ID: 471904
Cookbook: browseurl.jbs
Time: 07:40:28
Date: 26/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

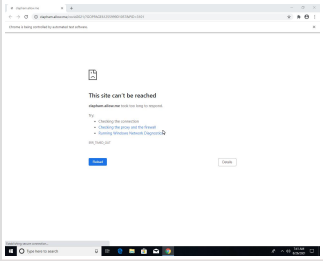
Windows Analysis Report https://clapham.allow.me/cov…

Overview

General Information

Sample URL:	http://https://clapham.allow.me/covid2021/?GOPPAGE61255999D1057&PID=3101
Analysis ID:	471904
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

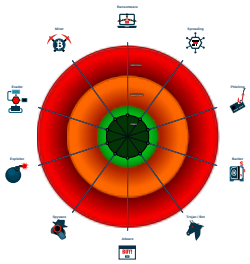
Detection

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

Signatures

No high impact signatures.

Classification



Analysis Advice

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

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

Process Tree

- **System is w10x64**
- chrome.exe (PID: 852 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://clapham.allow.me/covid2021/?GOPPAGE61255999D1057&PID=3101' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5076 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1548,783261014365729635,14637000979693343300,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1732 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2021

Jbx Signature Overview

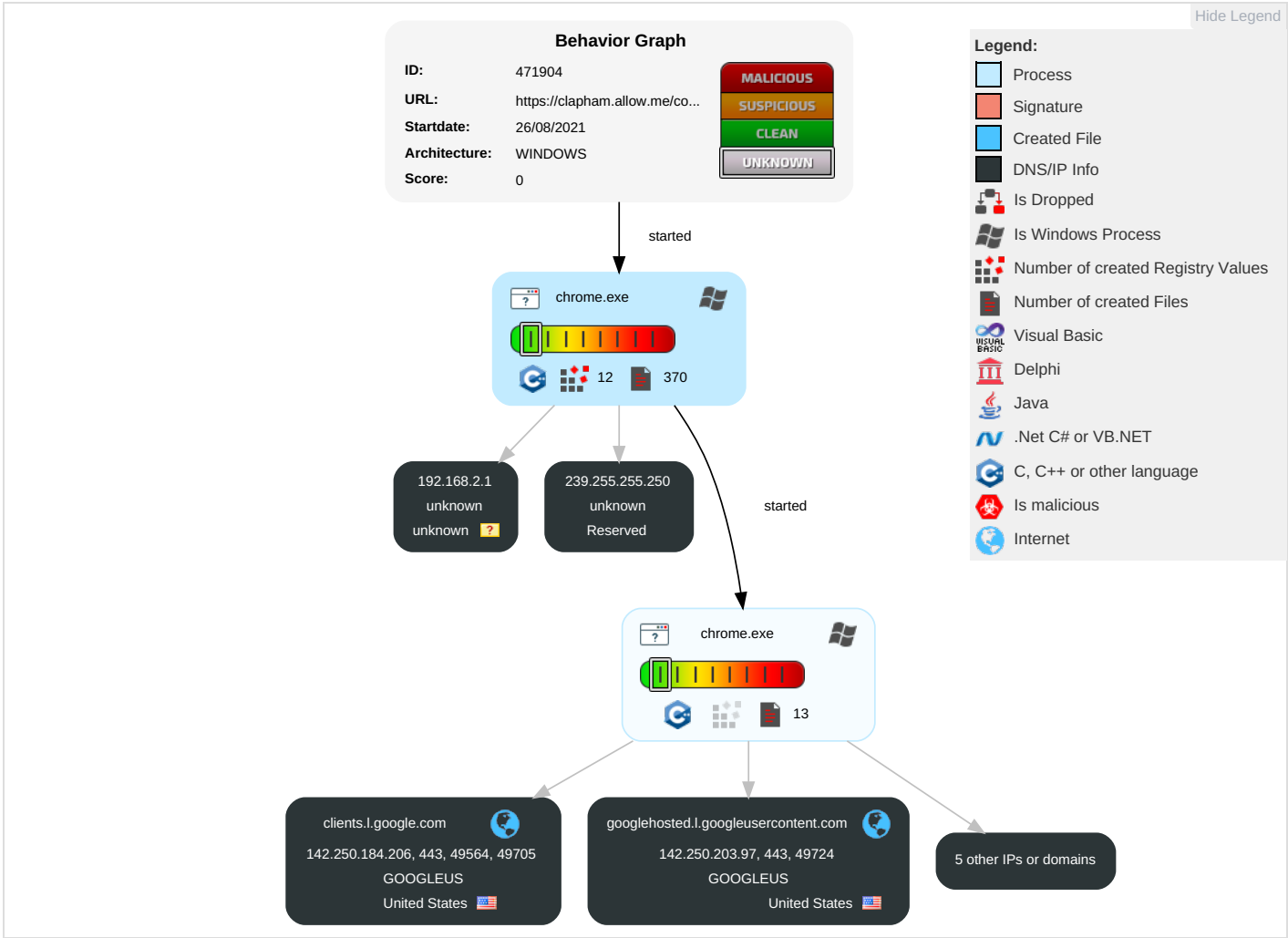
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	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

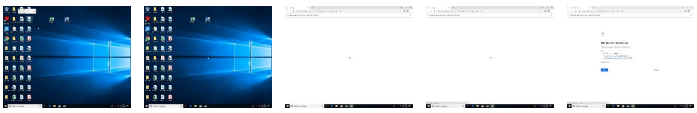


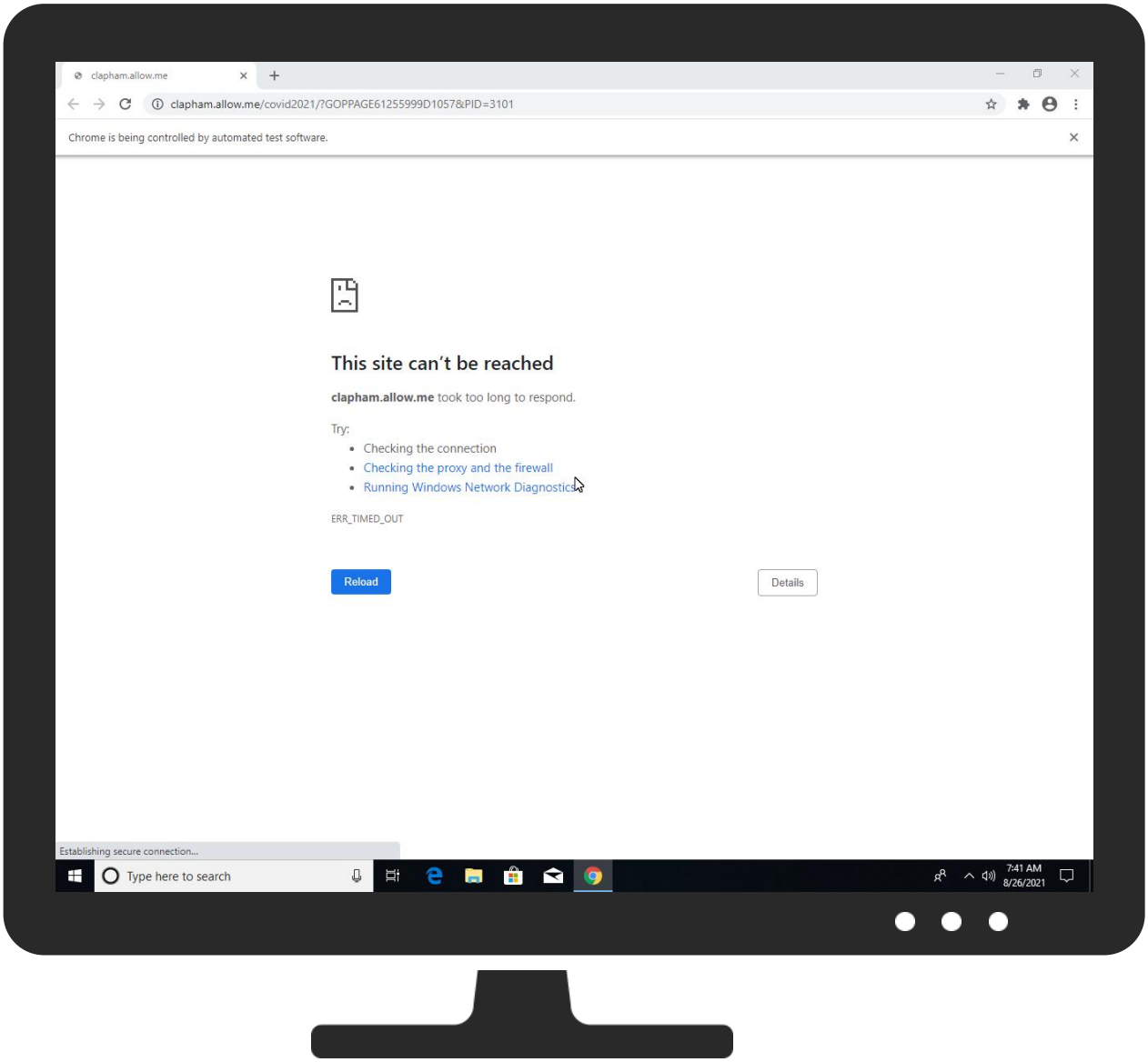
Copyright Joe Security LLC 2021

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://clapham.allow.me/covid2021/?GOPPAGE61255999D1057&PID=3101	0%	Virustotal		Browse
http://https://clapham.allow.me/covid2021/?GOPPAGE61255999D1057&PID=3101	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
clapham.allow.me	52.56.219.240	true	false		unknown
clients.l.google.com	142.250.184.206	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.56.219.240	clapham.allow.me	United States		16509	AMAZON-02US	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
142.250.184.206	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	471904
Start date:	26.08.2021
Start time:	07:40:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://clapham.allow.me/covid2021/?GOPPAGE61255999D1057&PID=3101
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

Copyright Joe Security LLC 2021

Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.win@27/173@4/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All
Errors:	• URL not reachable

Simulations

Behavior and APIs

Time	Type	Description
07:41:26	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:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

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:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
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):	3.133376811589353
Encrypted:	false
SSDEEP:	6:kKgHCdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:YH+5kPlE99SNxAhUe0et
MD5:	E7B5236470190FC1896F9BF8F44B3764
SHA1:	A4ADBC9F7B20745108293F14545EC419FD7057F4
SHA-256:	92170AD024521AC4A8AAB128F0029BF7D57F65FC72117BFB7EB1F991413FAB12
SHA-512:	7EBAB83BCC02EF983546523A3C3C6E95B23BDD6ED30117B56D44C9077910F45FBF2942C57E6222222AEBC877405F9ECA7DE46E0045EE33B880BDF9740B757FE9
Malicious:	false
Reputation:	low
Preview:	p..... .....L..s....(..... .....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\37adb945-28e1-4f5e-8a3c-3806da6422cf.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):	178080
Entropy (8bit):	6.078843623541878
Encrypted:	false
SSDEEP:	3072:P5nmm8A1PCyn3BOIrdvrVslFcbXafIB0u1GOJmA3iuRt:xnP8oPjxwaqfIlUOoSiuRt
MD5:	F92F578764DC1A39BFE2AE07C6655CB5
SHA1:	423CD39C0113441F1ADB5703882C76C9033E2CDF

C:\Users\user\AppData\Local\Google\Chrome\User Data\37adb945-28e1-4f5e-8a3c-3806da6422cf.tmp	
SHA-256:	F477974FA981BE8521C93D45D5D6ED129AE3E233E90F32C62BE5514BB411184D
SHA-512:	C8C655AEE62EF96F70A00475B15C252B272490976415626D28706621822852345451ADD07C7FFA901CCF8F073D4A9643E76A5988A1B0F78024FC3AAD6F8DADEAE
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.629988884569137e+12,"network":1.629956486e+12,"ticks":6842890079.0,"uncertainty":5036518.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

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):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D0212942563 72C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ef83f2e-7335-4d1a-afb1-a90612b7c869.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):	22594
Entropy (8bit):	5.535888625396798
Encrypted:	false
SSDEEP:	384:5kntgLlIEX51kXqKf/pUZNCgVLH2HfDTrU1HGunT+ngqYW4Q:nLlg51kXqKf/pUZNCgVLH2HfvrUJGung
MD5:	9BCCF9C645A550970B280AEBFAF48CE6
SHA1:	5425EA812A012B1FA48EA8DE34F5D7AF19E21D09
SHA-256:	1066CBEA3741ED11B3CBB97E88CADC76127C848961C932CE39FD7026C6765A02
SHA-512:	E6D16B4D8D027879275BE1C6F6BB9964538A7674397A6E44163B35B17C5DE78F61220188BC74FC3998D7C2E76929583AC3A6073598CCE50440FF64511CC231BF
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":"13274462481134628","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\476210a3-ee29-4f24-96ab-a6580b3fd396.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):	1039
Entropy (8bit):	5.567823319207455
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvq7wUlbRUenHQ:YI6UUhVseKUewqPeUer2Uef0wUllUenw
MD5:	A8FED1D97B7DA9EEB08DDB16447645E5
SHA1:	13EF38D20C1E4CD8591D6C964E65BB5F24C0C808
SHA-256:	5048CD2BAD288A703FB82B9D40F67EF30B6BB4412AF9E2F184DC3E4BD738152D
SHA-512:	87A666A1FA2E642C641C1EB75D553CE881CAEEC09EF642E756C03CA1FF651B70E8E6286BBDD8746E55BDC68F97278B55A19D1BAE32223315D233A2A59217F4A1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\476210a3-ee29-4f24-96ab-a6580b3fd396.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1661524886.613034,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629988886.613038},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6660e9d0-b3ee-4379-9b31-4c2029ccdf8b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.273752678742619
Encrypted:	false
SSDEEP:	6:mYAlw4q2PWXp+N23iKKdK9RXXTZIFUtppAgJZmwPpAV13DkwOWXp+N23iKKdK9Rn:5R4va5Kk7XT2FUtppXJ/Pp+13D5f5KkT
MD5:	4B0D45B2B4B7FF1E5BAEFADA18B18F05
SHA1:	16FD1C64DC1F61460DB176ED0A50994B838F2ECF
SHA-256:	58DAD615D32A5D53193E95C317886445984CBF16C50E5BD6DFD56002E29B314F
SHA-512:	B9528853B0F3B80A41E6C3943685437008E76E39F07180D58372B0D03ED88F6B1EBC90D48A960577CEA59A86F2CDAAB230BE72CDC97F61BABF20A98351DFA52
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.944 19b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/26-07:41:27.946 19b0 Recovering log #3.2021/08/26-07:41:27.947 19b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.273752678742619
Encrypted:	false
SSDEEP:	6:mYAlw4q2PWXp+N23iKKdK9RXXTZIFUtppAgJZmwPpAV13DkwOWXp+N23iKKdK9Rn:5R4va5Kk7XT2FUtppXJ/Pp+13D5f5KkT
MD5:	4B0D45B2B4B7FF1E5BAEFADA18B18F05
SHA1:	16FD1C64DC1F61460DB176ED0A50994B838F2ECF
SHA-256:	58DAD615D32A5D53193E95C317886445984CBF16C50E5BD6DFD56002E29B314F
SHA-512:	B9528853B0F3B80A41E6C3943685437008E76E39F07180D58372B0D03ED88F6B1EBC90D48A960577CEA59A86F2CDAAB230BE72CDC97F61BABF20A98351DFA52
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.944 19b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/26-07:41:27.946 19b0 Recovering log #3.2021/08/26-07:41:27.947 19b0 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Size (bytes):	318
Entropy (8bit):	5.280486964369888
Encrypted:	false
SSDEEP:	6:mYATN4q2PWXp+N23iKKdKyDZIFUtppAQ13JZmwPpAXPDkwOWXp+N23iKKdKyJLJ:54N4va5Kk02FUtpp313J/Pp4D5f5KkWJ
MD5:	4DF02DEFE2D3AC15A9F7F428A40E1727
SHA1:	C9F7C9A6BAF2B3E2E0420E27B710D08BF519CDD4
SHA-256:	63064DCC3BFAB02F6A116AFC9B3EF0416A215B2493A9C83C3A7BEC40725823DA
SHA-512:	6DE7F6FABC481B76EB7CD84927CE351D69183160E9E099795B491678DAAEB0D03AFE9DB497E698CBD150E1A19D5C404AC775295FE1D66E5E514FFF672FBB8D7
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.934 19b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/26-07:41:27.935 19b0 Recovering log #3.2021/08/26-07:41:27.936 19b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old.` (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.280486964369888
Encrypted:	false
SSDEEP:	6:mYATN4q2PWXp+N23iKKdKyDZIFUtppAQ13JZmwPpAXPDkwOWXp+N23iKKdKyJLJ:54N4va5Kk02FUtpp313J/Pp4D5f5KkWJ
MD5:	4DF02DEFE2D3AC15A9F7F428A40E1727
SHA1:	C9F7C9A6BAF2B3E2E0420E27B710D08BF519CDD4
SHA-256:	63064DCC3BFAB02F6A116AFC9B3EF0416A215B2493A9C83C3A7BEC40725823DA
SHA-512:	6DE7F6FABC481B76EB7CD84927CE351D69183160E9E099795B491678DAAEB0D03AFE9DB497E698CBD150E1A19D5C404AC775295FE1D66E5E514FFF672FBB8D7
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.934 19b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/26-07:41:27.935 19b0 Recovering log #3.2021/08/26-07:41:27.936 19b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9687170285935388
Encrypted:	false
SSDEEP:	24:M6cLgAZOZD/JqLbJLbXaFpEO5bNmISHn06UwQ8:M68NOZJq5LLOpEO5J/Kn7Uj8
MD5:	77419A374EDF5886AD7A9294098A7601
SHA1:	A1CEEA20F6F257985F613FAB28D4DE0AB386C305
SHA-256:	FE322A4534BCB6D3EA48E6FBE9BFE5B2949DAF6238819C2A6D088470717897D9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
SHA-512:	A907AB4C806D87C613A233E10EA959BE696BB7D85CA4850A715CBBAFA584F73F7E11AB14EB1A12C4C0F46B167F1573DA408D91A199880E89DAA56C73E5AC86 3
Malicious:	false
Reputation:	low
Preview:	.....g4..... ....

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):	1093
Entropy (8bit):	3.5407851931228325
Encrypted:	false
SSDEEP:	24:34STwM9IlrlAEVUwHIDhz+wCUwH+RILlL:34EbYxpFlqjeDRL
MD5:	EBDD1D9503BC973C324DED9FB9BB9576
SHA1:	D891D37AC796EF7ECD8ADD92E2CFEC9F2CB923D8
SHA-256:	93C7825B140911804E007AA3CC7665751589DA1127A554516A9536B87E6A8CB9
SHA-512:	2E4E12AD07A17ACB4F0351F46088CCA238F13630AA25E22FBE3A14DF6EE63D8A1C2A5AB25C6BA6E7B99D42F083ECDA04DBAD43FED8C9E0C0788FD9C409771 F13
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...8d7b4a26_5c4b_4969_843d_f2e4fccbc827..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....A...https://clapham.allow.me/covid2021/?GOPPAGE61255999D1057& PID=3101.....h.....`.....\w.....\w...0.....H.....A...h.t.t.p.s.:././.c.l.a.p.h.a.m...a.l.l.o.w...m.e./ .c.o.v.i.d.2.0.2.1./.?.G.O.P.P.A.G.E.6.1.2.5.5.9.9.9.D.1.0.5.7.&.P.I.D.=.3.1.0.1.....8.....0.....8..... .....A...https://clapham.allow.me/covid2021/?GOPPAGE61255999D1057&PID=3101.....)/.....

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	

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):	5.2606880419259685
Encrypted:	false
SSDEEP:	6:mY6ZN+q2PWXp+N23iKKdK8aPrqIFUtpp6uXZmwPp63BVkwOWXp+N23iKKdK8amLJ:56qva5KkL3FUtpp6uX/Pp63P5f5KkQJ
MD5:	C1B21AE3467C82CD87F693350A7C86EA
SHA1:	A30A48EC3BDE145BFE1F3EF5692DF115DFEB66AB
SHA-256:	3756577B82766FF3ECE30F494A7A8141E5F14071F25E0688F3EF81FD6F02E361
SHA-512:	B471BB09FEF89F34E5B274E78ACEC0FF8555A42566D0CF8D9B4139F117734C20F5ED9A644C5E26FAA4D3E229F646410A6866DC1EBA91B053FA1BB398C9F54E3 9
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.473 1768 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/26-07:41:21.474 1768 Recovering log #3.2021/08/26-07:41:21.475 1768 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.2606880419259685
Encrypted:	false
SSDEEP:	6:mY6ZN+q2PWXp+N23iKKdK8aPrqIFUtpp6uXZmwPp63BVkwOWXp+N23iKKdK8amLJ:56qva5KkL3FUtpp6uX/Pp63P5f5KkQJ
MD5:	C1B21AE3467C82CD87F693350A7C86EA
SHA1:	A30A48EC3BDE145BFE1F3EF5692DF115DFEB66AB
SHA-256:	3756577B82766FF3ECE30F494A7A8141E5F14071F25E0688F3EF81FD6F02E361
SHA-512:	B471BB09FEF89F34E5B274E78ACEC0FF8555A42566D0CF8D9B4139F117734C20F5ED9A644C5E26FAA4D3E229F646410A6866DC1EBA91B053FA1BB398C9F54E3 9
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.473 1768 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/26-07:41:21.474 1768 Recovering log #3.2021/08/26-07:41:21.475 1768 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5.. ....f.5................f.5................f.5...............

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):	5.221221715642914
Encrypted:	false
SSDEEP:	6:mYZhsnQL+q2PWXp+N23iKKdK8NIFUtppZh0qG1ZmwPpZhmQLVkwOWXp+N23iKKdF:5ZhsVva5KkpFUtppZh091/PpZhR5f5Kb
MD5:	8EBC93BF832BD748256857DD89CBFB9B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
SHA1:	D4BA2BD2E675FE983429187AD56046CEB4FD03D6
SHA-256:	4A295EE3060EC715008E1C9DB1294F341F6004826189DB6D3BC1FF1A79954DB9
SHA-512:	26C7F76CFC10283E619CC57CC3522ACBEDBFEA74A8B7A05CB5008987A1FDA9FC700D4E91F155D723156A2DD4E40237E904EF1AF2B62AFC91D68EAB01FCE15ED
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:24.046 1478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/26-07:41:24.047 1478 Recovering log #3.2021/08/26-07:41:24.048 1478 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old` (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.221221715642914
Encrypted:	false
SSDEEP:	6:mYZhsnQL+q2PWXp+N23iKKdK8NIFUtppZh0qG1ZmwPpZhmQLVkwOWXp+N23iKKdF:5ZhsVva5KkpFUtppZh091/PpZhR5f5Kb
MD5:	8EBC93BF832BD748256857DD89CBFB9B
SHA1:	D4BA2BD2E675FE983429187AD56046CEB4FD03D6
SHA-256:	4A295EE3060EC715008E1C9DB1294F341F6004826189DB6D3BC1FF1A79954DB9
SHA-512:	26C7F76CFC10283E619CC57CC3522ACBEDBFEA74A8B7A05CB5008987A1FDA9FC700D4E91F155D723156A2DD4E40237E904EF1AF2B62AFC91D68EAB01FCE15ED
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:24.046 1478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/26-07:41:24.047 1478 Recovering log #3.2021/08/26-07:41:24.048 1478 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=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclJ5n0lTpw5JBHV1Kph3/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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.29786883278
Encrypted:	false
SSDEEP:	6:mYAVc1N4q2PWXp+N23iKKdK25+Xqx8chI+IFUtppAcJZmwPpAcDkwOWXp+N23iKG:50yN4va5KkTXfchI3FUtpp/J/Pp/D5fk
MD5:	DABB857C1927B49A924E6B16DFF48BAB
SHA1:	F2DF0F037E4F9C584EC069BA8DA81411B179107E
SHA-256:	4F85C0F5D8D4AAEDF78D5FB5DCE00C79B1ACE9B2EEB43F606B43D04F750D57C0
SHA-512:	3F40360E8FB8C0CCE76DDBC77DBF8798A3BE1737E7F104452AB1DCEE784A96EEB05B27A63954958BA20CA0329AB060CFA37C65D09921824379B3D1222CAE912
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.926 19b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/26-07:41:27.928 19b0 Recovering log #3.2021/08/26-07:41:27.928 19b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.oldSS (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.29786883278
Encrypted:	false
SSDEEP:	6:mYAVc1N4q2PWXp+N23iKKdK25+Xqx8chI+IFUtppAcJZmwPpAcDkwOWXp+N23iKG:50yN4va5KkTXfchI3FUtpp/J/Pp/D5fk
MD5:	DABB857C1927B49A924E6B16DFF48BAB
SHA1:	F2DF0F037E4F9C584EC069BA8DA81411B179107E
SHA-256:	4F85C0F5D8D4AAEDF78D5FB5DCE00C79B1ACE9B2EEB43F606B43D04F750D57C0
SHA-512:	3F40360E8FB8C0CCE76DDBC77DBF8798A3BE1737E7F104452AB1DCEE784A96EEB05B27A63954958BA20CA0329AB060CFA37C65D09921824379B3D1222CAE912
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.926 19b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/26-07:41:27.928 19b0 Recovering log #3.2021/08/26-07:41:27.928 19b0 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):	5.262076228263013
Encrypted:	false
SSDEEP:	6:mYAv4q2PWXp+N23iKKdK25+XuoIFUtppAc3JZmwPpApDkwOWXp+N23iKKdK25+Xp:5s4va5KkTXYFUtpphJ/Pp+D5f5KkTXHJ
MD5:	20E166B2EA34092280E966FAB8AE2AA1
SHA1:	0DD2E69012053E6DA4D9B68F79AB014FADDFF7DC
SHA-256:	9662F1844920276122F52F3A11CE693184E30A147FBDD4330051462FC0C103CD
SHA-512:	4DED7C8B95F21349E63323731CD486C3E80D6646A81042792D046AA19C1519DE3C9B432A28E57CCEAF4587BAFB6CD6E517E43CE0E644FC997636A88F5B99C52
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.921 19b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/26-07:41:27.922 19b0 Recovering log #3.2021/08/26-07:41:27.923 19b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.262076228263013
Encrypted:	false
SSDEEP:	6:mYAv4q2PWXp+N23iKKdK25+XuoIFUtppAc3JZmwPpApDkwOWXp+N23iKKdK25+Xp:5s4va5KkTXYFUtpphJ/Pp+D5f5KkTXHJ
MD5:	20E166B2EA34092280E966FAB8AE2AA1
SHA1:	0DD2E69012053E6DA4D9B68F79AB014FADDFF7DC
SHA-256:	9662F1844920276122F52F3A11CE693184E30A147FBDD4330051462FC0C103CD
SHA-512:	4DED7C8B95F21349E63323731CD486C3E80D6646A81042792D046AA19C1519DE3C9B432A28E57CCEAF4587BAFB6CD6E517E43CE0E644FC997636A88F5B99C52
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.921 19b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/26-07:41:27.922 19b0 Recovering log #3.2021/08/26-07:41:27.923 19b0 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):	5.296730714746152
Encrypted:	false
SSDEEP:	6:mYAY4q2PWXp+N23iKKdKWT5g1IdqIFUtppAqJZmwPpAqDkwOWXp+N23iKKdKWT5i:5D4va5Kkg5gSRFUtpptJ/PptD5f5Kkgk
MD5:	6E84440977D6AC714DCFE2F82006E1CE
SHA1:	935D77348E01098ED91656D287775F2763D2BE3E
SHA-256:	DA9339B84029717382E4D0310ECBB98084AD75D04FD1676DADE4382A3B854A93
SHA-512:	5401FFC74085F331F5F677958BD1AAD35B9875A29369EC97D5980F12C161996D8FEE70191F08F7626ADFA0D30154BAC1171065B00C4C1A73C764CD0AECCF4AD
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.911 19b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/26-07:41:27.913 19b0 Recovering log #3.2021/08/26-07:41:27.913 19b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.oldLL (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.296730714746152
Encrypted:	false
SSDEEP:	6:mYAY4q2PWXp+N23iKKdKWT5g1IdqIFUtppAqJZmwPpAqDkwOWXp+N23iKKdKWT5i:5D4va5Kkg5gSRFUtpptJ/PptD5f5Kkgk
MD5:	6E84440977D6AC714DCFE2F82006E1CE
SHA1:	935D77348E01098ED91656D287775F2763D2BE3E
SHA-256:	DA9339B84029717382E4D0310ECBB98084AD75D04FD1676DADE4382A3B854A93

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.oldLL (copy)	
SHA-512:	5401FFC74085F331F5F677958BD1AAD35B9875A29369EC97D5980F12C161996D8FEE70191F08F7626ADFA0D30154BAC1171065B00C4C1A73C764CD0AECCF4AD
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.911 19b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/26-07:41:27.913 19b0 Recovering log #3.2021/08/26-07:41:27.913 19b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1093
Entropy (8bit):	3.5407851931228325
Encrypted:	false
SSDEEP:	24:34STwM9IlrlAEVUwHlDhz+wCUwH+RlLlL:34EbYxpFlqjeDRL
MD5:	EBDD1D9503BC973C324DED9FB9BB9576
SHA1:	D891D37AC796EF7ECD8ADD92E2CFEC9F2CB923D8
SHA-256:	93C7825B140911804E007AA3CC7665751589DA1127A554516A9536B87E6A8CB9
SHA-512:	2E4E12AD07A17ACB4F0351F46088CCA238F13630AA25E22FBE3A14DF6EE63D8A1C2A5AB25C6BA6E7B99D42F083ECDA04DBAD43FED8C9E0C0788FD9C409771F13
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1..,.....$...8d7b4a26_5c4b_4969_843d_f2e4fccbc827.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....A...https://clapham.allow.me/covid2021/?GOPPAGE61255999D1057&PID=3101.....h.....`.....\w.....\w...0.....H.....A...h.t.t.p.s.:././.c.l.a.p.h.a.m...a.l.l.o.w...m.e./.c.o.v.i.d.2.0.2.1./.?.G.O.P.P.A.G.E.6.1.2.5.5.9.9.9.D.1.0.5.7.&.P.I.D.=.3.1.0.1.....8.....0.....8..... .....A...https://clapham.allow.me/covid2021/?GOPPAGE61255999D1057&PID=3101.....)/.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.204282770097242
Encrypted:	false
SSDEEP:	6:mY6twDM+q2PWXp+N23iKKdK8a2jMGIFUtpp6V6gZmwPp60SDMVkwOWXp+N23iKKV:56tN+va5Kk8EFUtpp6V/Pp603V5f5Kkw
MD5:	59FBB8B518F30AD3D8B4B8A47556235B
SHA1:	0397F404C9CA656C84454AF965A28AF1C20F25E9
SHA-256:	BAF596F1A49B72E9782836915994A5E41D78971E4BAD44B9BF5DB325310508A8
SHA-512:	676664B31C14A6E50B7A79666F4C8690C5669077D817B99D2241873C80745D0511ACF8078DD493F8252788C3E5460804C31464F610C396E112AB45F2805ED00A
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.145 131c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:41:21.150 131c Recovering log #3.2021/08/26-07:41:21.157 131c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.204282770097242
Encrypted:	false
SSDEEP:	6:mY6twDM+q2PWXp+N23iKKdK8a2jMGIFUtpp6V6gZmwPp60SDMVkwOWXp+N23iKKV:56tN+va5Kk8EFUtpp6V/Pp603V5f5Kkw
MD5:	59FBB8B518F30AD3D8B4B8A47556235B
SHA1:	0397F404C9CA656C84454AF965A28AF1C20F25E9
SHA-256:	BAF596F1A49B72E9782836915994A5E41D78971E4BAD44B9BF5DB325310508A8
SHA-512:	676664B31C14A6E50B7A79666F4C8690C5669077D817B99D2241873C80745D0511ACF8078DD493F8252788C3E5460804C31464F610C396E112AB45F2805ED00A
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.145 131c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:41:21.150 131c Recovering log #3.2021/08/26-07:41:21.157 131c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateRl (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

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):	5.284246659174082
Encrypted:	false
SSDEEP:	6:mY6up+q2PWXp+N23iKKdKgXz4rRIFUtpp6XZmwPp6IIGVkwOWXp+N23iKKdKgXzW:56dva5KkgXiuFUtpp6X/Pp6IX5f5Kkgi
MD5:	53753949056AAEF3383B4ACF78601D23
SHA1:	6F387A66CD3B78F155530B6FB304C4D0E579DFC1
SHA-256:	CEBBEB2762E3F3515C90AF73D2CEEC3016A16E8C67B34864FC57295BDEC9F472
SHA-512:	94B30C35D04183A931DB93F8B3A6B2D92A8ABFB82B4881D0C3E85E4506451E8B317DEAB1DDACC8E3F57FB6839D34803611AF521AC0D6FC45F0E3ED75F6B50B4
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.494 1438 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/26-07:41:21.495 1438 Recovering log #3.2021/08/26-07:41:21.496 1438 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.oldnt (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.284246659174082
Encrypted:	false
SSDEEP:	6:mY6up+q2PWXp+N23iKKdKgXz4rRIFUtpp6XZmwPp6IIGVkwOWXp+N23iKKdKgXzW:56dva5KkgXiuFUtpp6X/Pp6IX5f5Kkgi
MD5:	53753949056AAEF3383B4ACF78601D23

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.oldnt (copy)	
SHA1:	6F387A66CD3B78F155530B6FB304C4D0E579DFC1
SHA-256:	CEBBEB2762E3F3515C90AF73D2CEEC3016A16E8C67B34864FC57295BDEC9F472
SHA-512:	94B30C35D04183A931DB93F8B3A6B2D92A8ABFB82B4881D0C3E85E4506451E8B317DEAB1DDACC8E3F57FB6839D34803611AF521AC0D6FC45F0E3ED75F6B50B4
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.494 1438 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/26-07:41:21.495 1438 Recovering log #3.2021/08/26-07:41:21.496 1438 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5461
Entropy (8bit):	5.171766067123608
Encrypted:	false
SSDEEP:	96:nxCLP79So7Bt7jcKIoPok0JCKL8VbOTQVuwn:nxCX9TBt7jc6K4K6
MD5:	CEFC249F4104AC3B579491073AD07D44
SHA1:	4DD38DD6B92C61DB67B12EA26D34F5A557568018
SHA-256:	A1AB4A3D6D44BCCD444CFBA1E6D4760C781FF18F53A4F9F5079C5658586E1D5C
SHA-512:	E315DB2635FD6FAC6C5A973AAF6B317F5C1D2CDFA7A47B309842B0B940E2AF6DEA7B9C1DE827139E7BAB6D2B0D9AAFCDABFDF6B4E25B40E8385A834D6DF8572A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13274462481429237","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22594
Entropy (8bit):	5.535888625396798
Encrypted:	false
SSDEEP:	384:5kntgLllEX51kXqKf/pUZNCgVLH2HfDTrU1HGunT+ngqYW4Q:nLlg51kXqKf/pUZNCgVLH2HfvrUJGung
MD5:	9BCCF9C645A550970B280AEBFAF48CE6
SHA1:	5425EA812A012B1FA48EA8DE34F5D7AF19E21D09
SHA-256:	1066CBEA3741ED11B3CBB97E88CADC76127C848961C932CE39FD7026C6765A02
SHA-512:	E6D16B4D8D027879275BE1C6F6BB9964538A7674397A6E44163B35B17C5DE78F61220188BC74FC3998D7C2E76929583AC3A6073598CCE50440FF64511CC231BF
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":"13274462481134628","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Malicious:	false
Reputation:	low
Preview:	..&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):	5.187978509889844
Encrypted:	false
SSDEEP:	6:mY6xyq2PWXp+N23iKKdKrQMxIFUtpp6n11ZmwPp6njRkwOWXp+N23iKKdKrQMFLJ:56Uva5KkCFUtpp6n11/Pp6nF5f5KktJ
MD5:	7C310BA2B1ADD7B5BD47C7BAC6605D29
SHA1:	D4692EAEB8F126DF9AE3F4A56BCD7EF8695292CF
SHA-256:	4B9126F233B8A46798C37A30D965A22D87A6C41EC05E1A906A2754E5200E6878
SHA-512:	729E74185C73D8989BBEF0B3B51C06D4D87945236FEB8856B57731CFCB6F8E27F8A6A694E3ECA505B54E893E74EFCD3424843F1ADDECC346C344CA8694CD78B
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.413 1430 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/26-07:41:21.415 1430 Recovering log #3.2021/08/26-07:41:21.415 1430 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old=M (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.187978509889844
Encrypted:	false
SSDEEP:	6:mY6xyq2PWXp+N23iKKdKrQMxIFUtpp6n11ZmwPp6njRkwOWXp+N23iKKdKrQMFLJ:56Uva5KkCFUtpp6n11/Pp6nF5f5KktJ
MD5:	7C310BA2B1ADD7B5BD47C7BAC6605D29
SHA1:	D4692EAEB8F126DF9AE3F4A56BCD7EF8695292CF
SHA-256:	4B9126F233B8A46798C37A30D965A22D87A6C41EC05E1A906A2754E5200E6878
SHA-512:	729E74185C73D8989BBEF0B3B51C06D4D87945236FEB8856B57731CFCB6F8E27F8A6A694E3ECA505B54E893E74EFCD3424843F1ADDECC346C344CA8694CD78B
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.413 1430 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/26-07:41:21.415 1430 Recovering log #3.2021/08/26-07:41:21.415 1430 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):	5.169524024527111
Encrypted:	false
SSDEEP:	6:mY6EAq2PWXp+N23iKKdK7Uh2ghZIFUtpp6mhZmwPp6PkwOWXp+N23iKKdK7Uh2gd:56EAva5KklhHh2FUtpp6mh/Pp6P5f5KF
MD5:	603C9B6289B69D95F5FF797C8125B31C
SHA1:	CED1250D0795358E145BC7CC718AFB3A7E1600FD
SHA-256:	38CE57221993DEFC55328673C942160DB18CFE98404C379E479FDCB60C31E776
SHA-512:	049A06895468D360F4515D1A57EEF69ECF5441F7460A46D9DC945316BA342AC1FD66C56843D25B3F19D9F255E3E9B8486101A8C8C74559DF45DE266D36022870
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.132 14f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/26-07:41:21.138 14f0 Recovering log #3.2021/08/26-07:41:21.140 14f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Size (bytes):	348
Entropy (8bit):	5.169524024527111
Encrypted:	false
SSDEEP:	6:mY6EAq2PWXp+N23iKKdK7Uh2ghZIFUtpp6mhZmwPp6PkwOWXp+N23iKKdK7Uh2gd:56EAva5KklhHh2FUtpp6mh/Pp6P5f5KF
MD5:	603C9B6289B69D95F5FF797C8125B31C
SHA1:	CED1250D0795358E145BC7CC718AFB3A7E1600FD
SHA-256:	38CE57221993DEFC55328673C942160DB18CFE98404C379E479FDCB60C31E776
SHA-512:	049A06895468D360F4515D1A57EEF69ECF5441F7460A46D9DC945316BA342AC1FD66C56843D25B3F19D9F255E3E9B8486101A8C8C74559DF45DE266D36022870
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.132 14f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/26-07:41:21.138 14f0 Recovering log #3.2021/08/26-07:41:21.140 14f0 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\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.269543552012892
Encrypted:	false
SSDEEP:	12:56uva5KkFFUtpp63Is1/Pp63Ie5f5KkOJ:56sa5Kkfgf636Bf5KkK
MD5:	E3ED92D89E6673A07E8ED122AB3E3127
SHA1:	1B55EBFC19348962D57DB1BE10DD6B4E75AFC831
SHA-256:	B8D6FA6EA6BCD79655192B296A34B9C88E6147AAD55437165C3969B049E0B864
SHA-512:	FED7228619400EFACD9DAB34EACE59D98030CA1109BD398491B232A21F89CB424DF52787EC09A5F20C71C8916B485E0AEEE5FE415BA6F3536804B02EA50231AB
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.446 1430 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:41:21.448 1430 Recovering log #3.2021/08/26-07:41:21.448 1430 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\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.269543552012892
Encrypted:	false
SSDEEP:	12:56uva5KkFFUtpp63Is1/Pp63Ie5f5KkOJ:56sa5Kkfgf636Bf5KkK
MD5:	E3ED92D89E6673A07E8ED122AB3E3127
SHA1:	1B55EBFC19348962D57DB1BE10DD6B4E75AFC831
SHA-256:	B8D6FA6EA6BCD79655192B296A34B9C88E6147AAD55437165C3969B049E0B864
SHA-512:	FED7228619400EFACD9DAB34EACE59D98030CA1109BD398491B232A21F89CB424DF52787EC09A5F20C71C8916B485E0AEEE5FE415BA6F3536804B02EA50231AB
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.446 1430 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:41:21.448 1430 Recovering log #3.2021/08/26-07:41:21.448 1430 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\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.341461917462129
Encrypted:	false
SSDEEP:	12:56Qva5KkmiuFUtpp6x1/Pp6Ir5f5Kkm2J:56ia5KkSgf6xf60f5Kkr
MD5:	483D435699C81B8151F6A15039EB36E6
SHA1:	4E9750DF79674013EB4C4145E218F32E79089F36
SHA-256:	34F8D9C1896564D499194C271C27470BC05971C715AC8237B9FF4EFD10B05835
SHA-512:	9D21A9F12DFF602E56729F0C2DE82BCD4C02C811AB0E95B4EDFD5E7F574F18D3F41D483AA776715244F1C827834C23F41A891D5A6BF08EC31C94C27EF370F0E
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.493 1478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/26-07:41:21.495 1478 Recovering log #3.2021/08/26-07:41:21.496 1478 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.341461917462129
Encrypted:	false
SSDEEP:	12:56Qva5KkmiuFUtpp6x1/Pp6Ir5f5Kkm2J:56ia5KkSgf6xf60f5Kkr
MD5:	483D435699C81B8151F6A15039EB36E6
SHA1:	4E9750DF79674013EB4C4145E218F32E79089F36
SHA-256:	34F8D9C1896564D499194C271C27470BC05971C715AC8237B9FF4EFD10B05835
SHA-512:	9D21A9F12DFF602E56729F0C2DE82BCD4C02C811AB0E95B4EDFD5E7F574F18D3F41D483AA776715244F1C827834C23F41A891D5A6BF08EC31C94C27EF370F0E
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.493 1478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/26-07:41:21.495 1478 Recovering log #3.2021/08/26-07:41:21.496 1478 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\c97a104f-7566-4bec-a021-7fbb5efdf72b.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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.2467132997124315
Encrypted:	false
SSDEEP:	12:5V2va5KkkGHArBFUtppVn1/PpVmST5f5KkkGHAryJ:5Oa5KkkGgPgfxfI8f5KkkGga
MD5:	13DFDC959F4E0D57F3C065022710EFED
SHA1:	5415CAD81D31F0A254BF6D7FB78350E2EEC6B07E
SHA-256:	2D34802644A50F8C83DF40E7495E112E9B88E51263507DB2751DAFDB47CD0C9B
SHA-512:	AB78B339F94E4A00F42B0F5366C2562312C260CB701E373B357DDA48C1D1E67C970808EC2D3535C485EE6D82A36270FF094B16F86BD156DCAF6F5B5F34DFB7E
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:28.459 1478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:41:28.462 1478 Recovering log #3.2021/08/26-07:41:28.464 1478 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.olds. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.2467132997124315
Encrypted:	false
SSDEEP:	12:5V2va5KkkGHArBFUtppVn1/PpVmST5f5KkkGHAryJ:5Oa5KkkGgPgfxfI8f5KkkGga
MD5:	13DFDC959F4E0D57F3C065022710EFED
SHA1:	5415CAD81D31F0A254BF6D7FB78350E2EEC6B07E
SHA-256:	2D34802644A50F8C83DF40E7495E112E9B88E51263507DB2751DAFDB47CD0C9B
SHA-512:	AB78B339F94E4A00F42B0F5366C2562312C260CB701E373B357DDA48C1D1E67C970808EC2D3535C485EE6D82A36270FF094B16F86BD156DCAF6F5B5F34DFB7E
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:28.459 1478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:41:28.462 1478 Recovering log #3.2021/08/26-07:41:28.464 1478 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):	5.259042424515017
Encrypted:	false
SSDEEP:	12:5VVyva5KkkGHArqiuFUtppVI/PpVmwR5f5KkkGHArq2J:5Ua5KkkGgCgfaIyf5KkkGg7
MD5:	CDD406F7616811638C71A12B4A2F0432
SHA1:	31786AB9DCDDDBA3E01E2FF40F40D0AB232C8D7F
SHA-256:	026E47609A66122476515C168DB2070ECE894D779D8C52D48E9D9A618110A300
SHA-512:	8F36495C9631BAD759283EE59BC3845665A2F060F3946F75FD33ECF9BECCADFEF5BC05C0EF426BB55B5ADDA843CFB45CFADF59759C0753AC52D24B36DFA97F 9F
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:28.460 1454 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/26-07:41:28.463 1454 Recovering log #3.2021/08/26-07:41:28.464 1454 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.259042424515017
Encrypted:	false
SSDEEP:	12:5VVyva5KkkGHArqiuFUtppVI/PpVmwR5f5KkkGHArq2J:5Ua5KkkGgCgfaIyf5KkkGg7
MD5:	CDD406F7616811638C71A12B4A2F0432
SHA1:	31786AB9DCDDDBA3E01E2FF40F40D0AB232C8D7F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
SHA-256:	026E47609A66122476515C168DB2070ECE894D779D8C52D48E9D9A618110A300
SHA-512:	8F36495C9631BAD759283EE59BC3845665A2F060F3946F75FD33ECF9BECCADFEF5BC05C0EF426BB55B5ADDA843CFB45CFADF59759C0753AC52D24B36DFA97 9F
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:28.460 1454 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/26-07:41:28.463 1454 Recovering log #3.2021/08/26-07:41:28.464 1454 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\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.227067630552924
Encrypted:	false
SSDEEP:	6:mY6fq2PWXp+N23iKKdKpIFUtpp6pzZZmwPp6dmPkwOWXp+N23iKKdKa/WLJ:56fva5KkmFUtpp6pN/Pp6Y5f5KkaUJ
MD5:	5A9C4EE0426D53188BB8C046EEC35E89
SHA1:	868EDD18EEB89FD4CD72374712A89AE0D89499FB
SHA-256:	7AB46EF84161014555ACB3F49AC972DD03B0940D316FA77FEEB133F1F1900295
SHA-512:	19ADB0007D7CC44B88AD5BDD2D64159173D6145258E10C6F32EE8F571C8F56F8E91FBEFA0D5DA7BBE25DFDB15D108B75118E8337A3070D1376DA1219FF3083
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.137 1704 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/26- 07:41:21.141 1704 Recovering log #3.2021/08/26-07:41:21.144 1704 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/ 000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.227067630552924
Encrypted:	false
SSDEEP:	6:mY6fq2PWXp+N23iKKdKpIFUtpp6pzZZmwPp6dmPkwOWXp+N23iKKdKa/WLJ:56fva5KkmFUtpp6pN/Pp6Y5f5KkaUJ
MD5:	5A9C4EE0426D53188BB8C046EEC35E89
SHA1:	868EDD18EEB89FD4CD72374712A89AE0D89499FB
SHA-256:	7AB46EF84161014555ACB3F49AC972DD03B0940D316FA77FEEB133F1F1900295
SHA-512:	19ADB0007D7CC44B88AD5BDD2D64159173D6145258E10C6F32EE8F571C8F56F8E91FBEFA0D5DA7BBE25DFDB15D108B75118E8337A3070D1376DA1219FF3083
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:21.137 1704 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/26- 07:41:21.141 1704 Recovering log #3.2021/08/26-07:41:21.144 1704 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):	5.36452543739855
Encrypted:	false
SSDEEP:	12:5SYva5KkkOrsFUtppSs/PpSM5f5KkkOrzJ:5Sqa5Kk+gfSkSWf5Kkn
MD5:	A58AADAF4B02511F4C49603124B635B8
SHA1:	F2CBE1A30E8C6D6C9ED09CEBD37731E23B508EAA
SHA-256:	A5199C72B9B196D1A9C2EBD1E99ACE267138A7326C3CFEDBAC5D904C43B841F6
SHA-512:	FA9E81227A32F62D4913333959D274F9CB82B30D68B863D55D3E415351E033BC9AD32937AA6F612CB59F543E06BFAC1856C18FF7614EF899CA6848D1FB088312
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:29.417 1474 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/26-07:41:29.418 1474 Recovering log #3.2021/08/26-07:41:29.418 1474 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.oldt (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.36452543739855
Encrypted:	false
SSDEEP:	12:5SYva5KkkOrsFUtppSs/PpSM5f5KkkOrzJ:5Sqa5Kk+gfSkSWf5Kkn
MD5:	A58AADAF4B02511F4C49603124B635B8
SHA1:	F2CBE1A30E8C6D6C9ED09CEBD37731E23B508EAA
SHA-256:	A5199C72B9B196D1A9C2EBD1E99ACE267138A7326C3CFEDBAC5D904C43B841F6
SHA-512:	FA9E81227A32F62D4913333959D274F9CB82B30D68B863D55D3E415351E033BC9AD32937AA6F612CB59F543E06BFAC1856C18FF7614EF899CA6848D1FB088312
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:29.417 1474 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/26-07:41:29.418 1474 Recovering log #3.2021/08/26-07:41:29.418 1474 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.567823319207455
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvq7wUlbRUenHQ:YI6UUhVseKUewqPeUer2Uef0wUllUenw
MD5:	A8FED1D97B7DA9EEB08DDB16447645E5
SHA1:	13EF38D20C1E4CD8591D6C964E65BB5F24C0C808
SHA-256:	5048CD2BAD288A703FB82B9D40F67EF30B6BB4412AF9E2F184DC3E4BD738152D
SHA-512:	87A666A1FA2E642C641C1EB75D553CE881CAEEC09EF642E756C03CA1FF651B70E8E6286BBDD8746E55BDC68F97278B55A19D1BAE32223315D233A2A59217F4A1
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1661524886.613034,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629988886.613038},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b8582f10-15bc-4af1-a5ef-8f3441619614.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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b8582f10-15bc-4af1-a5ef-8f3441619614.tmp	
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT69 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.5475572333867165
Encrypted:	false
SSDEEP:	3:tUK6WaLku0gZmwv3lWaLRFojV8sIWaLSZBmWGv:mYAV0gZmwPpARFsVvpA6Bmtv
MD5:	117121331C9FD83CB02EE5F6DCD06D69
SHA1:	388D0F529BC66B76A7161EC7AF342809128AAE8E
SHA-256:	B23D86644A322C797ADC8DB48B60755E732F2A79BFD5CE226D3A9D3266FC4B0C
SHA-512:	3668214E09036C6E42C3DF34D6211A7C522D46CFAD5DD6D56FF8197EF77448554191563B1412C77F4643DD60D519FC5A5BE75866DEC8A24D231C243A5E6336AI
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.706 13dc Recovering log #3.2021/08/26-07:41:27.761 13dc Delete type=0 #3.2021/08/26-07:41:27.762 13dc Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.oldt (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.5475572333867165
Encrypted:	false
SSDEEP:	3:tUK6WaLku0gZmwv3IWaLRFojV8sIWaLSZBmWGv:mYAV0gZmwPpARFsVvpA6Bmtv
MD5:	117121331C9FD83CB02EE5F6DCD06D69
SHA1:	388D0F529BC66B76A7161EC7AF342809128AAE8E
SHA-256:	B23D86644A322C797ADC8DB48B60755E732F2A79BFD5CE226D3A9D3266FC4B0C
SHA-512:	3668214E09036C6E42C3DF34D6211A7C522D46CFAD5DD6D56FF8197EF77448554191563B1412C77F4643DD60D519FC5A5BE75866DEC8A24D231C243A5E6336A
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.706 13dc Recovering log #3.2021/08/26-07:41:27.761 13dc Delete type=0 #3.2021/08/26-07:41:27.762 13dc Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V........leveldb.BytewiseComparator...#...........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fd6261c6-de22-45ca-8171-f47aa763e05b.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):	5461
Entropy (8bit):	5.171766067123608
Encrypted:	false
SSDEEP:	96:nxCLP79So7Bt7jcKIoPok0JCKL8VbOTQVuwn:nxCX9TBt7jc6K4K6
MD5:	CEFC249F4104AC3B579491073AD07D44
SHA1:	4DD38DD6B92C61DB67B12EA26D34F5A557568018
SHA-256:	A1AB4A3D6D44BCCD444CFBA1E6D4760C781FF18F53A4F9F5079C5658586E1D5C
SHA-512:	E315DB2635FD6FAC6C5A973AAF6B317F5C1D2CDFA7A47B309842B0B940E2AF6DEA7B9C1DE827139E7BAB6D2B0D9AAFCDABFDF6B4E25B40E8385A834D6DF8 572A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13274462481429237","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"co untryid_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","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.2871322191023955
Encrypted:	false
SSDEEP:	6:mYAO3+q2PWXp+N23iKKdKfrzAdIFUtppAlqZmwPpAUVkwOWXp+N23iKKdKfrzILJ:5kva5Kk9FUtpp6q/Ppp5f5Kk2J
MD5:	C031893C9FA84A2A1293AC406D988948
SHA1:	65034A4BFEF697B52172CFA538CEDB1D3E9DC539

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
SHA-256:	8FEC76D254B02FEAC7DC845790622D8BFEB173C950A701208879EE9FBB994BF1
SHA-512:	76AEE67945760C78814D4716800DF6F6407C8E135607469864B0837BAB8FC1CF196B07A70BA51857D1F4BC0C351DF892121FF9975663EBA5B9B92EB58752F02D
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.957 1438 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/08/26-07:41:27.959 1438 Recovering log #3.2021/08/26-07:41:27.960 1438 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.oldl (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.2871322191023955
Encrypted:	false
SSDEEP:	6:mYAO3+q2PWXp+N23iKKdKfrzAdIFUtppAlqZmwPpAUVkwOWXp+N23iKKdKfrzILJ:5kva5Kk9FUtpp6q/Ppp5f5Kk2J
MD5:	C031893C9FA84A2A1293AC406D988948
SHA1:	65034A4BFEF697B52172CFA538CEDB1D3E9DC539
SHA-256:	8FEC76D254B02FEAC7DC845790622D8BFEB173C950A701208879EE9FBB994BF1
SHA-512:	76AEE67945760C78814D4716800DF6F6407C8E135607469864B0837BAB8FC1CF196B07A70BA51857D1F4BC0C351DF892121FF9975663EBA5B9B92EB58752F02D
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:41:27.957 1438 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/08/26-07:41:27.959 1438 Recovering log #3.2021/08/26-07:41:27.960 1438 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
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\Local StateTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateTM (copy)	
Size (bytes):	178080
Entropy (8bit):	6.078843623541878
Encrypted:	false
SSDEEP:	3072:P5nmm8A1PCyn3BOIrdvrVslFcbXafIB0u1GOJmA3iuRt:xnP8oPjxwaqfllUOoSiuRt
MD5:	F92F578764DC1A39BFE2AE07C6655CB5
SHA1:	423CD39C0113441F1ADB5703882C76C9033E2CDF
SHA-256:	F477974FA981BE8521C93D45D5D6ED129AE3E233E90F32C62BE5514BB411184D
SHA-512:	C8C655AEE62EF96F70A00475B15C252B272490976415626D28706621822852345451ADD07C7FFA901CCF8F073D4A9643E76A5988A1B0F78024FC3AAD6F8DADEAE
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.629988884569137e+12,"network":1.629956486e+12,"ticks":6842890079.0,"uncertainty":5036518.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Temp\16259f46-e1b7-4fc9-a34a-724aa2e46fc8.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
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\a53f7a9d-c55c-4149-9be2-b9a4dfd653ca.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
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):	5446
Entropy (8bit):	4.643287567952941
Encrypted:	false
SSDEEP:	96:2UlO5epENZtaIA5mtSYvuy4kCWDlH9hqSrjAiNdN0C5XpKC5:/4tvokCQJpn5v
MD5:	C2B7C38293EC3A59E309F51FCC4CA08C
SHA1:	6874601FCFB152ED144E30126B134D0BF643AE33

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
SHA-256:	6238163485A3910D8865730C7436D0681B11AD8E1745EAAD63551065E8B8D0BA
SHA-512:	570B65A07F3D2594813B73FC4E7EFDC667058714315715D371370AE4A9238F3B41AFB70F1E108F5375BA44E04E6EDA32DA70CA106E1E92CAC05BB1C72B71E773
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET d84a5ed9e281cad4bc9414e1b3b3ec4da6da0d66a18c81cdbfab677895ce6817 7714d7fd77e24f2a1901524b35f524e44 612e07a3887b68f5ab9167c825e2523.SERVER_HANDSHAKE_TRAFFIC_SECRET d84a5ed9e281cad4bc9414e1b3b3ec4da6da0d66a18c81cdbfab677895ce6817 d cf884f49c4cd3542b02be17cc036316a1f22b194aebacb128bcc756912da4df.CLIENT_HANDSHAKE_TRAFFIC_SECRET 7e218c5027f517fd0bb8c8570de0d22eef cf9301c4bfe05b13e55abd1b420973 ab8e81d6fba65e0c95378a420c43a5089f292316a03bbdd3ce0db44cf054ee50.SERVER_HANDSHAKE_TRAFFIC_SECRET 7e 218c5027f517fd0bb8c8570de0d22eefcf9301c4bfe05b13e55abd1b420973 1b01f0a13528666d363ba22af635e90dce3365158e92e7ac82edf333b5d98dd6.CLIENT_HANDS HAKE_TRAFFIC_SECRET 515dfbb4a9384fd5175178ab892f0ed62ee9c98353d1a36240e44a02945dd5f6 7dc80ab2493c9d3c310022682b3ff317310f842de8bc7 44578fed56f648308a3.SERVER_HANDSHAKE_TRAFFIC_SECRET 515dfbb4a9384fd5175178ab892f0ed62ee9c98353d1a36240e44a02945dd5f6 43d3884bb2a6c cad993e9adfb10fe87b654e7bfb20f3ccb32f634a575c4b8748.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\c0b5d918-5298-487e-9c6d-8ab323979e6b.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\d6e23a16-077f-49e3-8f66-547a77fda079.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./ ?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\16259f46-e1b7-4fc9-a34a-724aa2e46fc8.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\16259f46-e1b7-4fc9-a34a-724aa2e46fc8.tmp	
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\scoped_dir852_1122722386\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMICTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ...."..".. },.. "craw_connect_to_network": {.. "message": "..... .. .."..".. },.. "iap_unavailable": {.. "message": ".. ...."..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\en\messages.json	
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\es_419\messages.json	
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEA D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA7555
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... ."... },.. "app_name": {.. "message": "Chrome ... ."... },.. "craw_app_unavailable": {.. "messa ge": "..... .. .."... },.. "craw_connect_to_network": {.. "message": "..... ...."... },.. "iap_unavailable": {.. "message": "..-.. ...."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... ."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D03 6E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\hu\messages.json	
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\ja\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome .....".. },.. "app_name": {.. "message": "Chrome .....".. },.. "craw_app_unavailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": ".....".. },.. "iap_unavailable": {.. "message": ".....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome .....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir852_1122722386\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome . ... ..".. },.. "app_name": {.. "message": "Chrome . ... ..".. },.. "craw_app_unavailable": {.. "message": ".. .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .....".. },.. "iap_unavailable": {.. "message": ".. .. ..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome. .....".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 26, 2021 07:41:26.616682053 CEST	192.168.2.3	8.8.8.8	0x9e3e	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:41:26.625891924 CEST	192.168.2.3	8.8.8.8	0x5de4	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:41:26.626255035 CEST	192.168.2.3	8.8.8.8	0xcfbf	Standard query (0)	clapham.allow.me	A (IP address)	IN (0x0001)
Aug 26, 2021 07:41:28.393798113 CEST	192.168.2.3	8.8.8.8	0x4fee	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
Aug 26, 2021 07:41:26.642398119 CEST	8.8.8.8	192.168.2.3	0x9e3e	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:41:26.642398119 CEST	8.8.8.8	192.168.2.3	0x9e3e	No error (0)	clients.l.google.com		142.250.184.206	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 26, 2021 07:41:26.665771961 CEST	8.8.8.8	192.168.2.3	0x5de4	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Aug 26, 2021 07:41:26.806385040 CEST	8.8.8.8	192.168.2.3	0xcfbf	No error (0)	clapham.allow.me		52.56.219.240	A (IP address)	IN (0x0001)
Aug 26, 2021 07:41:28.434216976 CEST	8.8.8.8	192.168.2.3	0x4fee	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:41:28.434216976 CEST	8.8.8.8	192.168.2.3	0x4fee	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
Aug 26, 2021 07:41:26.873087883 CEST	52.56.219.240	443	192.168.2.3	49709	CN=*.allow.me, OU=Domain Control Validated CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Jan 26 11:47:32 CET 2021 Tue May 03 09:00:00 CEST 2011 Tue Sep 01 02:00:00 CEST 2009	Wed Feb 09 17:54:09 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri Jan 01 00:59:59 CET 2038	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=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Sep 01 02:00:00 CEST 2009	Fri Jan 01 00:59:59 CET 2038		
Aug 26, 2021 07:41:26.876842976 CEST	52.56.219.240	443	192.168.2.3	49710	CN=*.allow.me, OU=Domain Control Validated CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Jan 26 11:47:32 CET 2021 Tue May 03 09:00:00 CEST 2011 Tue Sep 01 02:00:00 CEST 2009	Wed Feb 09 17:54:09 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri Jan 01 00:59:59 CET 2038	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=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Sep 01 02:00:00 CEST 2009	Fri Jan 01 00:59:59 CET 2038		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 852 Parent PID: 4824

General

Start time:	07:41:20
Start date:	26/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://clapham.allow.me/covid2021/?GOPPAGE61255999D1057&PID=3101'
Imagebase:	0x7ff77b960000
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

Analysis Process: chrome.exe PID: 5076 Parent PID: 852

General

Start time:	07:41:21
Start date:	26/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1548,783261014365729635,14637000979693343300,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1732 /prefetch:8
Imagebase:	0x7ff77b960000
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021