2 12 5d 5a e8 75 cf e0 6c cd 28 7e 36 eb 57 f8 57 16 95 6a 6f c4 30 2e ad a3 d5 0a da af b5 af cf f0 45 05 97 56 f0 ca 1f 94 3f 47 f5 1b d4 28 10 30 59 71 23 7b d3 69 2d 72 4c c2 d2 1a a4 f4 11 43 1b 75 f3 93 8e be 96 d1 c1 f7 4e ab d8 47 a9 f4 93 22 70 17 a7 c8 54 d8 66 47 e7 39 7c 76 88 ca 65 b4 b9 8e f3 bb 2f 5f 1b cd 2d a4 15 fb 8a 96 dc 18 c7 90 a4 7e fa dd d2 ba a1 6b 78 77 b9 dd fc 8d 4b 3f 8d 42 19 ef e4 07 40 1c d3 55 1b a8 97 9a 3b ce b6 f5 1d f3 a4 8a 72 97 ff 31 57 fd 88 cb 47 78 af 8e 36 8f d1 d5 85 d1 dc f8 a7 a9 4e eb 8b b9 76 64 54 34 53 3b b4 60 d4 38 0d d6 af d0 f9 37 b3 be 73 b7 bc 6e ea 7a af a9 9d d6 c1 83 32 b0 25 64 9c d6 d1 46 d5 96 c3 67 55 42 38 8c 24 42 a4 65 6d fd d6 28 d4 da 8d dc f3 17 af da 8d 13 b4 bd 38 28 87 af 97 ee f6 0f c9 91 d1 da 46 67 7b c3 24 78 5f bb fb 58 34 f4 2d 32 43 53 bb 45 da 0f 3b dd 5c 2c 18 97 4d 3b 6e 68 15 63 33 87 b6 ee a7 f7 fa c9 31 ce 8a 75 1f 38 c6 59 59 b2 c3 f6 5f f3 2f 85 06 d1 61 47 05 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 319}T]OPpfkA7nVJ8eddQF1 3TpNaCY^}>~F`:!()3#\.}(Lp=%q5>o21rir8:8r< YQ5FGHjzR{1'Bd%t#moIyY`e!?Y2a>v6 $"STg0V^1QD|D"j8iBz&M2aIAL (H@zVUq9dKz,%;uUE?%etN:@3"=$NJlJo+?_932D+@v;QTjMGMu/j`H]Zul(~6 WWjo0.EV?G(0Yq#{i-rLCuNG"pTfG9|ve/_-~kxwK?B@U;r1WGx6NvdT4S;`87snz2%dFgUB8$Bem(8(Fg{$x_X4-2 CSE;\,M;nhc31u8YY_/aG0
Aug 3, 2021 22:34:17.164823055 CEST	1325	OUT	GET /favicon.ico HTTP/1.1 Host: tonysglovesandsafety.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://tonysglovesandsafety.com/ Accept-Encoding: gzip, deflate Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Aug 3, 2021 22:34:17.371238947 CEST	1326	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 20:34:17 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 33 31 39 0d 0a 1f 8b 08 00 00 00 00 00 00 03 7d 54 5d 4f da 50 18 be c6 c4 ff 70 c4 ec 66 09 6b 41 c6 14 aa 37 db cd 6e 96 dd ed ba d0 56 9a 15 4a e0 38 65 64 c9 64 13 51 e7 d4 88 46 91 85 31 fc 20 33 16 a7 c9 54 a0 f3 cf 70 4e eb 15 7f 61 e7 b4 e5 43 59 96 5e b4 7d cf f3 3e cf f3 7e b4 dc 98 a0 46 60 3a 21 82 28 8c 29 33 a3 23 5c ef 2e f2 02 7d 8f 89 90 07 91 28 9f 4c 89 70 da 3d 07 25 cf a4 9b c6 a1 0c 15 71 06 35 1b c6 e9 3e ce 6f a2 d5 32 c7 d8 31 72 98 82 69 72 38 3a f2 38 13 e3 93 b3 72 3c c8 86 12 bc 20 c8 f1 59 f2 14 51 15 35 19 1c f7 fb fd 1f 46 47 c2 aa 90 ce 48 6a 1c 7a 52 f2 7b 31 e8 f5 27 16 42 d6 ab c4 c7 64 25 1d 74 23 6d ad ad 6f bb 09 f4 49 8c 97 e3 99 79 59 80 d1 60 80 65 09 d0 21 f7 b2 8f 00 3f 07 d5 10 05 59 1e 32 61 3e f2 76 36 a9 ce c5 85 20 18 f7 b1 fc d3 09 de d1 05 e3 92 24 d9 12 96 22 f0 06 08 53 54 94 67 a3 30 08 fc 94 56 91 e3 a2 e7 5e c4 31 ef 51 44 89 80 7c 14 44 b5 22 c4 a8 18 87 03 6a 1e a7 38 69 42 7a 26 4d 85 80 c3 32 61 d9 0d ab 49 41 4c 06 bd 89 05 20 f0 a9 a8 28 80 f1 48 40 98 0a 07 7a cd a1 cc 56 11 de 8c 0d f6 84 55 08 d5 18 71 39 9c 64 4b d1 7a fc 2c cb da 25 cd 3b 75 84 55 45 08 01 a7 3f 80 25 97 65 1a 74 0b e9 d1 4e 3a a5 40 9f 33 aa ae 22 3d 00 d6 24 1c 4e 4a 49 bc a9 4a 6f a6 0e 2b f0 f9 08 b6 3f 5f 0b 04 14 39 33 d8 c7 09 bb 32 8e e9 ae 06 c7 44 9d 0d a3 2b 40 76 c5 c5 09 f2 3b 10 51 f8 54 6a da 4d 47 4d d7 cc 75 2f 6a cd d6 fd 60 e9 48 d6 10 d0 19 8c cd e0 e2 12 5d 5a e8 75 cf e0 6c cd 28 7e 36 eb 57 f8 57 16 95 6a 6f c4 30 2e ad a3 d5 0a da af b5 af cf f0 45 05 97 56 f0 ca 1f 94 3f 47 f5 1b d4 28 10 30 59 71 23 7b d3 69 2d 72 4c c2 d2 1a a4 f4 11 43 1b 75 f3 93 8e be 96 d1 c1 f7 4e ab d8 47 a9 f4 93 22 70 17 a7 c8 54 d8 66 47 e7 39 7c 76 88 ca 65 b4 b9 8e f3 bb 2f 5f 1b cd 2d a4 15 fb 8a 96 dc 18 c7 90 a4 7e fa dd d2 ba a1 6b 78 77 b9 dd fc 8d 4b 3f 8d 42 19 ef e4 07 40 1c d3 55 1b a8 97 9a 3b ce b6 f5 1d f3 a4 8a 72 97 ff 31 57 fd 88 cb 47 78 af 8e 36 8f d1 d5 85 d1 dc f8 a7 a9 4e eb 8b b9 76 64 54 34 53 3b b4 60 d4 38 0d d6 af d0 f9 37 b3 be 73 b7 bc 6e ea 7a af a9 9d d6 c1 83 32 b0 25 64 9c d6 d1 46 d5 96 c3 67 55 42 38 8c 24 42 a4 65 6d fd d6 28 d4 da 8d dc f3 17 af da 8d 13 b4 bd 38 28 87 af 97 ee f6 0f c9 91 d1 da 46 67 7b c3 24 78 5f bb fb 58 34 f4 2d 32 43 53 bb 45 da 0f 3b dd 5c 2c 18 97 4d 3b 6e 68 15 63 33 87 b6 ee a7 f7 fa c9 31 ce 8a 75 1f 38 c6 59 59 b2 c3 f6 5f f3 2f 85 06 d1 61 47 05 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 319}T]OPpfkA7nVJ8eddQF1 3TpNaCY^}>~F`:!()3#\.}(Lp=%q5>o21rir8:8r< YQ5FGHjzR{1'Bd%t#moIyY`e!?Y2a>v6 $"STg0V^1QD|D"j8iBz&M2aIAL (H@zVUq9dKz,%;uUE?%etN:@3"=$NJlJo+?_932D+@v;QTjMGMu/j`H]Zul(~6 WWjo0.EV?G(0Yq#{i-rLCuNG"pTfG9|ve/_-~kxwK?B@U;r1WGx6NvdT4S;`87snz2%dFgUB8$Bem(8(Fg{$x_X4-2 CSE;\,M;nhc31u8YY_/aG0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 3544 Parent PID: 2480

General

Start time:	22:34:10
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' --start-maximized --enable-automation 'http://tonysglovesandsafety.com'
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: 5708 Parent PID: 3544

General

Start time:	22:34:11
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=1568,2662458852142118270,11731089809733117219,131072 --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

Disassembly