ID: 452263
Cookbook: browseurl.jbs
Time: 02:33:09
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

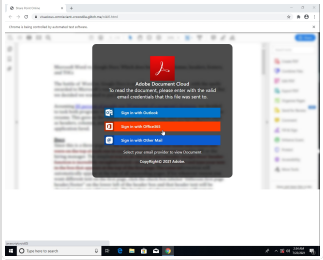
Windows Analysis Report https://vivacious-omniscient-…

Overview

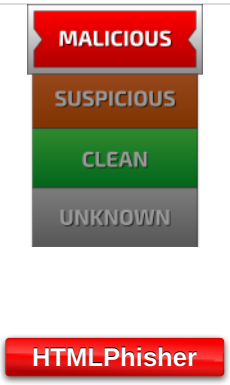
General Information

Sample URL:	http://https://vivacious-omniscient-crocodile.glitch.me/nikifi.html
Analysis ID:	452263
Infos:	

Most interesting Screenshot:



Detection

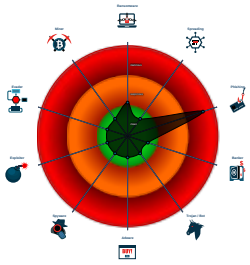


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on sh…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- HTML body contains low number of …
- HTML title does not match URL

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6436 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://vivacious-omniscient-crocodile.glitch.me/nikifi.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6668 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1452,4658061009318139164,17467065807480813581,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1840 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

Phishing site detected (based on shot template match)

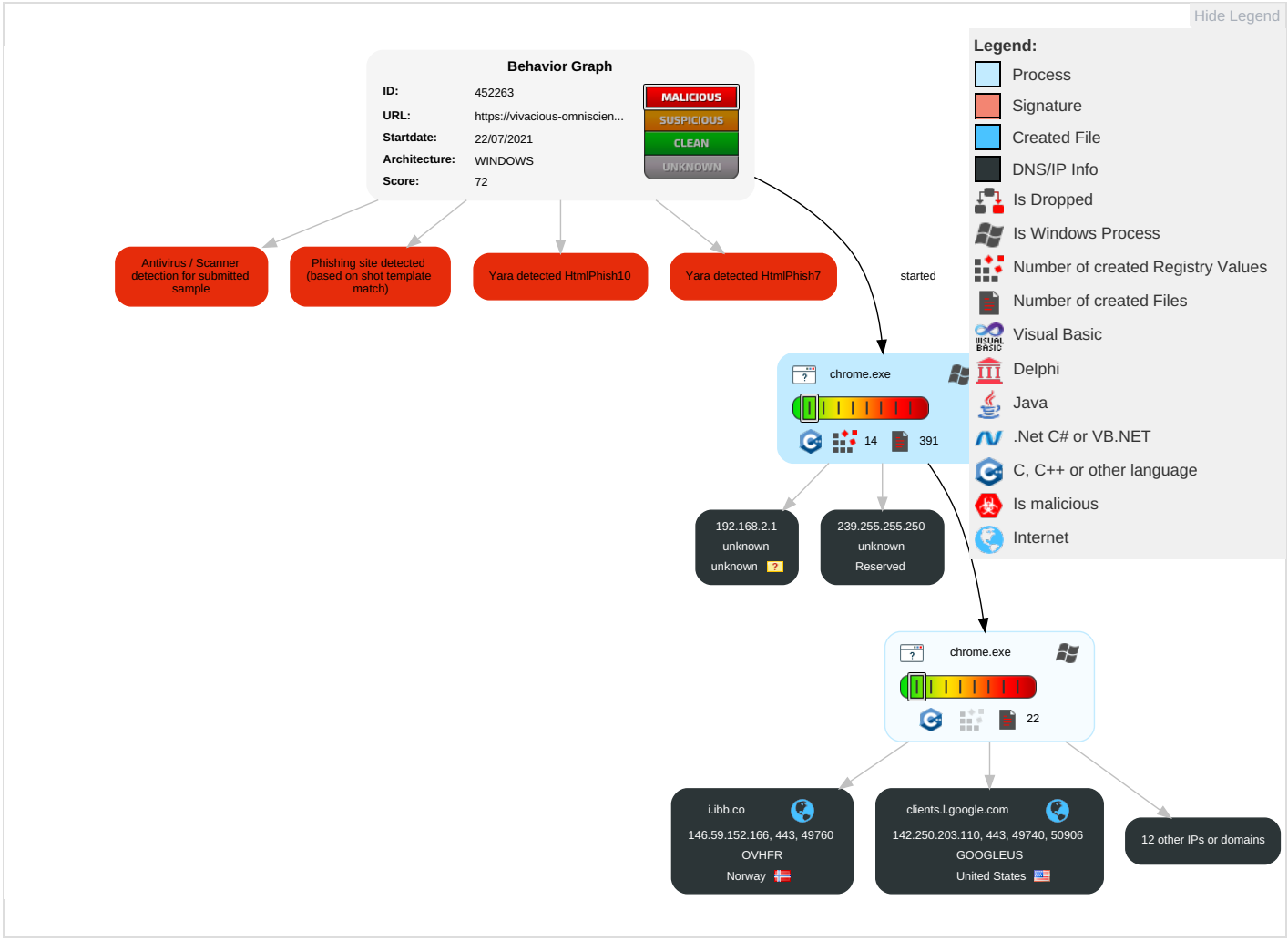
Yara detected HtmlPhish10

Yara detected HtmlPhish7

Mitre Att&ck Matrix

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

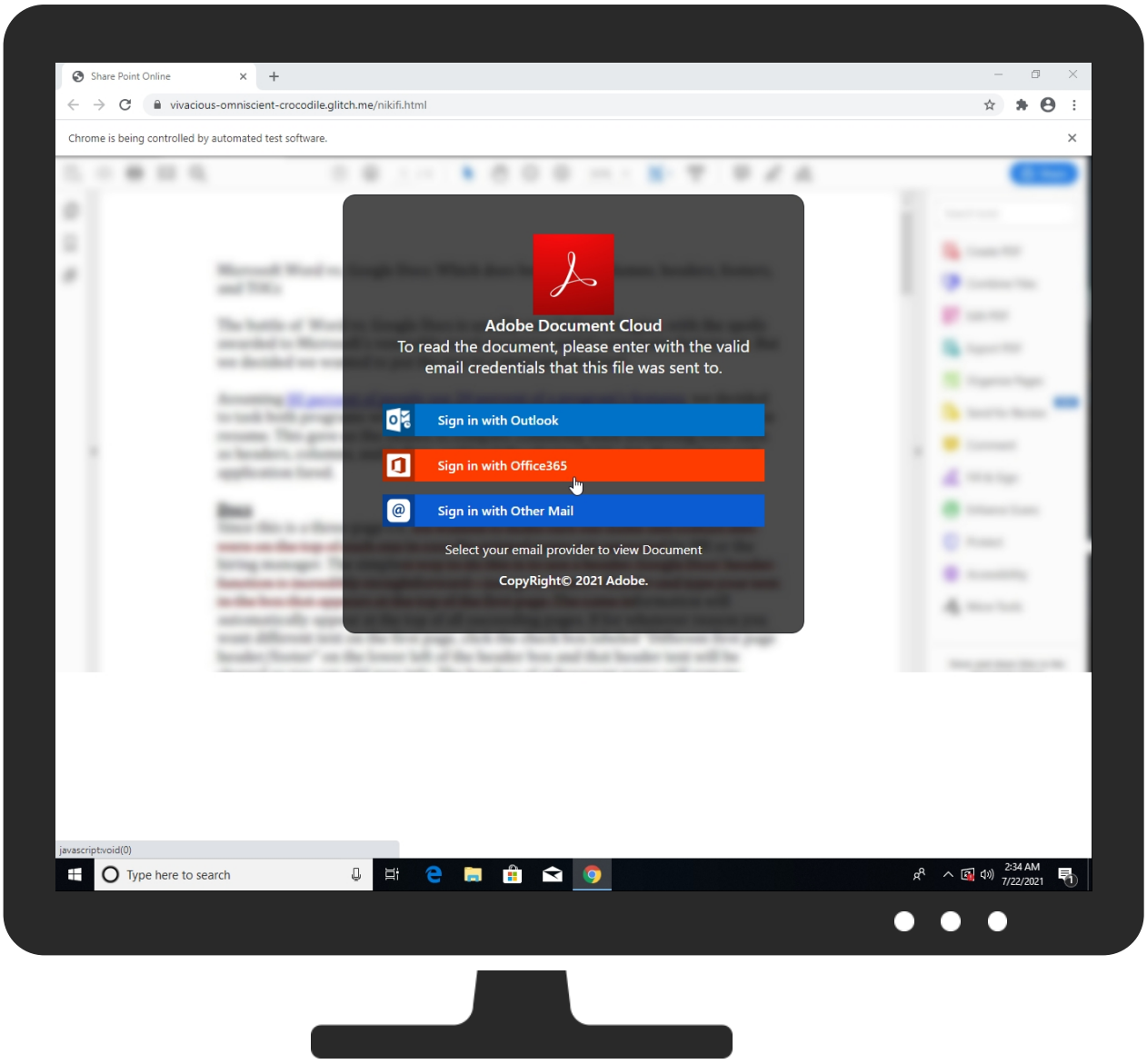
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://vivacious-omniscient-crocodile.glitch.me/nikifi.html	0%	Avira URL Cloud	safe	
http://https://vivacious-omniscient-crocodile.glitch.me/nikifi.html	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

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	

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/externalb	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.23.99	true	false		high
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
vivacious-omniscient-crocodile.glitch.me	107.23.110.216	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
i.ibb.co	146.59.152.166	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://vivacious-omniscient-crocodile.glitch.me/nikifi.html	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.23.110.216	vivacious-omniscient-crocodile.glitch.me	United States		14618	AMAZON-AESUS	false
146.59.152.166	i.ibb.co	Norway		16276	OVHFR	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.23.99	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452263
Start date:	22.07.2021
Start time:	02:33:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://vivacious-omniscient-crocodile.glitch.me/nikifi.html
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@28/172@10/11
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
02:34:03	API Interceptor	1x Sleep call for process: chrome.exe modified

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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2F A0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{...,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.130954046540265
Encrypted:	false
SSDEEP:	6:kKvqdoW+N+SkQlPlEGYRMY9z+4KlDA3RUellD1Ut:m5kPlE99SNxAhUe0et
MD5:	D5E17F07C011FFDE6967B52227A873E4
SHA1:	A4801B501B37B0D25861657676258B4F33AB191F
SHA-256:	93F20C441E06681EAA4C68E993E535E77299325EF8C6D764EA15D106386355BD
SHA-512:	FADC0FDC9CBF86F12F0C1439E72C736E80EDC9623EA5E99C7518EFC86D65095DD5E56E772A0DB68EE9931DB787C47DBF60991C7C5B24DCC652FA1F874CEB0 96
Malicious:	false
Reputation:	low
Preview:	p..... .....d.E.~..(..... .....T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\46652cd4-2224-43c2-89d0-e0eb09079147.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):	174555
Entropy (8bit):	6.079534841262942
Encrypted:	false
SSDEEP:	3072:vslkZExZKKJEuwA4x37SiHnDcWYKWFuFcbXafIB0u1GOJmA3iuRP:00ExzgRx37iWYFOaqfIlUOoSiuRP
MD5:	5122CB92C3892D5932E6933F4F3B60C3
SHA1:	7DD1EAE05E743F9EC13DDF201449E68E2A90B1FE
SHA-256:	B2B0133AA4B96E27F0CEAFEABDF3B9337659F8EB26A4493DC48BE4FD57BFA1B9
SHA-512:	044CB60BC0512DBB9B93534DFF55D64356E8D8A9FEE7E23491DA2DFEEBD0FEBA6C2DDA6E8EB04DF80C07E26FE9B132024C968D19AF06F2AC45CAE4D250753 877
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":1.626914041691184e+12,"network":1.626914043e+12,"ticks":5556256593.0,"uncertainty":3719033.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715919805"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\933e9575-566f-471d-a9f2-aaad24fc214c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.750719566455277
Encrypted:	false
SSDEEP:	384:jbY3n96ABhm7yNTrIvvF3g/xgH58GEDrupnfxYRddcrmLm2Bq1LXrgOxRvNO1D6u:QK11q9AI0eDTtB0n7uVKb13B8
MD5:	637904BBCEE097D2534D3F6819C876E4
SHA1:	B8CF12A0EBDE7F2D2D2A1545FE77027B45C3EBF1
SHA-256:	EF034C366927B6408F5D958157264390892067E50A0CC044E71884FE25F32268
SHA-512:	E747B8B9A010DB1713EB84616082755E6BBD250EB6CB07D701CF434D17920B10682FA5AC9A5FBDE09B2BF653C03CF64DC0D794686C73F81F822BF33FF0171CAE
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...`@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\95390e74-c8f0-402f-8276-ca2285ce4913.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):	174555
Entropy (8bit):	6.079534613845904
Encrypted:	false
SSDEEP:	3072:VslkZExZKKJEuwA4x37SiHnDcWYKWFuFcbXafIB0u1GOJmA3iuRP:60ExzgRx37iWYFOaqfIlUOoSiuRP
MD5:	7646C22BD7EF9FDF7325CA266C3495D7
SHA1:	14363E567D57B1F1CD88DADB8726F4A399863362
SHA-256:	963FD6DF79D79F20D12F84A0179E4590312E139F539DEF2888E18F630ED8E69E
SHA-512:	FD4A1AAF428AFF8019D9674A32BA9A912E0F9AAC01096F3CA3EE7AB464D10699F1B857B2999C2AD99BDA227154A71E264406CF6AA2251F0CA8D39F07088EEB57
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":1.626914041691184e+12,"network":1.626914043e+12,"ticks":5556256593.0,"uncertainty":3719033.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0ad19918-fc43-4903-9c0f-be5477909b31.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0ad19918-fc43-4903-9c0f-be5477909b31.tmp	
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\48dc906a-8f03-42c6-89f9-f7f3ded42ab3.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):	5.577078117920283
Encrypted:	false
SSDEEP:	384:U5tteLlhzX21kXqKf/pUZNCgVLH2HfDlrULYFA4dq:zLlJ21kXqKf/pUZNCgVLH2HfhrUL2An
MD5:	EE3ED4C3C401094FBB27BAD4E9D3922F
SHA1:	160140258BA1CE866F18801848F463E06A5A9629
SHA-256:	E2CDF55EFB461159BDA5CC01BCBC09B9945B8AE4E8F2D26CDD6BF74B3427AA05
SHA-512:	D88D75CCDDF7AEABD8DBC0B8544F65C23DD6DF65D3283E24AF7CE959C12754104206C518F422B20DD178D296BDC4DE4DDF2F34E04CD348BD805231E00CC2DF
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":"13271387638916361","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4dd5182e-9824-4c6a-ac6c-5f05305a52ff.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):	5.536012305362423
Encrypted:	false
SSDEEP:	384:U5tt3LlhzX21kXqKf/pUZNCgVLH2HfDlrULHG1MnZEYshA4s:sLlJ21kXqKf/pUZNCgVLH2HfhrUbGmnz
MD5:	8C2142721DD971CB9983C41DD9D3E38D
SHA1:	8D64530CCC4B3BCC3F0E6B929BA0937A78F5220C
SHA-256:	7D4A66BB2AB774957C6E4AD9F6421B75AA75AA1A151C7764210C6B096B2E08C9
SHA-512:	9D27D05C5386B9EAC68B502967C7B2BCA3753826993E12F96FCD695184F9C22F1863F0B898A75AB713B71E926130C8E47F7DA603CC33B5E677BDE4838346AF87
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":"13271387638916361","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6b30da6f-5cd3-4dfd-a7a0-a2999d9a9cd2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	22602
Entropy (8bit):	5.536080975945647
Encrypted:	false
SSDEEP:	384:U5tt3LlhzX21kXqKf/pUZNCgVLH2HfDlrULHGwMnZEY2A4w:sLlJ21kXqKf/pUZNCgVLH2HfhrUbGRnF
MD5:	47A5C9FFAF1C55E57901D6AC294F6312

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6b30da6f-5cd3-4dfd-a7a0-a2999d9a9cd2.tmp	
SHA1:	B143F407A5A7D8FE0125589241A36D54CF94ADFC
SHA-256:	4727A2B7E06FC70109575BDD4B6B373CB6A27D7A4A9CDAD66CE76E74DF09A12C
SHA-512:	998AE59BC453E8E11BF63BFF655C3A924EB5BFA419C9B44A559785D9EFA6012382F91A23972DE51DA92288FD6340E5A44885673A7C3FA9A4824E82DB7CC8BE0
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":"13271387638916361","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6ba2ee26-4fa1-4f27-a743-0d3560267c8a.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):	1544
Entropy (8bit):	5.583847086457133
Encrypted:	false
SSDEEP:	48:YKVwUR6UUhdJeUwXKUjYqPeUekUevwUGsYUpPUeP:gUoUUwUwKUjHPeU3UdUbYUpPUg
MD5:	0108D19E21DDBF7E275E0D1A19DBF2BB
SHA1:	00DEF223E39087100460A2AD246560DA0C4540F1
SHA-256:	4D9B019BBC9509DC0D7912108BFBD984F05D1CC67A539033C92EDE3D1DA953C9
SHA-512:	0CD123EBC3081DDC500F0FD0D977564F61B30699B56B04E55287B6556DEE339ADF0E142A347B929424E0CFE0143E4C8F5B32538370C1BD08364DD755FA57C60
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1642694074.342495,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626914074.342501},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1658450043.533593,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626914043.533599},{"expiry":1658450043.557599,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626914043.557605},{"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_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8816117f-ebbd-45fe-bd0a-42fca94a5484.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\890dfe68-3042-4848-b5bc-56a92a4eb6d4.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):	5217
Entropy (8bit):	4.96583792986151
Encrypted:	false
SSDEEP:	96:nnLJtMpIKIM5k0JCKL8GzkpS1wbOTlVuHn:nnLjMpIah4K/kY+
MD5:	82015554430ECC1E6942E6656C2B0103
SHA1:	72D93DA90D27B53907B9D375DFC8E06A136A49F2
SHA-256:	3FF305B32CCA5BC8F19E7EF6957DCE9BCAEA9DDC0DCB671DED167CCFA6C3B3B0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\890dfe68-3042-4848-b5bc-56a92a4eb6d4.tmp	
SHA-512:	C90E5421B84B591DE462B73E8BBB0945C24520E07507F3D52B459D834B5556259AF2883F761D7E061C38575332558DF5009A238DA82B96DAA36690730BEBEE36
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271387639211629","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.25151495184978
Encrypted:	false
SSDEEP:	6:mpo+q2Pwkn23iKKdK9RXXTZIFUtpM1XWZmwPM1iVkwOwkn23iKKdK9RXX5LJ:+o+vYf5Kk7XT2FUtpOXW/POiV5Jf5KkT
MD5:	17CB2F30EEC1B2B9A6CED44C2347B246
SHA1:	D836FE7B1066AA5E881D08A2427407B52ABD202B
SHA-256:	FCB0ACE95BDF8FE20E17AB3DC1502E5A828507899DA5525A6A18AB599FFBDAC6
SHA-512:	D5A098708D9CF93EF6108CA00C6047495C0B143C3B0185268B56EA317465B1B495E6B1545E9DBE42DEC42F82C9D752B9D772E70A5182F1875774B2B67E001579
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:15.584 18cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/22-02:34:15.586 18cc Recovering log #3.2021/07/22-02:34:15.586 18cc 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):	5.219471233096227
Encrypted:	false
SSDEEP:	6:mAcEB+q2Pwkn23iKKdKyDZIFUtpRCPWZmwPR2EjNVkwOwkn23iKKdKyJLJ:mEB+vYf5Kk02FUtpeW/PBV5Jf5KkWJ
MD5:	8A130919839F7938107F325D01E76269
SHA1:	2527C2152C1E4BF65ECB688B9C1A2BB006FAC6F8
SHA-256:	0D04762F71B4435CE4DE9097232F26A1D145F7B80115936E258FD0C2FA01D123
SHA-512:	50DA9046D4EF2295F22713F569F5FFC789285E166E8CA88CCC85C4A17C4AE0707AD7EB6569F4C27A02867258CBA8747FE07780DDA633CB621E68F3B89C8C301
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:15.571 18cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/22-02:34:15.573 18cc Recovering log #3.2021/07/22-02:34:15.577 18cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a75a9a55cba1243_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.555148855868312
Encrypted:	false
SSDEEP:	3:m+lmplt6OA8RzYP2FycyGYWCULLuFvDpvLDIKC7GX0u9oJOD/lHCmJtJ8LyuPZ3o:mh5YerCUlGfOwDgmJ4LnunhvllZK6t
MD5:	04622D8DB25EDE9528428316BB32FE13
SHA1:	442BF239203B307F2CE5A20B049497B5E7DFAEAA
SHA-256:	FC32B7494CEC0DE44FA44D676B50D98E5137953B12DB9AE88506809F919FBF80
SHA-512:	E26E30F51CDDD82C106EBF32C2C4391E02F2C446A3024301826E7510E1C8BC3BA5BB1DB05AB46980E65291CEB95566D2652BA43472A7CE102247ADA67247FFDA
Malicious:	false
Reputation:	low
Preview:	0\r..m......g....'......_keyhttps://code.jquery.com/jquery-3.2.1.slim.min.js .https://vivacious-omniscient-crocodile.glitch.me/l...A&/.............U.........G...H.#..c...J.WX....`....L+.A..Eo......7..<.........A..Eo..................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\52fc0a871822482c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	260
Entropy (8bit):	5.515274792604013
Encrypted:	false
SSDEEP:	6:mePYET08NaYWbVOqZtGfOrF+HgswQz2XvkpRK6t:zg8NaY8ZrrF+nu/Cr
MD5:	0ACDAB2EE7C1283005D599E374FE9881
SHA1:	468584CD6F125691FF70531311134A541CAAE154
SHA-256:	BEE0F9B5643B27E5D8A017894F88A33DC4362316CF12E793D51733E036A71E27
SHA-512:	2D974D41B4EDA8E2AFF610199AD2153ABBA15178906F624E84CE3D2C4F699B68F26B39359613A5A4C4BCE44A908E0BE24490AFD237A98AF39A6273AD384D2F3
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://vivacious-omniscient-crocodile.glitch.me/Io..A&/.....w.....E...L.)(.{>C...\o..zD{h7AJ.....A..Eo.....x$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\63957e9a65d2b5ce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.412038848591414
Encrypted:	false
SSDEEP:	6:mt2EY68E9xEEUgLErtGfOmqFgahl0mPMFdrGhK6t:C2QYgqmoF7
MD5:	8C149874B0D983B2D280237142FEDCA1
SHA1:	5765C8C861E84B091235ED27DA91E387DE53505A
SHA-256:	1B37E428C1ED78309544E9A9DC0B01A1E73263625422DE7BC9196D74353D97E1
SHA-512:	E95375D025E86F451ED8B104E28911BFD67B38E467BC96E84EE1A6EFD5149212492F346473DEA8F20767632FAD95EFD4D9F8C27C0D65D6DB8F37A53EC34936A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z...Y....._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://vivacious-omniscient-crocodile.glitch.me/....A&/.....:%<AQ.../....<.....V....K...J...A..Eo.....#.\.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\84f65aecb1b65fd4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94200
Entropy (8bit):	5.771304221401622
Encrypted:	false
SSDEEP:	1536:pzlUQ8g58regIkAjEez3QjsPkgLttsOgWCxjusVEMrKSWb9G1qvSPS:2K873Cbkstsg6ju2EMtR1qd
MD5:	4D4B3D9CC565B6C268863622BDA17AB3
SHA1:	BE7E12B90AC6E8BAA32B889DD6C4B55F5A4F847F
SHA-256:	89AF3B3ED017876AEA792D5E5F8F1E21BA87274EEFD8A4EF800D00720A324BFD
SHA-512:	2521D10B4ECF98B1FFD936CE08A217DA8F4BCAF962D21C0721C1EEA55BF7A6624531429425F10B4298ABA16009A45CAAF7C44301183142E276DDF4D2A77A6E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...1b.V....BD15C51291033A7315D3F0FE1588BD6F2D41AE1ECAB39AE986CE71401B9E2B19.....'.JN....O ....n.....!.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`...I`....Da....*.....Q.@..N.....module....Q.@.....exports...QcR.....documen t.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!....@...https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.jsa..... ..D`....D`....D`.....`z...&...&..!.&....&.(S....!..`.C.....q.L`.....Rc@.....M.....Qb.Md....d.....Qbb.....e.....Qb..`.....f.....Qb..v....h.....S...Qb.....j.....Qb.i.Q....k.....Qb.. .)....I.....Qb~?.....n.....Qb2.X.....o.....QbjC.=....p.....Qb...u....q.....Qb2.G.....r.....QbZa.L....s.....R....Qb..)$....v.....Qb..*.....w.....Qb.....x.....Qb...f....y....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8b46160d68ace9ef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	383
Entropy (8bit):	6.023553735027593
Encrypted:	false
SSDEEP:	6:mgjYSHT8NWQAlKPUQy0GfO0ugkSGkg/kK6tEvXcGy8CgXBVSvkg/th:N5z8NWQCUUISGNOKvMp8CgXXSvN
MD5:	03528854FAB1129509BC9AC639BA4D1B
SHA1:	1F9082FA461CFD65CB5DD231CE32B2AA66DFB0C4
SHA-256:	8F33630F95CAD51F4A47415C9599D673CB4DC124BE211B949E53982A1DC08EDD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8b46160d68ace9ef_0	
SHA-512:	CB6C06D7A573B6D803384E397F6E3C25E8B5DF95C2F7EFA06348F4BC0379B8E2A14D2E179095DBC42235BFFEEC054A5EBA740AA88988132C8F2B67B45FA60F16
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w....._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://vivacious-omniscient-crocodile.glitch.me/..*.A&/.....m.....1"...6.....@.....\...A..Eo.....=`".....A..Eo.....*.A&/.Po..BD15C51291033A7315D3F0FE1588BD6F2D41AE1ECAB39AE986CE71401B9E2B19m.....1"...6.....@.....\...A..Eo.....xPK.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c591876147cc49bb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.502763959810829
Encrypted:	false
SSDEEP:	6:mOSlXYlNYpSVkiGfOoiKugbuPzJy74+K6t:NWZpSV7osw/
MD5:	B809D92C3F3E93D86183AB1177171658
SHA1:	05C8CADE3DBA8ED1EC34F2E4A1F80454027841A3
SHA-256:	C75A02CEA34D6E0EF61D1B771F5CBD3B9E298ADC12E05F3C55A8A305F0CA779C
SHA-512:	4CC003D24EC78C20E46394DBDD131BE456AEC5D30CC37C4415221FDDF40B159BE18604C5A7F4DFD28ADBA4D2A9348E200A9D941DA42BE648733039127011A59
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`.....u....._keyhttps://kit.fontawesome.com/585b051251.js .https://vivacious-omniscient-crocodile.glitch.me/.T+.A&/.....+T..c.m.kR.c..}.o....)6llvy..A..Eo.....%k~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	zlib compressed data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	5.018025848707652
Encrypted:	false
SSDEEP:	6:LK/duCEs3l4XWvJFbwluJ2RqdcTxzPawAfyDan59:LK7zVDBxWZXUyuH
MD5:	36B68A27226212DDD5AE55231E80ED40
SHA1:	4C4B5DB7B018F3828068D60D57578730EA42F9FF
SHA-256:	C08A0ECBA7DD06956A0F1055654444ADA0CB2005A3431CAAD4B849390EA47876
SHA-512:	0CB6756F70CA1F7D5BAEFB18B5A0DCEF55DFF2F0A84C1CA6578E39A9F7FCA6AF95D10E5F10061B28CE9DB9DB7ECA03ED0AA0A4FF1A3CC940B8517B807A553148
Malicious:	false
Reputation:	low
Preview:	x...."=ioy retne....._...Z...w2.A&/..q.....e.~.c.w2.A&/.....,H"....R.w2.A&/.....I.Ga....4#.A&/.....h..F..4#.A&/.....^}.Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....C..\..u..w2.A&/.....4T/f.C3....&../.....:.A&/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	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):	0.9726511754734752
Encrypted:	false
SSDEEP:	24:ze9H6pf1H1oNtcqLbJLbXaFpEO5bNmISHn06UwP8:zbfvoNqq5LLOpEO5J/Kn7UQ8
MD5:	227A5B12B8ECFD44F9E549DAC0C8E878
SHA1:	084DFCB9DFC03246AED9502272A40A4E5AF219E2
SHA-256:	BB267EA042526CB5FBB64AA80A7CD903F2ACC38B04BDFEE0529937161EC1B6D5
SHA-512:	693D217EFA538887AD88DD1A948B1C0E2C1B0E47CC293A738282D44195647F05C3798B02396F30FBB40C82B160BC611599D071E12DB698739D1B623D8A1F6872
Malicious:	false
Reputation:	low
Preview:	.....v._..... ....

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):	1481
Entropy (8bit):	3.3313654534594406
Encrypted:	false
SSDEEP:	24:34SgXlrlJdTcmh50uX1CVEpsZL3S6jb6ZTcZulLlL:34f1xncsCg1CVEpM3ShcZqRL
MD5:	099431A73EDC9E9B5BC0DF5BAC818ACE
SHA1:	5C1FB743735E1F201F7289A820EDF3077E92D341
SHA-256:	5F9367BC241DF6736C6D234775D5C85468210E07F5194775CCED9A01FD7CA023
SHA-512:	3C3C9989DDED2CA5B4D6E802E4DCE591375B336D587A780DEAF2B295C7BC93A2FE73DB56DEBCC95AB73E2C3E98C307D52E1A68AEAC1D03D257C4741E7F97AFA
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...94182f0c_d720_487f_a826_a8c20c2905f6.....z..K..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....E..@.....<...https://vivacious-omniscient-crocodile.glitch.me/nikifi.html....S.h.a.r.e. . P.o.i.n.t. .O.n.l.i.n.e.D...@.....8.....h.....`.....`.....{.q.....{.q.....<...h.t.t.p.s.:./.v.i.v.a.c.i.o.u.s.-.o.m. n.i.s.c.i.e.n.t.-.c.r.o.c.o.d.i.l.e...g.l.i.t.c.h...m.e./.n.i.k.i.f.i...h.t.m.l.....8.....0.....8.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f. o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....2..... .[.e.m.a.i.l. .p.a.s.s.w.o.r.d. .].

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.2404368266143635
Encrypted:	false
SSDEEP:	6:mPq6q2Pwkn23iKKdK8aPrqIFUtpoXZZmwPogpkwOwkn23iKKdK8amLJ:v6vYf5KkL3FUtpcZ/Pn5Jf5KkQJ
MD5:	1E7C0268C9D54B7428ACB4BAF150A36A
SHA1:	1B87769397A5D518DDBB901E0B0E68B0AB1F9757
SHA-256:	C9E5BC0ABAF585799328B9977AFB7EECD9DEBB490BDAA6A484A404406B7A8172
SHA-512:	96E32CEF9C45E20781CF73125893E3B7EC3295AEE26766C5F4D29B26958AF1897ECA780F960FED92823D0459C988807EAB50EFA8C4D546AA5F1398569E09F8BA
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:33:59.216 19b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/22-02:33:59.217 19b4 Recovering log #3.2021/07/22-02:33:59.218 19b4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5...............

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):	5.1670439033435045
Encrypted:	false
SSDEEP:	6:m1JTjL+q2Pwkn23iKKdK8NIFUtpmJb1ZmwPmJcLVkwOwkn23iKKdK8+eLJ:2xjyvYf5KkpFUtpmP/PmuR5Jf5KkqJ
MD5:	118865BF8B965F871EB3B15B594A8273
SHA1:	94C0A4A6B5602C70BB84D4750C197F7F8F9B0659
SHA-256:	00F11E2C1C4CA097497615A829A6BE0ACD7C7303675A623305592C7B8AE78303
SHA-512:	BB3227F5193CE563FB41C19F5758E7306CA965F3C5FF6CA9E881BECD6F28EBC846B71F502C490BC74A4E35AC9D6BEE006935B08758F3B2F8C91938DE334A488
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:01.461 1a38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/22-02:34:01.463 1a38 Recovering log #3.2021/07/22-02:34:01.464 1a38 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\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.244152238566348
Encrypted:	false
SSDEEP:	6:mtudN+q2Pwkn23iKKdK25+Xqx8chI+IFUtpIMAWZmwPIM3VkwOwkn23iKKdK25+M:+udN+vYf5KkTXfchI3FUtpWW/PdV5Jfk
MD5:	8B23B7018A987D756916A8BAC6176DCA
SHA1:	DF4866017EF91440E3F53DB17C84DCF79B31E916
SHA-256:	918E75311E2E2715738EB310B2DC16E113E5A4178C9B1DC00C7687B6E210DA22
SHA-512:	32F51B4433D8252F3F78714988C326ABC16657CD9CD50C812809A71EE7F77C2018608FABFD7018C01B7C8E099CB47157C1D3CC92270278A4A181A70C9EB82D6
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:15.522 18cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/22-02:34:15.524 18cc Recovering log #3.2021/07/22-02:34:15.524 18cc 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):	5.2064114339463545
Encrypted:	false
SSDEEP:	6:mGm+q2Pwkn23iKKdK25+XuoIFUtpXQamWZmwPX2EjNVkwOwkn23iKKdK25+XuxWd:Hm+vYf5KkTXYFUtpXQPW/PXzV5Jf5Kkl
MD5:	354C50325B7E79F15C88F7E7F8BFFFA0
SHA1:	E93AD7199C873402C43F4F63E8DDCD51942166CB
SHA-256:	AC097E94E495D29A628015A91DE35EEF8F9268A4716450C3B99286A8A6628449
SHA-512:	D0A560B0F7B49A0AAA0235CBAA47D865ECC866575AC9645A0C11410661E65C9E4BC871477BE1F1CB13C469784C633ED26FB6B01EA570AAD19D140B346C0FE5B
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:15.514 18cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/22-02:34:15.515 18cc Recovering log #3.2021/07/22-02:34:15.517 18cc 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):	5.2720469052767065
Encrypted:	false
SSDEEP:	6:mMEm+q2Pwkn23iKKdKWT5g1IdqIFUtpD2NZZmwPDQNNVkwOwkn23iKKdKWT5g1Iu:zEnvYf5Kkg5gSRFUtpD2f/PDA5Jf5Kkn
MD5:	3AF3412D2478B6DDF99725AF30494B89
SHA1:	7EF564E8B0E472CA6DFB87ABC579BF9DE87426E5
SHA-256:	6DA12F27709C3A47F6F480F3882691810FA663436ABE2C895401A92A447E6AC2
SHA-512:	51F8031B52407751E0BD4C29B86739B037B22666A8A99D63565E27F76F07241353126F39250819D4187D8685F5283D4A554B2AA4A8A14734866112590A8B7BE6
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:15.428 19b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/22-02:34:15.430 19b8 Recovering log #3.2021/07/22-02:34:15.432 19b8 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):	0.12166949061075875
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvAlvRftGfO/UBWR2l0Oo/lCxthiRrGCxC+/erlGlpGfO/UJ:TL+A/yvRfrcBM2l0NuQRrGI/HcJ
MD5:	7AB949D50DB1F2680F04D15498440D73
SHA1:	0AD72775230991DAF5CD2DEDA86CA4DD9CC9A49A
SHA-256:	622DE4DDC335858AF6F8AFC4444FD0201FD69A93F98478B0FDAB4C578AA88EDC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
SHA-512:	812EBC610EECD72486FB3B180BED3CFEBC545A4EA2C6A25D10A1D3D5814D0F681755AA0C05140CAA3A911ED395702D64B2DC5DB998BD1C057F8186D089A20 B2
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):	704
Entropy (8bit):	5.215770309007964
Encrypted:	false
SSDEEP:	12:CVRKsggWD3dBCgkLf839Tt3sp9JkaaexBl46koQ/38dXGu1TBk778B/xgskZBa9d:CXWD3/Ch83T3C9JkCF+8suY78BJgskfl
MD5:	AFA9FEA670DEABFF94B3F2CFECC17C96
SHA1:	0F3761F9A82A4585EC1146B597C0B9E7AB528A8A
SHA-256:	8865FBE028ADF3E94DD1098AE4C4E52B299F97563F77BE885D8B880539F55593
SHA-512:	4D70E82E085D9594D8191B164B259A08CC5CC6E0B9DF983299EAB1134E5F1A1AA2E4ACD252DF2B63A639AB6A5805EB8908F85581B57AB72DF02A1D9523D791E 4
Malicious:	false
Reputation:	low
Preview:	.....".[....crocodile..glitch..html..https..me..nikifi..omniscient..online..point..share..vivacious*.....crocodile.....glitch.....html.....https.....me.....nikifi.....omniscient.....onl ine.....point.....share.....vivacious..2.....a.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t..... ...u.....v...:e.....Bv...r..... .....*<https://vivacious-omniscient-crocodile.glitch.me/nikifi.html2.Share Point Online :.....J.....'.18.....

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):	0.04708131321038462
Encrypted:	false
SSDEEP:	3:P/iv3llu/fllv/7oNllv/64fllv/1HNllv/29tFllv/3Ffllv/54tFllv/+lMRgB:0uKle1z4xg9bNFlWCj/lRl3n
MD5:	8CA114D126514499388DD15337494878
SHA1:	C0DD411EADF56ECD9EFEC345AC56A15296120B4F
SHA-256:	6F1EBD8E6532837C0B44D620A722D8E6C56E3C4E2B4DC9F74190A4A941922272
SHA-512:	46A958B56F30AAD414DB019C6C899E2BF9E5436BFF9BA790039942C17F56D7112EA86E10C41858CC76FA73106BAB1E18129208F2AA7634572E1183B39937AA03
Malicious:	false
Reputation:	low
Preview:	.....|..... ....

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):	5.463393800558467
Encrypted:	false
SSDEEP:	48:iVRGkeha7bMa8db4HXwbQSefgGtONrS0U9RdiN9Zh:/a7bMZdb4HXwbQ5fgGtirS0B
MD5:	E32A82A8A3330D9D0F71AC29919316B0
SHA1:	A64958100549527513FAA64CD1A4246F456A52B4
SHA-256:	72800C1FC674AD6E2779714BE944EC007D6E6712C728F2111CFBC01DC94C1792
SHA-512:	EFFC47D385F63C8E054208BE304235BF92AA16B66BBA8E61A87E662534F8DCF50D81F4CE328C745A7530CF9BF156F0FFB60D67E4954F953A5BC6E07A7FA117E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Preview:	..c....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..740947000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-22 02:34:17.43][INFO][mr.Init] MR instance ID: 8e7890fd-b7e9-4eb3-90d1-fe05e58c1ab0\n","[2021-07-22 02:34:17.43][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-22 02:34:17.43][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-07-22 02:34:17.43][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-22 02:34:17.43][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-07-22 02:34:17.43][INFO][mr.CastProvider] Query enabled: true\n","[2021-07-22 02:34:17.44][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.193064837710453
Encrypted:	false
SSDEEP:	6:mkcuCIq2Pwkn23iKKdK8a2jMGIFUtplcfjZZmwPlchkwOwkn23iKKdK8a2jMmLJ:VcuCIvYf5Kk8EFUtplcbZ/Plch5Jf5KV
MD5:	917E3CF9C25B98E4B60C089C3D03572F
SHA1:	32D5C12743D64FD7D67EA02A9E700A5DBB4829D2
SHA-256:	CDA084911CC6ADF2E54648041D526B5E788378F9A5D8FEC4F08375E9BC82001F
SHA-512:	954624A1793939B89FCF10E1728FF2572A309CE8B254F4DF75214BB901A306B150C1FD010F7F4DC05A75570F4F7878427C4915C1BB44BDB221DAAF17221CB76E
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:33:58.990 1a34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/22-02:33:58.992 1a34 Recovering log #3.2021/07/22-02:33:58.994 1a34 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.212304807082594
Encrypted:	false
SSDEEP:	6:mPtXuQ39+q2Pwkn23iKKdKgXz4rRIFUtpotSJZmwPotRt9VkwOwkn23iKKdKgXzW:0XuvYf5KkgXiuFUtpEs/PEr5Jf5KkgXS
MD5:	97B879091C5C518B23F1334B21C0346B
SHA1:	D4D25E98B391252149CA3DEF1BC49E76D86D1838
SHA-256:	4A69EB5B36C608CFB209C94CFA08E64DBC0CF6E7AD20ABDE06C4E53F2DC716ED
SHA-512:	DAF0BEC76FCF3D0104A1AE4E28B8AC527FAD4622F16365D77CC85F34DFC84D5A2C3DD84BB53E21C26F347C1BACEF5D6138435C339345F9DC687D997E14DDEFF
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:33:59.242 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/22-02:33:59.243 1a48 Recovering log #3.2021/07/22-02:33:59.244 1a48 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\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	1.157158578564297
Encrypted:	false
SSDEEP:	192:wIElwQF8mpcSJ2Y5SIElwQF8mpcSFYzZzYz/4j1:w2Y5KCzi4j1
MD5:	DC46EE1FA2E190B9E2345AF12C582545
SHA1:	8A52AFF63AFB6014BB8D41D119B6495A90BB02FD
SHA-256:	B887C70F4E3E773C199CBB310BE42D63D03572B4B0F2FFFB4279B23EF25C5390
SHA-512:	D692FFBEA0C719ADADE656973183D2BDCB37D91B26EA3F846C93A3A79D633CE5145D230A4564E0C034805BC8E2EA2577B1C64D92409B53900D2A888EC6EB3F5
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	50296
Entropy (8bit):	0.7950317578708084
Encrypted:	false
SSDEEP:	96:4UhIElwQF8mpcS7ifYN6rxIElwQF8mpcS7:HhIElwQF8mpcSefYErxIElwQF8mpcS7
MD5:	12E072A5A9C9D4F63DE95F732C59F996
SHA1:	CB4E74F6E4BBB84FCC6C0774D3500E12CBAEB673
SHA-256:	D03C7FED70D4AA547029F9A473361963A13535617E07FC4BD7E94FBF737912EC
SHA-512:	2AB3DC19D6F8D2BF07D0AC9D8FE40A0BE00DF0344B1FE8C8B2BEA42BD3DC7127DAB35B5C323095BD75BDA46702E4C95EF6E4BDD59466271EFB474E3CE36DFEE
Malicious:	false
Reputation:	low
Preview:	.....^a..... ....

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):	5.170234899212139
Encrypted:	false
SSDEEP:	6:mPpIN+q2Pwkn23iKKdKrQMxIFUtpoRXZmwPoctVkwOwkn23iKKdKrQMFLJ:VIvYf5KkCFUtpU/PfT5Jf5KktJ
MD5:	B5E75FA4F9044F62836213F488AB8E08
SHA1:	0C0711656C90A88653F08BB1581ECAC7384A31F0
SHA-256:	D2E3425E2C50A12B59BEB6FF7A8E570F07A825B797CD758AADF60C088F17D45E
SHA-512:	0D94612ED11E4D0854477AF6FE3E181D2D75841C3C9097025438D5BB40CE7646919BC5E0406D73F107DA74E06214A2C5B2CAC90E6C5697BD103024A4584BE4D
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:33:59.156 19e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/22-02:33:59.157 19e8 Recovering log #3.2021/07/22-02:33:59.158 19e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.188746467969741
Encrypted:	false
SSDEEP:	6:mkcnC9+q2Pwkn23iKKdK7Uh2ghZIFUtplcSJZmwPlcH9VkwOwkn23iKKdK7Uh2gd:VcC9+vYf5KkIhHh2FUtplcSJ/PlcH9VM
MD5:	046B04C3610AA70EF2F22EC9D8FBD99B
SHA1:	EDB69D78823D189C890719102E71A94ED02F9D54

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SHA-256:	86F4870FF64EEFC9FC2203F1ADF4974207A222957B73C3A4F8B1BA723D9FC3EF
SHA-512:	75BEE749FB4BC4C3245C73C0EB1045613D6FF0658EDAE8E05DA19AA3E454994E9ECA0C079F5CDE2E7CF82132F191A7A05A7278761A9088088F50E8DF139D8C7A
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:33:58.926 19dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/07/22-02:33:58.931 19dc Recovering log #3.2021/07/22-02:33:58.932 19dc 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\8ce78a94-de43-4950-bff1-2ff5d6016432.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\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):	5.260112688444995
Encrypted:	false
SSDEEP:	6:mPG+q2Pwkn23iKKdKusNpV/2jMGIFUtpo9ZmwPoBVkwOwkn23iKKdKusNpV/2jM4:b+vYf5KkFFUtpo/P4V5Jf5KkOJ
MD5:	6541F6A11B6AC7DCD42B99C24D6F3A4D
SHA1:	E567B05D1D52D59E027DF4F4653D8B23B3694EBA
SHA-256:	3D044188074A0263D73BE0E05FCF85B9A19314D16092530D16FDDA9B592475AE
SHA-512:	3B7D497B0E5D6357C070F8CF61DE849F3944300693CA242B6742F8F34CB954A576B39BF40A2146102BF160CC1D08C2A6A25C30461B8FB4FC3DB7A32A6C034BF
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:33:59.196 1a4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-02:33:59.197 1a4c Recovering log #3.2021/07/22-02:33:59.197 1a4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.29136210878094
Encrypted:	false
SSDEEP:	12:0NyvYf5KkmiuFUtpETu/PETWR5Jf5Kkm2J:+YYf5KkSgxDJf5Kkr
MD5:	F9759653EFB9411D1891D06BAAA83160
SHA1:	1BC1EBB38CBCCD07A0FA8AE6738FC7D08F482023
SHA-256:	9D8A15B7D6BE6A72985088871E2EE4DA30F737DAE26978E715BAA1F38C87DFD4
SHA-512:	368926C6FB72A57F4F9FDDEACFDE15766C8FA6A0A784EBCD00CF6210A92E2856F6634961005FF2EEB1218400623A22FB4A6DEE44FA84A600C7AB803960DC3F9
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:33:59.243 1a38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/07/22-02:33:59.246 1a38 Recovering log #3.2021/07/22-02:33:59.246 1a38 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):	5.292281613830528
Encrypted:	false
SSDEEP:	6:m3B9+q2Pwkn23iKKdKusNpZQMxIFUtpP3JZmwP8dN9VkwOwkn23iKKdKusNpZQMT:SivYf5KkMFUtpPZ/PA5Jf5KkTJ
MD5:	7C0069B259339FD1B6BE72D1C927F939
SHA1:	330EE90C6E0BDC58106D36C94F4688438788ED4C
SHA-256:	63096997735FE9F484B545CF815AFF255A5C9F94924C0014E5295259BB4C7194
SHA-512:	9005E82A7C5F571E7B905F2F7C6DFFE0994E1D4355FD91CE8EC2EBC1259F628C533AC4A82FDF76AD1F3E901AE82ACEFF9753F5FB1626AA92F9E5464853148C7
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:15.964 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/07/22-02:34:15.965 1a48 Recovering log #3.2021/07/22-02:34:15.966 1a48 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
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):	5.214404105721459
Encrypted:	false
SSDEEP:	12:UvYf5KkkGHArBFUtpHZ/PBz5Jf5KkkGHAryJ:eYf5KkkGgPg1lJf5KkkGga
MD5:	ED326CB7969209CDF4FECDD3750F3415
SHA1:	830FB9A0A475ECF643A7E71127CB0F07E13FCFC8
SHA-256:	A179C1846D31241E47B8600993CEA47AC38198BCA027243C0DE449D4371A2198
SHA-512:	4EF7C150AE4B3C6677A6C534D8F266DE5028BE1CC454B2A4ABDC1678C803B7797703F8543ED17DCEB7A2E297A89982627D6C600E79010300D36C4975FBB4D98
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:15.700 19e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-02:34:15.704 19e8 Recovering log #3.2021/07/22-02:34:15.706 19e8 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.216034299453171
Encrypted:	false
SSDEEP:	12:RAMvYf5KkkGHArqiuFUtpn11/P/5Jf5KkkGHArq2J:RJYf5KkkGgCgfJf5KkkGg7
MD5:	0C577F8727C0D378C5EEF692ED7321E4
SHA1:	6F3AE58288C21F64544254C13F89694F1F82F587
SHA-256:	1F043165417DBFED33C5BBC78204F811C31E8B37096088281AF67723F0B746D8
SHA-512:	730CF8458618FDD8976654AAE7B5B892E412DCF519A80081EE7052DE305DF5DA3CEDADB902A2DC51AC639B423A59250E009BD3FA1D8460138F217B01259EE39
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:15.712 19e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/07/22-02:34:15.715 19e4 Recovering log #3.2021/07/22-02:34:15.717 19e4 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):	5.1573398892044855
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
SSDEEP:	12:HvYf5KkkGHArAFUtpf11/PfF5Jf5KkkGHArfJ:PYf5KkkGgkgpJf5KkkGgV
MD5:	687A7DB2EE0CDC5F516BC60E3E9C1B02
SHA1:	A325AD9E716F23D7A5A3A12ED07FDC2A7840F58B
SHA-256:	3DDC60FBDFAB7EF853C229B9EB663980836A8D6AF4E78734F262F88603A6575D
SHA-512:	9D90A28690978C38A71F90EB6EA386BFEAD3A2D7A4D7C9C127C17548B5ECD5D58F98870849B85617794ACCCAC26692908D7156F339A9E7AF8717A0B4092E9BB
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:30.940 19e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/07/22-02:34:30.943 19e4 Recovering log #3.2021/07/22-02:34:30.943 19e4 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\a1867aa1-840d-4cec-a3d2-ea69dc6a1e78.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):	5.236199648365085
Encrypted:	false
SSDEEP:	6:mkcylyq2Pwkn23iKKdKpIFUtplcEF1ZmwPlcETRkwOwkn23iKKdKa/WLJ:VcylvYf5KkmFUtplcE1/PlcG5Jf5KkaQ
MD5:	0274A97EECFA9F46864B46C690C72BA4
SHA1:	2D34B97079FDCA614577CD9D35BE464E7E90BE60
SHA-256:	63F94313C54D70EB30EBBBC1B50FFA06390924797C4D5C157A071B8DF74C660E
SHA-512:	0743E5C602055AF9E7DF3E04A697155911932160EE9A3E79034BB835390EA8EC319627DC2994F122C8F889AB71A07F9522F2552576D91066EB885820A600368F
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:33:58.924 19e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/22-02:33:58.928 19e4 Recovering log #3.2021/07/22-02:33:58.928 19e4 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):	5.2811083623765045
Encrypted:	false
SSDEEP:	6:mhq2Pwkn23iKKdKks8Y5JKKhdIFUtp8ZZmwPBkwOwkn23iKKdKks8Y5JKKTLJ:gvYf5KkkOrsFUtpQ/PB5Jf5KkkOrzJ
MD5:	4F5F40E6C2A63FCD962140754A46EB6F
SHA1:	BF988C22A57172CF91B2CEC315F3762E507C6429
SHA-256:	CACE129E1BC3593F696BFCC79E077F2B5E8228D947B480398D6F9D01EB9321A3
SHA-512:	DBCEB5A97742C5841BEC29F6663958D153AB1BDF6146C48DA77A3B73F01D3DE38743EF2A1EE826EF2F4C6EEC380E8ED0835D34A5850F7AE36DA7AA0A3F0C61CF
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:17.411 19b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/22-02:34:17.412 19b4 Recovering log #3.2021/07/22-02:34:17.413 19b4 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\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:nZI:nO
MD5:	B107DDCA1112E58930CBBC96E7FC5AD9
SHA1:	2B4316AA8A7F8C29AE497766810E12095A2C6AFB
SHA-256:	CF41D8E4F9C305BC842971D0D6182E5E10DC5F209FB2DB8A9FC2EC37A56340DE
SHA-512:	17CF16FA6ABB538A50CD8572CB38A4F1E42EF9B2DC2737EB5F3D3B8E8C0CA246ED86DED1BD88136D16BE1812FFE261F4193281CCF6D10E8D04948290BA526E08
Malicious:	false
Reputation:	low
Preview:	.....|...,.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b1b666ab-bb79-4a6e-b55a-e152b1950b82.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):	2799
Entropy (8bit):	4.862060771479396
Encrypted:	false
SSDEEP:	48:Y2nzMKDHGXtwWsKoRSepsF8zsO6qC5gJh86N+4l5snkzsiDsuyKsBP3gYhbw:JnzMKDHGXOco0PExC5GC6N+WoYX8PxhM
MD5:	EABAB5B7F46E602DE06D3A95AC1FA17C
SHA1:	1343FC23BE1277BFF4183DC084444843E77768D6
SHA-256:	2D3A142B163A69F42A995A46BCDFE63E9BC7512BF2FA608F5225C74A574E7158
SHA-512:	FF42EC6AED206B8D64309EA9C5E5B01495F08159AF40D86B48562D7BF431A6F56C12E523C7D9AAB7D9FB24B02DD7864E03DEB4E653173DB02C97EFD677E466B
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273979642936647","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"isolation":[],"server":"https://kit.fontawesome.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273979643506489","port":443,"prot

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.426100848929159
Encrypted:	false
SSDEEP:	3:tUKIC2P+EGFmWZmwv32C2gvFOA7V8s2C2gvFOA7WGv:m3UFmWZmwP+gvFjVv+gvFjtv
MD5:	FDB4A619BEA984337CA6F56B30496171
SHA1:	6F6709D2F9E49A8AB451F0BAFDBECD4290E1C12D
SHA-256:	905C8CB4BF13D7F22F9257BB46C2820563CF002DC049E9DE377868D02B782001
SHA-512:	C75724215221AE253514884BD41BFC8CC655F9A0C1EA9A75E346D6EDA31FDC0CB2762544AFC61A63288DD5480E8E9B49AE9C61188DBA12DAF2033E7B6AF4E80
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:34:14.132 18cc Recovering log #3.2021/07/22-02:34:14.260 18cc Delete type=0 #3.2021/07/22-02:34:14.260 18cc 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:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e5c5a9d3-8e30-4de6-934e-e201c72de554.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):	1376
Entropy (8bit):	5.58049257246071
Encrypted:	false
SSDEEP:	24:Ym6H0UhsS+kJVIUTkIG1KUjXzkq/HeUe8zUeT7wU43NYxYUkRUeiQ:Ym6UUhdJeUwXKUjYqPeUekUevwUEsYU8
MD5:	A85BCB1E7C16B1DB218DB7C5691B7325
SHA1:	C71288012BBA0E7D412044DD1C14FB422C80F2A5
SHA-256:	E799D59EDDB3BD2B653EC923A00523DE9D7A73EC339F3985F7037E1B22234CF1
SHA-512:	F801B053107E14B8D69CE245C9DCC21C6442916D1B2A7C6DAE6A26BDED6CD9E10C32A039B9FF16764D7831857998DEE73BC1883D612053A5ABEDA35F0D6A64B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e5c5a9d3-8e30-4de6-934e-e201c72de554.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1658450043.533593,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626914043.533599},{"expiry":1658450043.557599,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626914043.557605},{"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":1658450042.936765,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ec8b62d7-bbc6-4ca7-9625-9edb4daeabd5.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):	5813
Entropy (8bit):	5.167728940525638
Encrypted:	false
SSDEEP:	96:nnLSoMzVdGwwFlIKIM5k0JCKL8GzkpS1wbOTlVuHn:nnL/MzXuFlIah4K/kY+
MD5:	65B4F9620ADC458E8087250F7A7B22D4
SHA1:	5468180268DCF79DFDFE5726B4421F350A387948
SHA-256:	EBE49A7295FDBAE71850EDB488369C26000152DD30AE891AFAB2E589B80074F3
SHA-512:	1583322D4AAF3626B0F8167B6499C5B537AEB2157453FF2A063554AC3BE5DFE123DDB78CA86D54F1204A8B7C668C0721C064DBDDBD8027B4F62005DC9C4E07
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271387639211629","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\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\dae13946-cbe1-4e54-bc64-06aa5f815488.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\dae13946-cbe1-4e54-bc64-06aa5f815488.tmp	
Category:	dropped
Size (bytes):	174555
Entropy (8bit):	6.079534468236113
Encrypted:	false
SSDEEP:	3072:VydkZExZKKJEuwA4x37SiHnDcWYKWFuFcbXaflB0u1GOJmA3iuRP:UMExzgRx37iWYFOaqfIlUOoSiuRP
MD5:	19705C504DC88BE0683A6DA889C1CF6F
SHA1:	7A777B6B01DEDDE2A0CE661D5024819D066F12D2
SHA-256:	A9A35E171B455DF9C3ACF79BAF9E65B7C46B31DBAD21C33299A24B4A6DE0FFFA
SHA-512:	A217D9C95919C05566BF29DA0BA643FEAC234A385A4B1F4E7D4F570ECF128CF371BB3F32918EC0FF11E3A707143D232B3CBD9995C605DF19B31494735974E0D
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":1.626914041691184e+12,"network":1.626914043e+12,"ticks":5556256593.0,"uncertainty":3719033.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Temp\229fe51b-f1d2-40c3-b8b0-1035172b36dd.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\33208a7b-289c-4b64-a6a7-29e1f4763fdc.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
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..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\bae6bfdc-6cd3-46ef-bd38-7610a5fb99d5.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

C:\Users\user\AppData\Local\Temp\bae6bfdc-6cd3-46ef-bd38-7610a5fb99d5.tmp	
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

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):	12670
Entropy (8bit):	4.6471439140835855
Encrypted:	false
SSDEEP:	192:jLVLsVklGYrh1w/ZFsMcTdeg5FmQ79Xn9wMzMwMDQTeSj:jLVLsklGow/ZFsZeY9wQT
MD5:	2DFEE57403E13D72EAC1A560DA43A63F
SHA1:	21175091526C55816C81DEAD238D867701504DFD
SHA-256:	92DA2EC183AE74674B658B62C083A30A7F66B41AFA9A4706D4BE801B93F4A80E
SHA-512:	839CD4041B2E94D6D38621DE077C0B2FE39DEA254FE9C76857993ABEAC8D2D8521A82493E4B98969587DDF7D4FB63F56EAD2F349C3B7CD26D9AACA8C7CED8CA
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 764557b765167a387d3431cd48289755f89ff5a87d4d24963c119add8d6a6961 bb774b99355b24be272df03f57e18b5b55cd1b98c614359418406e49d8e88725.SERVER_HANDSHAKE_TRAFFIC_SECRET 764557b765167a387d3431cd48289755f89ff5a87d4d24963c119add8d6a6961 a4e5dffa4109f5d6cb969b6ca23917fa1f03782cb736b91baeaf0c7d12d7676f.CLIENT_HANDSHAKE_TRAFFIC_SECRET 434d399add66ed80c810d8449cf2fdf7970e940dca789cb03a97ce18320f184e 49d8ad6abbd82147ca5a72bdd59b7cc3fe58a8a4fa1b8c5c3639ff3dde010814.SERVER_HANDSHAKE_TRAFFIC_SECRET 434d399add66ed80c810d8449cf2fdf7970e940dca789cb03a97ce18320f184e e5361416b4cd95a081eb7022f7afbac847c06cb5e70849296f5c582b45f53b84.CLIENT_HANDSHAKE_TRAFFIC_SECRET ee6fae3443328e9d4c1483c37ae0d63eee2ecf0f0ca77329c7fe4d09a578026c fcaa987ecbf522d9d7957c4b32d6d9e68a2239f77857df4b0cc5d394ebb4499a.SERVER_HANDSHAKE_TRAFFIC_SECRET ee6fae3443328e9d4c1483c37ae0d63eee2ecf0f0ca77329c7fe4d09a578026c 6b8a3d01b5906073cfa74f9b57d01f3c049ae34b0e04514628428e2d53bee007.CLIENT_TRAFFIC_SECRET_0 7645

C:\Users\user\AppData\Local\Temp\cc861f09-9ff1-4dcb-809b-e38bd74d072e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;..~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.:.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\am\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0lprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA 2
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "......... .. ..".. },.. "1428448869078126731": {.. "message": "........ .. ..".. },.. "1522140683318860351": {.. "message": "........... .. .., ...".. },.. "1550904064710828958": {.. "message": "......".. },.. "1636686747687494376": {.. "message": ".......".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "....... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:IPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4 C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE 1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. " END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "1522140683318860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\de\messages.json	
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\es\messages.json	
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71EEEE
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Congelaci.n de im.genes".. },.. "12139579827238759 20": {.. "message": ".Cu.l de las siguientes respuestas describe mejor tu red?".. },.. "12827687646031907 5": {.. "message": "Detecci.n de dispositivo".. },.. "14284488690781267 31": {.. "message": "Fluidez del v.deo".. },.. "15221406833188603 51": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "15509040647108289 58": {.. "message": "V.deo fluido".. },.. "16366867476874943 76": {.. "message": "Perfecta".. },.. "18027627465894571 77": {.. "message": "Volumen".. },.. "18503975003120203 88": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB11202723566
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Hangub".. },.. "12139579827238759 20": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "12827687646031907 5": {.. "message": "Seadme tuvastamine".. },.. "14284488690781267 31": {.. "message": "Video sujuvus".. },.. "15221406833188603 51": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "15509040647108289 58": {.. "message": ".htlane".. },.. "16366867476874943 76": {.. "message": "T.iuslik".. },.. "18027627465894571 77": {.. "message": "Helitugevus".. },.. "18503975003120203 88": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".... ... .".. },.. "12139579827238759 20": {.. "message": ".... .. ..".. },.. "12827687646031907 5": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "....".. },.. "16366867476874943 76": {.. "message": "....".. },.. "18027627465894571 77": {.. "message": "..... ...".. },.. "18503975003120203 88": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\fi\messages.json	
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A5261952050 21
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "152214068331886 0351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C00 0
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "128276876460319075": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-s mooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smoot h".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51 B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Se fige".. },.. "1213957982723875920": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "1428448869078126731": {.. "message": "Fluidit. de la vid.o".. },.. "1522140683318860351": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "1550904064710828958": {.. "message": "Fluide".. },.. "163 6686747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\gu\messages.json	
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876 460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "128276 876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15507
Entropy (8bit):	5.290847699527565
Encrypted:	false
SSDEEP:	192:Pdapr6h85tRwVQgkvJryLkla5Kfndg/V6c8TEKdl:Arwot2Q7BryVce/V6uml
MD5:	3ED90E66789927D80B42346BB431431E
SHA1:	2B061E3271DF4255B1FFC47BDB207CDEC0D9724F
SHA-256:	0B41E3C42414F72C9A12C05F8772597F9685115366A774C66018467AD4B71A74
SHA-512:	92BE43F1FFC8EFBF5BBC50573AC4C65F6104416A5B6CD04404C3A9854CA3DCF2A43A4044C168590CDF83887D234495843572331ADCD5B020D2E48A3956F3C16
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Zamrzavanje".. },.. "1213957982723875920": {.. "message": "Koje od sljede.eg najbolje opisuje va.u mre.u?".. },.. "128276876460319075": {.. "message": "Otkrivanje ure.aja".. },.. "1428448869078126731": {.. "message": "Ujedna.enost videoreprodukcije".. },.. "1 522140683318860351": {.. "message": "Povezivanje nije uspjelo. Poku.ajte ponovo.".. },.. "1550904064710828958": {.. "message": "Glatko".. },.. "16366867 47687494376": {.. "message": "Savr.ena".. },.. "1802762746589457177": {.. "message": "Glasno.a".. },.. "1850397500312020388": {.. "message": "Vidite li svoj Chromecast u $START_LINK$aplikaciji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "co ntent": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15682
Entropy (8bit):	5.354505633120392
Encrypted:	false
SSDEEP:	192:CCEAproS9fZv+JwkDMrC2NSxoSgbV6c8TEKdl:5r5VZv+RDMrazoV6uml
MD5:	8E9FF7E49473C5734A2F6F0812E12EB3
SHA1:	A4F10DDD1580582533D5EB59EDF6D8048F887C81
SHA-256:	6CDD2FB39ADECE00E88B989E464B05ED1414092D0492F6D0AE58D549BFD1A46A
SHA-512:	E9A4AF31B1A276F395599BB620A3164CABF3459F3C102DD3F57DFEA734510BD985DE65CB409E1975559ACCC615075439A08E1DEBE22C90A0ABCAA3CAFEE79A C7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\hu\messages.json	
Preview:	{.. "1018945614885205 17": {.. "message": "Lefagy".. },.. "1213957982723875920": {.. "message": "Az al.bbiak k.z.l melyik jellemzi legjobban h.l.zat.t?".. },.. "1282768764603190 75": {.. "message": "Eszk.zfelfedez.s".. },.. "1428448869078126731": {.. "message": "Vide. folyamatoss.ga".. },.. "1522140683318860351" : {.. "message": "Sikertelen kapcsol.d.s. K.rj.k, pr.b.lja .jra.".. },.. "1550904064710828958": {.. "message": "Folyamatos".. },.. "1636686747687494376": {.. "message": "T.k.letes".. },.. "1802762746589457177": {.. "message": "Hanger.".. },.. "1850397500312020388": {.. "message": "L.tja a Chromecastot a $STA RT_LINK$Google Home alkalmaz.sbanEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15070
Entropy (8bit):	5.190057470347349
Encrypted:	false
SSDEEP:	192:GsprMtChjkWfrEWL0KRCnEOWV6c8TEKdl:9rtAEr3LTRuWV6uml
MD5:	7ADF9F2048944821F93879336EB61A78
SHA1:	C3DA74FB544684D5B250767BB0CB66FFB7C58963
SHA-256:	3630947E1075E3663AD3E4824D0BE42CB47C0D615D8053E83B9595047C8BA9BE
SHA-512:	1F28BB80E1839C5581106BEA3AE2501C7618249D7E3115819F5A9A87771D59F5DE346C1B9C87F7FFC390604D5B9888CE738E25F2F04A094002A0FB3B22CBEC95
Malicious:	false
Reputation:	low
Preview:	{.. "1018945614885205 17": {.. "message": "Membeku".. },.. "1213957982723875920": {.. "message": "Dari berikut ini, manakah yang paling mendeskripsikan jaringan Anda?".. },.. "1282768764603190 75": {.. "message": "Penemuan Perangkat".. },.. "1428448869078126731": {.. "message": "Kelancaran Video".. },.. "1522140683318860351": {.. "message": "Sambungan gagal. Coba lagi.".. },.. "1550904064710828958": {.. "message": "Lancar".. },.. "1636686747687494376" : {.. "message": "Sempurna".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Bisakah Anda melihat Chromecast di $START_LINK$aplikasi Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": " $1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15256
Entropy (8bit):	5.210663765771143
Encrypted:	false
SSDEEP:	192:lYprk52dAaykVza8rE0QWBKD9+vq0hKEV6c8TEKdl:qrlA8r6DalV6uml
MD5:	BB3041A2B485B900F623E57459AE698A
SHA1:	502F5EA89F9FB0287E864B240EA39889D72053A4
SHA-256:	025737EF8FA06706B3F26D0F52B4844244A6D33DAE1D82FEF2931A14C003D57E
SHA-512:	BA51784073BEF82F3A116B33DA406FDB10EC823B9EE74375C46036DAD8BDCB4141F60845DE141ABE42CEEF9251572F6AB287CA5FC7669C60E4F68071D5AB8C D
Malicious:	false
Reputation:	low
Preview:	{.. "1018945614885205 17": {.. "message": "Si blocca".. },.. "1213957982723875920": {.. "message": "Quale delle seguenti definizioni descrive meglio la tua rete?".. },.. "1282768764603190 75": {.. "message": "Rilevamento dispositivi".. },.. "1428448869078126731": {.. "message": "Uniformit. video".. },.. "1522140 683318860351": {.. "message": "Connessione non riuscita. Riprova.".. },.. "1550904064710828958": {.. "message": "Fluido".. },.. "1636686747687494376": {.. "message": "Perfetta".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Riesci a vedere il tuo dispositivo Chromecast nell'$START_LINK$app Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16519
Entropy (8bit):	5.675556017051063
Encrypted:	false
SSDEEP:	192:nkprPhQdxkRWrZe1wYpMR5wnAV6c8TEKdl:YrLRWri65wAV6uml
MD5:	6F2CC1A6B258DF45F519BA24149FABDC
SHA1:	8A58C7880C6D22765DCBB6BCE22A192C1B109AE1
SHA-256:	42ECFEE727CFC4F2845FEFDACE5EDC2E0A40AFAD69973A3B950CE653A7633342
SHA-512:	F7454F0E14301C59CC54361ACC0A1C6D072EF9BDF5DEA60646FB90B1CE47612785938C784A4CF1DE3E62648A14420374933B5F5DA43907BC00D3799FF163A3D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6436_1544878504\CRX_INSTALL_locales\ja\messages.json

Preview:

{.. "10198456l4885205l7": {.. "message": "...".. },.. "1213957982723875920": {.. "message": "...".. },.. "1282768764603190 75": {.. "message": "......".. },.. "1428448869078126731": {.. "message": ".....".. },.. "1522140683318860351": {.. "message": "...".. },.. "15509040 64710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..".. },.. "18503975 00312020388": {.. "message": "$START_LINK$Google Home ...END_LINK. Chromecast .....$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_ LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".

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
Jul 22, 2021 02:34:02.553657055 CEST	192.168.2.4	8.8.8.8	0x762b	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:02.555660009 CEST	192.168.2.4	8.8.8.8	0x95b7	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:02.558804035 CEST	192.168.2.4	8.8.8.8	0x6e79	Standard query (0)	vivacious-omniscient-crocodile.glitch.me	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:03.264573097 CEST	192.168.2.4	8.8.8.8	0x639e	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:03.266438007 CEST	192.168.2.4	8.8.8.8	0x847f	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:03.270030975 CEST	192.168.2.4	8.8.8.8	0xa04c	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.021018028 CEST	192.168.2.4	8.8.8.8	0x27dd	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.067945004 CEST	192.168.2.4	8.8.8.8	0x4445	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.068700075 CEST	192.168.2.4	8.8.8.8	0xa102	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:14.531488895 CEST	192.168.2.4	8.8.8.8	0x4897	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:34:02.615356922 CEST	8.8.8.8	192.168.2.4	0x95b7	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:02.618379116 CEST	8.8.8.8	192.168.2.4	0x6e79	No error (0)	vivacious-omniscient-crocodile.glitch.me		107.23.110.216	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:02.618379116 CEST	8.8.8.8	192.168.2.4	0x6e79	No error (0)	vivacious-omniscient-crocodile.glitch.me		52.5.55.81	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:34:02.618379116 CEST	8.8.8.8	192.168.2.4	0x6e79	No error (0)	vivacious-omniscient-crocodile.glitch.me		52.20.88.154	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:02.618379116 CEST	8.8.8.8	192.168.2.4	0x6e79	No error (0)	vivacious-omniscient-crocodile.glitch.me		52.86.228.72	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:02.621164083 CEST	8.8.8.8	192.168.2.4	0x762b	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:34:02.621164083 CEST	8.8.8.8	192.168.2.4	0x762b	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:03.313684940 CEST	8.8.8.8	192.168.2.4	0x639e	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:34:03.326100111 CEST	8.8.8.8	192.168.2.4	0x847f	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:03.326100111 CEST	8.8.8.8	192.168.2.4	0x847f	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:03.328790903 CEST	8.8.8.8	192.168.2.4	0xa04c	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:34:03.761674881 CEST	8.8.8.8	192.168.2.4	0x7309	No error (0)	gstaticadssl.l.google.com		172.217.23.99	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.081968069 CEST	8.8.8.8	192.168.2.4	0x27dd	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:34:04.127506018 CEST	8.8.8.8	192.168.2.4	0xa102	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.127506018 CEST	8.8.8.8	192.168.2.4	0xa102	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.128777027 CEST	8.8.8.8	192.168.2.4	0x4445	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.128777027 CEST	8.8.8.8	192.168.2.4	0x4445	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.128777027 CEST	8.8.8.8	192.168.2.4	0x4445	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.128777027 CEST	8.8.8.8	192.168.2.4	0x4445	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.128777027 CEST	8.8.8.8	192.168.2.4	0x4445	No error (0)	i.ibb.co		152.228.223.13	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.128777027 CEST	8.8.8.8	192.168.2.4	0x4445	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:04.128777027 CEST	8.8.8.8	192.168.2.4	0x4445	No error (0)	i.ibb.co		152.228.223.13	A (IP address)	IN (0x0001)
Jul 22, 2021 02:34:14.601497889 CEST	8.8.8.8	192.168.2.4	0x4897	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:34:14.601497889 CEST	8.8.8.8	192.168.2.4	0x4897	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)

HTTPS Packets

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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 02:34:02.955360889 CEST	107.23.110.216	443	192.168.2.4	49741	CN=glitch.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Jan 18 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Feb 16 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jul 22, 2021 02:34:02.958676100 CEST	107.23.110.216	443	192.168.2.4	49739	CN=glitch.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Jan 18 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Feb 16 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6436 Parent PID: 4108

General

Start time:	02:33:57
Start date:	22/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://vivacious-omniscient-crocodile.glitch.me/nikifi.html'
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: 6668 Parent PID: 6436

General

Start time:	02:33:59
Start date:	22/07/2021
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=1452,4658061009318139164,17467065807480813 58,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1840 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly