ID: 471913
Cookbook: browseurl.jbs
Time: 07:56:37
Date: 26/08/2021
Version: 33.0.0 White Diamond

Table of Contents

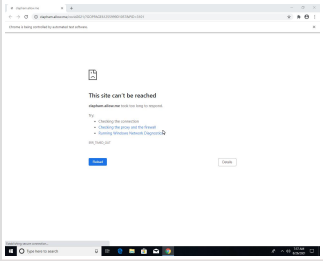
Windows Analysis Report https://clapham.allow.me/cov…

Overview

General Information

Sample URL:	http://https://clapham.allow.me/covid2021/?GOPPAGE61255999D1057&PID=3101
Analysis ID:	471913
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

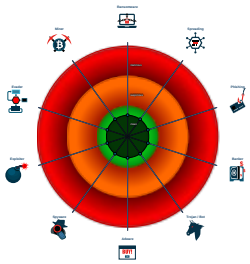
Detection

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: 5916 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: 2856 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1624,12626956359303723085,12777355795646735380,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1684 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

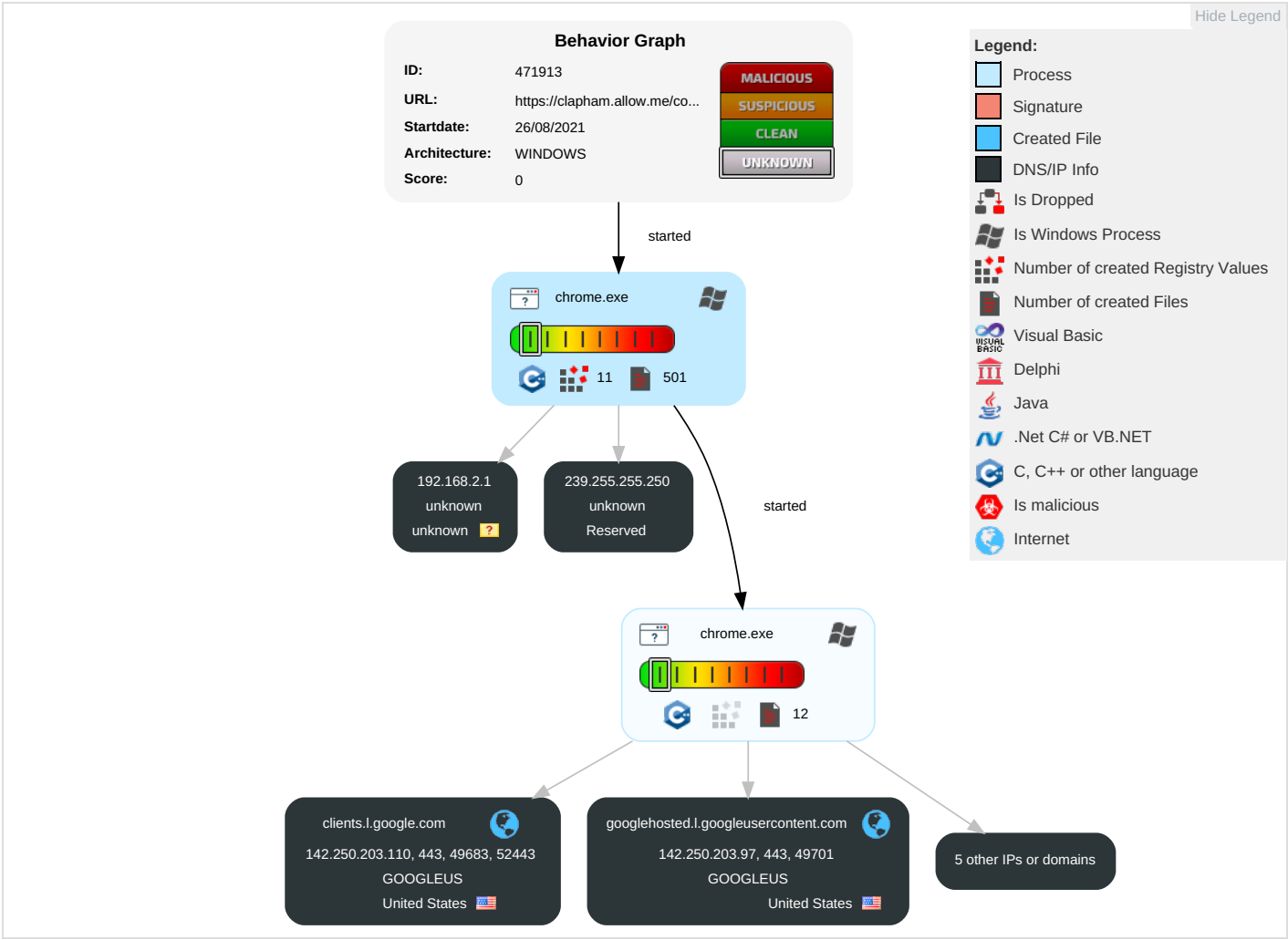
Click to jump to signature section

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

Mitre Att&ck Matrix

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

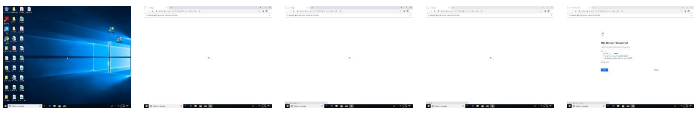
Behavior Graph

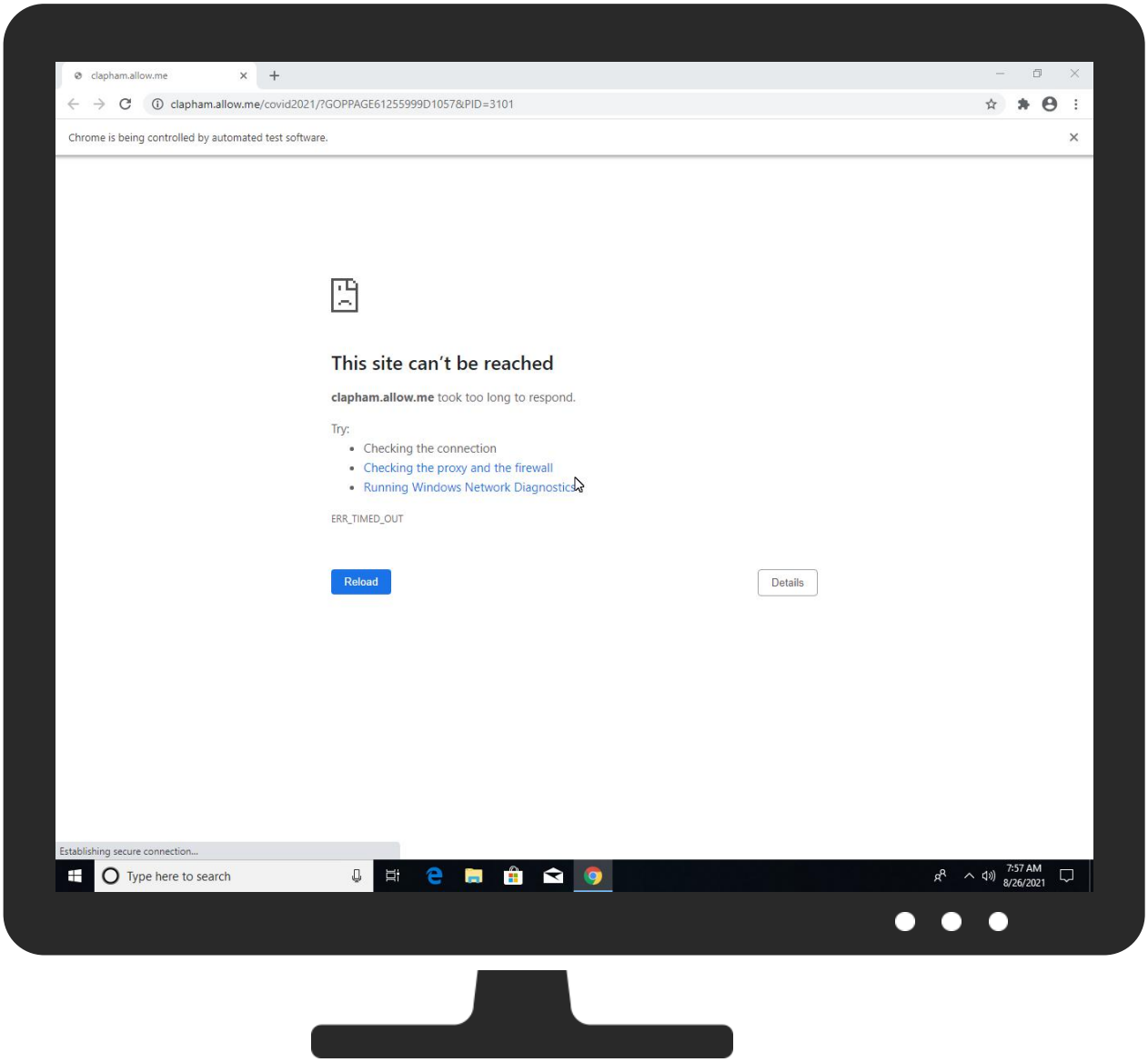


Screenshots

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	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
clapham.allow.me	52.56.219.240	true	false		unknown
clients.l.google.com	142.250.203.110	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
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
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

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	471913
Start date:	26.08.2021
Start time:	07:56:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 8s
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
Number of analysed new started processes analysed:	3
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@30/220@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
07:57:36	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.133376811589353
Encrypted:	false
SSDEEP:	6:kK4wSdoW+N+SkQlPlEGYRMY9z+4KlDA3RUellD1Ut:g/5kPlE99SNxAhUe0et
MD5:	86C4E6F02CAF9DF543C7905322CA6CE1
SHA1:	92D59011079B3400DBDD176048CDD75A3D5A223C
SHA-256:	9962495A9B6F09167DD47398CA55869BDCE51F80B08EB278FEE8F761A76A4025
SHA-512:	48AD6CF90571E94E321C1DF7E770FB7D27AE3D4959A2C0E1C3B266C56ACDAB2B94197DBBAD4CB408E076777F2C43E9CD017C584A76BB6EE2768ABCBE8431F DA8
Malicious:	false
Reputation:	low
Preview:	p..... .....sB#.....(..... .....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\4f7eeedd-d7f6-4182-8aa5-16f03c76db91.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):	369033
Entropy (8bit):	6.015161835361297
Encrypted:	false
SSDEEP:	6144:vP8oPjxD8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:XRjxwxzurRDn9nfNxF4ijZVtilB0
MD5:	50B0F4936D143DC1BAE9FE58361BD7C9
SHA1:	E8DE1CBC6FDF23BE9732EC6101C02BC26D879391
SHA-256:	813197B0DF62785619A8FC8DEEFA403426A0C4AE00212461094075F8B5FCD065
SHA-512:	B88258675D406A3194566C0FE191C01A90301A9D5496AD95B4FC7458927AAA2AFC4612CDAD13C7941000B14A977D8EAA49BF8082B2F16619EC50FDCDEFE9851
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":1.629989854462247e+12,"network":1.629957456e+12,"ticks":3939768103.0,"uncertainty":4956536.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1Qfj oKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP0 5zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327446345007

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0969cd07-a4bc-455e-b755-935dcc78342f.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\5a8e199c-81a9-4936-b706-5f64db957534.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):	874
Entropy (8bit):	5.561713251441355
Encrypted:	false
SSDEEP:	12:YdDZ6Hk3O+UAnIvld06cY8rNgmh4r+UAnIEllWcNnYj+UAnIECm13R7N+UAnI3L0:YT6H0UhHPkG1KUe9aUeCwB7wUWRUeIQ
MD5:	A58DB42A13D916CB1BB0C2347F218AB9
SHA1:	2CF80A8F1EC054544D6B61C00BAFBEC7C5A5EE89
SHA-256:	A8BE81843C9C12F4C1CEE879FA7D00076DEB2260E988B6C19658D9EF648D93A9
SHA-512:	09D3464DACA7E5B43C46131F47224B0984A20CB7B3814CF49533ED75563B59738BCA9E3BAB062FA0EAB27AFBB17FA6C6F2947FCF0AF6B07B028D6C5AD145475F4
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1661525856.342144,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629989856.342148},{"expiry":1633013028.952627,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.95263}],"version":2}

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):	336
Entropy (8bit):	5.257206408439038
Encrypted:	false
SSDEEP:	6:mJyFIq2P923iKKdK9RXXTZIFUtpuBWMZZmwPuBWMzkwO923iKKdK9RXX5LJ:xFIv45Kk7XT2FUtpo/Pw5L5Kk7XVJ
MD5:	672E71CCA91F2ED4C1403EF5305768D0
SHA1:	6DF496E674FE2A1AA86B36F27C6CED352B9FDA64
SHA-256:	9C523E08E0181DFFEA97E6EC7C432C6D3AC2980CB3C92C98A7A238E640AE61A8
SHA-512:	3B05B6042CDA43CE8FA14E3308EEBDD5EE4D933B95C8181ABE2F09796344ED446C7F881566250C3CE2A05BCDB2323479BB59AB03B800C72AFDD48955BBD396B
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.943 1390 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/26-07:57:39.948 1390 Recovering log #3.2021/08/26-07:57:39.948 1390 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)

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):	336
Entropy (8bit):	5.257206408439038
Encrypted:	false
SSDEEP:	6:mJyFIq2P923iKKdK9RXXTZIFUtpuBWMZZmwPuBWMzkwO923iKKdK9RXX5LJ:xFIv45Kk7XT2FUtpo/Pw5L5Kk7XVJ
MD5:	672E71CCA91F2ED4C1403EF5305768D0
SHA1:	6DF496E674FE2A1AA86B36F27C6CED352B9FDA64
SHA-256:	9C523E08E0181DFFEA97E6EC7C432C6D3AC2980CB3C92C98A7A238E640AE61A8
SHA-512:	3B05B6042CDA43CE8FA14E3308EEBDD5EE4D933B95C8181ABE2F09796344ED446C7F881566250C3CE2A05BCDB2323479BB59AB03B800C72AFDD48955BBD396B
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.943 1390 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/26-07:57:39.948 1390 Recovering log #3.2021/08/26-07:57:39.948 1390 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.2379964046275305
Encrypted:	false
SSDEEP:	6:mJRcFIq2P923iKKdKyDZIFUtpuPdZmwPuUIkwO923iKKdKyJLJ:/v45Kk02FUtpOd/PnI5L5KkWJ
MD5:	E5A40899337407D09376E6903246DCF2
SHA1:	3B0C54F36C949E702F7FAB615A681F242A8E35FF
SHA-256:	28E251B34361E248511BF0EBB13875F53249829D93BA1E044190A06267F0229E
SHA-512:	C12A9ECE6851E57E71591D842FF39D6D211FCBDBC1AE983642B0494704FBCC87938F422C6916CCACF34BEFD1D4A976FCAB0074A9CF6C8D473765C0FB7DB08A
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.921 1390 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/26-07:57:39.924 1390 Recovering log #3.2021/08/26-07:57:39.926 1390 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):	320
Entropy (8bit):	5.2379964046275305
Encrypted:	false
SSDEEP:	6:mJRcFIq2P923iKKdKyDZIFUtpuPdZmwPuUIkwO923iKKdKyJLJ:/v45Kk02FUtpOd/PnI5L5KkWJ
MD5:	E5A40899337407D09376E6903246DCF2
SHA1:	3B0C54F36C949E702F7FAB615A681F242A8E35FF
SHA-256:	28E251B34361E248511BF0EBB13875F53249829D93BA1E044190A06267F0229E
SHA-512:	C12A9ECE6851E57E71591D842FF39D6D211FCBDBC1AE983642B0494704FBCC87938F422C6916CCACF34BEFD1D4A976FCAB0074A9CF6C8D473765C0FB7DB08A
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.921 1390 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/26-07:57:39.924 1390 Recovering log #3.2021/08/26-07:57:39.926 1390 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:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC761F
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):	0.9691711894502852
Encrypted:	false
SSDEEP:	24:WIL4rtEy8LbqLbJLbXaFpEO5bNmISHn06UwBM8:WI+Gbq5LLOpEO5J/Kn7U18
MD5:	002817FB958CF68AC05B2727545A483D
SHA1:	06D6A1B915F3CB21C4B9C7F3ACE5428AC2A571A0
SHA-256:	AEF6A0FBFEF45E8F9B87ABC61FA25A5E54C8FC730B8C757F4AE1EE7FD5A61DE4
SHA-512:	01147E67E166B0EF9EAAF1455525B198C9268EA5302B76461B335072E25C6B9491DC86220A0F35472F8CB3CA9CB1D62531F21C88AF02B9AAD20923C1728AC556
Malicious:	false
Reputation:	low
Preview:	.....0Su..... ....

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):	3.533767321817729
Encrypted:	false
SSDEEP:	24:34S4iTz2tlrlCJc00ylmVUwHlkehz+wCUwH5lL:34l4SXxec002yFkMqjbL
MD5:	34ECBEC1412151922CFA0D4CD0C18345
SHA1:	550542734C65BBA0EB433D6D38806E2C74730FF3
SHA-256:	E2F181B16623523B5F88E380B8B58376965662CE4D8E03E918129D60792EE46B
SHA-512:	D16ED704FC8157C5D00159596A0B4C224651112422B482C7F2FE581094A918BD773879D3011A9918A10EFDF8B74603D13E74E784092DBE65DD0C06A92D4E63DE
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...89af184e_6c0f_42bc_b0cd_efb43211e220.....c..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....A...https://clapham.allow.me/covid2021/?GOP PAGE61255999D1057&PID=3101.....h.....`.....m.f.w...n.f.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:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.214394609295067
Encrypted:	false
SSDEEP:	6:mJbNAQ+q2P923iKKdK8aPrqIFUtpuiEAgZmwPuiEAQVkwO923iKKdK8amLJ:G3+v45KkL3FUtp8/P8V5L5KkQJ
MD5:	9B279592109CF754D58B87A14DD945F7
SHA1:	5CC59488C4B43FF2CE942DE757C64880024DF056
SHA-256:	EDF917AFA3E3492C650D6BEA429E0FD09D0D80083D8DC19E601A5924BB49B5CB
SHA-512:	E846C77065D7354E6C78AF1E6520E6C9C805EC880F4C7D8BABFF7C18A673685133995591151E0D8112ECDFAA3FB0FA8489F3FBEC3D0936943373985A6E0C210
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.435 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/26-07:57:30.437 57c Recovering log #3.2021/08/26-07:57:30.437 57c 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):	319
Entropy (8bit):	5.214394609295067
Encrypted:	false
SSDEEP:	6:mJbNAQ+q2P923iKKdK8aPrqIFUtpuiEAgZmwPuiEAQVkwO923iKKdK8amLJ:G3+v45KkL3FUtp8/P8V5L5KkQJ
MD5:	9B279592109CF754D58B87A14DD945F7
SHA1:	5CC59488C4B43FF2CE942DE757C64880024DF056
SHA-256:	EDF917AFA3E3492C650D6BEA429E0FD09D0D80083D8DC19E601A5924BB49B5CB
SHA-512:	E846C77065D7354E6C78AF1E6520E6C9C805EC880F4C7D8BABFF7C18A673685133995591151E0D8112ECDFAA3FB0FA8489F3FBEC3D0936943373985A6E0C210
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.435 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/26-07:57:30.437 57c Recovering log #3.2021/08/26-07:57:30.437 57c 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.230011320709102
Encrypted:	false
SSDEEP:	6:mJNQ+q2P923iKKdK8NIFUtpuRwgZmwPu2AQVkwO923iKKdK8+eLJ:j+v45KkpFUtp2Z/PH9V5L5KkqJ
MD5:	03326E3A47033C69AB33A7B678CE1AFC
SHA1:	0362B215D6790427A1C22859B4F0516F425FC9EA
SHA-256:	D47DB24EE742EA7BC97BA434C1D18A471B8072BA551BE46E53AE80D7D671D3BF
SHA-512:	2330AC573CD65CD1A37F84E0FA6CB2A5760FB0819CF80D1BEC13267041D2704D34D0715B959BD4D97A0694411B8367260A5F346B1302EAE70861FA57B312D390
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:33.859 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/26-07 :57:33.861 57c Recovering log #3.2021/08/26-07:57:33.862 57c 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):	319
Entropy (8bit):	5.230011320709102
Encrypted:	false
SSDEEP:	6:mJNQ+q2P923iKKdK8NIFUtpuRwgZmwPu2AQVkwO923iKKdK8+eLJ:j+v45KkpFUtp2Z/PH9V5L5KkqJ
MD5:	03326E3A47033C69AB33A7B678CE1AFC
SHA1:	0362B215D6790427A1C22859B4F0516F425FC9EA
SHA-256:	D47DB24EE742EA7BC97BA434C1D18A471B8072BA551BE46E53AE80D7D671D3BF
SHA-512:	2330AC573CD65CD1A37F84E0FA6CB2A5760FB0819CF80D1BEC13267041D2704D34D0715B959BD4D97A0694411B8367260A5F346B1302EAE70861FA57B312D390
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:33.859 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/26-07 :57:33.861 57c Recovering log #3.2021/08/26-07:57:33.862 57c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
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+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","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):	374
Entropy (8bit):	5.279628214757501
Encrypted:	false
SSDEEP:	6:mJBIq2P923iKKdK25+Xqx8chI+IFUtpu6ZmwPuLkwO923iKKdK25+Xqx8ch+/WLJ:Nv45KkTXfchI3FUtpl/PS5L5KkTXfchn
MD5:	08824D61EAEEC1D4FA474AA25567AE22
SHA1:	77DEB3F33E7E21EDEC8F20CE7F0E570642757434
SHA-256:	69396EEFCFE4A4F306CEE2F003BDD0DDEEDB7F7A79E1F74D72D4471A3C6DB476
SHA-512:	E5D41BF4053025F4A74E46128E4E3DC41AB7D5E320F1763411BFA1BA92476F48E1E3C29BC6FF1109E8F8F0580D3996F31729C1E4A957629751CCC21C1E58587C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/08/26-07:57:39.878 1390 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/26-07:57:39.886 1390 Recovering log #3.2021/08/26-07:57:39.887 1390 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.279628214757501
Encrypted:	false
SSDEEP:	6:mJBIq2P923iKKdK25+Xqx8chI+IFUtpu6ZmwPuLkwO923iKKdK25+Xqx8ch+/WLJ:Nv45KkTXfchI3FUtpl/PS5L5KkTXfchn
MD5:	08824D61EAEEC1D4FA474AA25567AE22
SHA1:	77DEB3F33E7E21EDEC8F20CE7F0E570642757434
SHA-256:	69396EEFCFE4A4F306CEE2F003BDD0DDEEDB7F7A79E1F74D72D4471A3C6DB476
SHA-512:	E5D41BF4053025F4A74E46128E4E3DC41AB7D5E320F1763411BFA1BA92476F48E1E3C29BC6FF1109E8F8F0580D3996F31729C1E4A957629751CCC21C1E58587C
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.878 1390 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/26-07:57:39.886 1390 Recovering log #3.2021/08/26-07:57:39.887 1390 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):	360
Entropy (8bit):	5.250964145494529
Encrypted:	false
SSDEEP:	6:mJVFtq2P923iKKdK25+XuoIFUtpu/2ZmwPuJFkwO923iKKdK25+XuxWLJ:8tv45KkTXYFUtpC2/PW5L5KkTXHJ
MD5:	FA9E30D7CA5D7022DEF3024A264194D2
SHA1:	5855C585C845C502594170E97B029666651687FF
SHA-256:	C40EC27A1B84E99090072713DBECFD25B04BAF4C5204A61F979F30D98C3EB34F
SHA-512:	3D206DC5AD7EFF0D296A89A82DD100B29BEADE35D9134D85BC8FFAFB4484A2AEF614C708ED90DBCF736A97722F1EFC272C26DEB81F68C56053ECFF2AF467F0D
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.660 1390 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/26-07:57:39.684 1390 Recovering log #3.2021/08/26-07:57:39.685 1390 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):	360
Entropy (8bit):	5.250964145494529
Encrypted:	false
SSDEEP:	6:mJVFtq2P923iKKdK25+XuoIFUtpu/2ZmwPuJFkwO923iKKdK25+XuxWLJ:8tv45KkTXYFUtpC2/PW5L5KkTXHJ
MD5:	FA9E30D7CA5D7022DEF3024A264194D2
SHA1:	5855C585C845C502594170E97B029666651687FF
SHA-256:	C40EC27A1B84E99090072713DBECFD25B04BAF4C5204A61F979F30D98C3EB34F
SHA-512:	3D206DC5AD7EFF0D296A89A82DD100B29BEADE35D9134D85BC8FFAFB4484A2AEF614C708ED90DBCF736A97722F1EFC272C26DEB81F68C56053ECFF2AF467F0D
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.660 1390 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/26-07:57:39.684 1390 Recovering log #3.2021/08/26-07:57:39.685 1390 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Size (bytes):	332
Entropy (8bit):	5.249178825172282
Encrypted:	false
SSDEEP:	6:mJ5QiVOq2P923iKKdKWT5g1IdqIFUtpu5UZZmwPu5UzkwO923iKKdKWT5g1I3ULJ:jiVOv45Kkg5gSRFUtpF/PX5L5Kkg5gSu
MD5:	DCD19322DC02C6A904C92A156CED72C2
SHA1:	88E79BCCCB2BA820A803BDE9EA60C3CF269B0ADB
SHA-256:	6CE4AA92E10A8E2D6411C52F8101D0AD12E77A31B133A9C6EDE76F912663601F
SHA-512:	9B2C09D7711B6478147D0BD1DAB99AF06A3ECAAE9FFA9AB22E1C6B2876CDEBD9CCB92EB3226BA443C9B48E753E5880F009D6349848CCDBEE6A98BAE37F749 0D4
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.335 1390 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08 /26-07:57:39.338 1390 Recovering log #3.2021/08/26-07:57:39.338 1390 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.oldg (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.249178825172282
Encrypted:	false
SSDEEP:	6:mJ5QiVOq2P923iKKdKWT5g1IdqIFUtpu5UZZmwPu5UzkwO923iKKdKWT5g1I3ULJ:jiVOv45Kkg5gSRFUtpF/PX5L5Kkg5gSu
MD5:	DCD19322DC02C6A904C92A156CED72C2
SHA1:	88E79BCCCB2BA820A803BDE9EA60C3CF269B0ADB
SHA-256:	6CE4AA92E10A8E2D6411C52F8101D0AD12E77A31B133A9C6EDE76F912663601F
SHA-512:	9B2C09D7711B6478147D0BD1DAB99AF06A3ECAAE9FFA9AB22E1C6B2876CDEBD9CCB92EB3226BA443C9B48E753E5880F009D6349848CCDBEE6A98BAE37F749 0D4
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.335 1390 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08 /26-07:57:39.338 1390 Recovering log #3.2021/08/26-07:57:39.338 1390 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Sessionbp (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1093
Entropy (8bit):	3.533767321817729
Encrypted:	false
SSDEEP:	24:34S4iTz2tlrlCJc00ylmVUwHlkehz+wCUwH5lL:34l4SXxec002yFkMqjbL
MD5:	34ECBEC1412151922CFA0D4CD0C18345
SHA1:	550542734C65BBA0EB433D6D38806E2C74730FF3
SHA-256:	E2F181B16623523B5F88E380B8B58376965662CE4D8E03E918129D60792EE46B
SHA-512:	D16ED704FC8157C5D00159596A0B4C224651112422B482C7F2FE581094A918BD773879D3011A9918A10EFDF8B74603D13E74E784092DBE65DD0C06A92D4E63DE
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...89af184e_6c0f_42bc_b0cd_efb43211e220.....c..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....A...https://clapham.allow.me/covid2021/?GOP PAGE61255999D1057&PID=3101.....h.....`.....m.f.w...n.f.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 (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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabs (copy)	
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):	334
Entropy (8bit):	5.175834704648797
Encrypted:	false
SSDEEP:	6:mJZi+q2P923iKKdK8a2jMGIFUtpuZmkZmwPuZyFFNVkwO923iKKdK8a2jMmLJ:mv45Kk8EFUtp+/P5Fz5L5Kk8bJ
MD5:	368805576D40CDC8D3FB6E3A2DDD982F
SHA1:	EEA4AD55215633962EA784851E7B6DB081EFADA1
SHA-256:	BCF9B2F684F0A9F985CD858A9AD9C4146205E745794F5AC6D73B83C30A21B3EF
SHA-512:	61397EB7433230893B88B09C7BD29C184CB4B0CD3EBAC0BF0EE568E1887F71D431BFFBB2D15456E341C57FDADD6020AE9B8EB4DFF45777854707F62FD38DCF7
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.158 1328 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:57:30.166 1328 Recovering log #3.2021/08/26-07:57:30.170 1328 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.175834704648797
Encrypted:	false
SSDEEP:	6:mJZi+q2P923iKKdK8a2jMGIFUtpuZmkZmwPuZyFFNVkwO923iKKdK8a2jMmLJ:mv45Kk8EFUtp+/P5Fz5L5Kk8bJ
MD5:	368805576D40CDC8D3FB6E3A2DDD982F
SHA1:	EEA4AD55215633962EA784851E7B6DB081EFADA1
SHA-256:	BCF9B2F684F0A9F985CD858A9AD9C4146205E745794F5AC6D73B83C30A21B3EF
SHA-512:	61397EB7433230893B88B09C7BD29C184CB4B0CD3EBAC0BF0EE568E1887F71D431BFFBB2D15456E341C57FDADD6020AE9B8EB4DFF45777854707F62FD38DCF7
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.158 1328 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:57:30.166 1328 Recovering log #3.2021/08/26-07:57:30.170 1328 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 State43 (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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

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):	333
Entropy (8bit):	5.220772135188778
Encrypted:	false
SSDEEP:	6:mJ2aAQ+q2P923iKKdKgXz4rRIFUtpuC4gZmwPuCNAQVkwO923iKKdKgXz4q8LJ:K9+v45KkgXiuFUtprB/PvN9V5L5KkgXS
MD5:	23095E6BB5137E8D39AD0EDF4809E0DD
SHA1:	707CC3DBA401CED53625E759BEE3EC36DFC7C683
SHA-256:	15BCE37A73D4741AA1D280AF8624F99CD6C360E4942D91F315760101843A55BB
SHA-512:	B147D527E3D93DD5C5018955935CF43DC694AD45B531F703E3A9195746F617943249E7D57335057C7F66AF8E4C6BBEF3B7B2304D429FA4910EC55E8E34622F24
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.460 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/26-07:57:30.469 57c Recovering log #3.2021/08/26-07:57:30.470 57c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.220772135188778
Encrypted:	false
SSDEEP:	6:mJ2aAQ+q2P923iKKdKgXz4rRIFUtpuC4gZmwPuCNAQVkwO923iKKdKgXz4q8LJ:K9+v45KkgXiuFUtprB/PvN9V5L5KkgXS
MD5:	23095E6BB5137E8D39AD0EDF4809E0DD
SHA1:	707CC3DBA401CED53625E759BEE3EC36DFC7C683
SHA-256:	15BCE37A73D4741AA1D280AF8624F99CD6C360E4942D91F315760101843A55BB
SHA-512:	B147D527E3D93DD5C5018955935CF43DC694AD45B531F703E3A9195746F617943249E7D57335057C7F66AF8E4C6BBEF3B7B2304D429FA4910EC55E8E34622F24
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.460 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/26-07:57:30.469 57c Recovering log #3.2021/08/26-07:57:30.470 57c 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):	4785
Entropy (8bit):	4.936317417564759
Encrypted:	false
SSDEEP:	48:YcmiklSiklqQqAPqqTlYclQKHoTw091aPc8C1Nfct/9BhUJo3KhmeSnpNGz0s6F5:nmdrLY9pSKI0Ik0JCKL8xpbOTQVuwn
MD5:	FB24375E481BA0FE25B3500E9A62FB02
SHA1:	A074CC19674FD21371358D9BAD00C713E7CF8FFA
SHA-256:	622A5E9AB6FB79EB25EFF5ACF27EEAB648A31EBDE549FAD50AD3145AADD91C92
SHA-512:	3E2E02C6FDFB65AD535FDF448857DF2EE74CC495F4ED6D859BE86A7E3E2E8148DBF6D531374F65A0D454DBBF409E88AEF9026EB58CF25CA6CFCAF8AC23EF0EDF
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13274463450428760","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	1.0110088256901535
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoo:wIElwQF8mpcSJ2YC1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
MD5:	C4572C0065A2DAC2D8EE9AA58224B891
SHA1:	36EEDBF08BD2AA510A83EA6843F31C3905E252F7
SHA-256:	5398A7FA57490995549F1E3044C5BA96FADADFA5B5BE6CF304A506098C1DC3FF
SHA-512:	821E36BE3A9CF07F29F2ACD11A80EFBEB323731FF3784570275A78166393438047E34E588E6473126E58456765BD92AD50F87A9CB079AF049E1C9D143B74E773
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8264463562656899
Encrypted:	false
SSDEEP:	48:DgqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUUY6:DghIElwQF8mpcSYd
MD5:	C32F97B8780A74E78C53FBC6B0CEA71F
SHA1:	40AA03612F6E83D88F361AEA99D87A1B993A28E2
SHA-256:	602044F2DC9ABDF59080DC50B99908190A5A932BC11908A363958BD08D3BC69B
SHA-512:	1475A83030810BF8256701271BB80BF64BED555ADBD47BBD107C156CBE9E1AEA2D2261C954EDBB7AE847EB99DC426734EA6C796B378A5AE434391173DAC5BC32
Malicious:	false
Reputation:	low
Preview:	.....{ ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure PreferencesE (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):	18940
Entropy (8bit):	5.568751349618025
Encrypted:	false
SSDEEP:	384:ZQ9t8LlHYXW1kXqKf/pUZNCgVLH2HfDxrUFHGr0VK4JB:NLlCW1kXqKf/pUZNCgVLH2HfdrUZGYVB
MD5:	CE2BFC4472EC25A9809A130E364D2BFE
SHA1:	F947381FAE7136BBBB12590EA7646090FC5BCADA
SHA-256:	83E682CBD80B3F79DA41E12FCB8312BFF737CE0FA499FA8D3B3F8592A4EA2B16
SHA-512:	87BBAECA5889CE8BE67F09EFB0CE75412F8ED88BC37AE65279F1D937DFD0EF00A2C52567A45B1A7C749B579FDFF5376DD4DFC8D068ED5C8E5FB7B2BFC4B08671
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":"13274463450145791","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	319
Entropy (8bit):	5.190776864309183
Encrypted:	false
SSDEEP:	6:mJb7JHlL+q2P923iKKdKrQMxIFUtpubbE1ZmwPubgP31LVkwO923iKKdKrQMFLJ:ulHlyv45KkCFUtp+u/P+gdR5L5KktJ
MD5:	703632EDDF72277B43924F1125EEA99F
SHA1:	E45E46730F15B180D7524F24DD7C4F74D61A6371
SHA-256:	81B3759F50C9BFB15FB266E0B63A48845226934A4F25AE6B14F5924C36F9AC28
SHA-512:	D2AE210B67C11A933F51A310333E72FEBD3A4F4BEC16C3873920323CD5C077B1EA66CA81114DDEEE6ACE61CBC679F3A2A38D8293F90A905966529AFB6E1691 1
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.348 1c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/26-07 :57:30.349 1c8 Recovering log #3.2021/08/26-07:57:30.350 1c8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.190776864309183
Encrypted:	false
SSDEEP:	6:mJb7JHlL+q2P923iKKdKrQMxIFUtpubbE1ZmwPubgP31LVkwO923iKKdKrQMFLJ:ulHlyv45KkCFUtp+u/P+gdR5L5KktJ
MD5:	703632EDDF72277B43924F1125EEA99F
SHA1:	E45E46730F15B180D7524F24DD7C4F74D61A6371
SHA-256:	81B3759F50C9BFB15FB266E0B63A48845226934A4F25AE6B14F5924C36F9AC28
SHA-512:	D2AE210B67C11A933F51A310333E72FEBD3A4F4BEC16C3873920323CD5C077B1EA66CA81114DDEEE6ACE61CBC679F3A2A38D8293F90A905966529AFB6E1691 1
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.348 1c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/26-07 :57:30.349 1c8 Recovering log #3.2021/08/26-07:57:30.350 1c8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/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):	347
Entropy (8bit):	5.159158354480269
Encrypted:	false
SSDEEP:	6:mJZBnR3+q2P923iKKdK7Uh2ghZIFUtpuZFCWZmwPuZHnR3VkwO923iKKdK7Uh2gd:A+v45KkIhHh2FUtpZW/PkBV5L5KkIhHd
MD5:	DF5C03B4F72D97584AB94ED1E086D1EF
SHA1:	490CA8060935BEE1AA9C6CA2852B0D32CCC2B813
SHA-256:	0798BE783B9BFC1A9EFF9DCC360D1A1B79AC2851187BAF43E24CF15213061B9B
SHA-512:	1E65C12701B775687A06D11912E535347E34A707E16F474A4D8A1C2C4830408EA2244F6FBF9B67717710ADD1AEC3B3A4BA632942D388DE5346B2ABA43BCD2DA
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.151 8cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/08/26-07:57:30.155 8cc Recovering log #3.2021/08/26-07:57:30.157 8cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Char acteristics 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):	347
Entropy (8bit):	5.159158354480269
Encrypted:	false
SSDEEP:	6:mJZBnR3+q2P923iKKdK7Uh2ghZIFUtpuZFCWZmwPuZHnR3VkwO923iKKdK7Uh2gd:A+v45KkIhHh2FUtpZW/PkBV5L5KkIhHd
MD5:	DF5C03B4F72D97584AB94ED1E086D1EF
SHA1:	490CA8060935BEE1AA9C6CA2852B0D32CCC2B813
SHA-256:	0798BE783B9BFC1A9EFF9DCC360D1A1B79AC2851187BAF43E24CF15213061B9B
SHA-512:	1E65C12701B775687A06D11912E535347E34A707E16F474A4D8A1C2C4830408EA2244F6FBF9B67717710ADD1AEC3B3A4BA632942D388DE5346B2ABA43BCD2DA
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.151 8cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/08/26-07:57:30.155 8cc Recovering log #3.2021/08/26-07:57:30.157 8cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Char acteristics 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):	429
Entropy (8bit):	5.262566993740236
Encrypted:	false
SSDEEP:	6:mJiaAQ+q2P923iKKdKusNpV/2jMGIFUtpu5QSpgZmwPugqPAQVkwO923iKKdKusO:+9+v45KkFFUtp/Sm/PZa9V5L5KkOJ
MD5:	090706AB45A19A912E50E0021D7C12D5
SHA1:	9F7FD02E6C7A11CF067F73C6B5445F29B4F99BBC
SHA-256:	423411FB784696ABBC529E961827E3F451AA152D65C902A5D96AF6D2C948E748
SHA-512:	5F3DB836657C01B759F81DC915E817AE525BE6EFC5B27CF05950C8F7502592B75C9FB6A0BFAD615C2723A2FA59FA6315B23A47B1CAF281A3B033CDD2A5F6A4E F
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.420 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:57:30.421 57c Recovering log #3.2021/08/26-07:57:30.422 57c Reusing old log C:\Users\user\AppD ata\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):	429
Entropy (8bit):	5.262566993740236
Encrypted:	false
SSDEEP:	6:mJiaAQ+q2P923iKKdKusNpV/2jMGIFUtpu5QSpgZmwPugqPAQVkwO923iKKdKusO:+9+v45KkFFUtp/Sm/PZa9V5L5KkOJ
MD5:	090706AB45A19A912E50E0021D7C12D5
SHA1:	9F7FD02E6C7A11CF067F73C6B5445F29B4F99BBC
SHA-256:	423411FB784696ABBC529E961827E3F451AA152D65C902A5D96AF6D2C948E748
SHA-512:	5F3DB836657C01B759F81DC915E817AE525BE6EFC5B27CF05950C8F7502592B75C9FB6A0BFAD615C2723A2FA59FA6315B23A47B1CAF281A3B033CDD2A5F6A4E F
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.420 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:57:30.421 57c Recovering log #3.2021/08/26-07:57:30.422 57c Reusing old log C:\Users\user\AppD ata\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 State2. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State2. (copy)	
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","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):	428
Entropy (8bit):	5.278875000200849
Encrypted:	false
SSDEEP:	6:mJySq2P923iKKdKusNpqz4rRIFUtpuXZmwPuFkwO923iKKdKusNpqz4q8LJ:Ov45KkmiuFUtpY/PA5L5Kkm2J
MD5:	CF8BF829B620706221FB91CD76B79B6A
SHA1:	08B96F1CB90C7E5E70C0550987A221ED50F493B4
SHA-256:	084F905E48850B975973E6867AB1DE8E73CD336240B23E71E554ED132EDD3981
SHA-512:	C8097DD11EB44F30A6D86AB8AF81B7A97F5416E6EA1527A8E3E44D7109BE1B720A48B303F0C6BF50E25B8452AF0B799E2245389FEC447AB6C78938C0D9FCBF51
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.464 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/26-07:57:30.465 f0 Recovering log #3.2021/08/26-07:57:30.465 f0 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.olde, (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.278875000200849
Encrypted:	false
SSDEEP:	6:mJySq2P923iKKdKusNpqz4rRIFUtpuXZmwPuFkwO923iKKdKusNpqz4q8LJ:Ov45KkmiuFUtpY/PA5L5Kkm2J
MD5:	CF8BF829B620706221FB91CD76B79B6A
SHA1:	08B96F1CB90C7E5E70C0550987A221ED50F493B4
SHA-256:	084F905E48850B975973E6867AB1DE8E73CD336240B23E71E554ED132EDD3981
SHA-512:	C8097DD11EB44F30A6D86AB8AF81B7A97F5416E6EA1527A8E3E44D7109BE1B720A48B303F0C6BF50E25B8452AF0B799E2245389FEC447AB6C78938C0D9FCBF51
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.464 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/26-07:57:30.465 f0 Recovering log #3.2021/08/26-07:57:30.465 f0 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\a0547d60-ec91-4de8-b973-4d02ee85174c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","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):	429
Entropy (8bit):	5.201227296631704
Encrypted:	false
SSDEEP:	12:aYyv45KkkGHArBFUtpKjPJ/PKXR5L5KkkGHAryJ:BY45KkkGgPgaQDL5KkkGga
MD5:	588B88E91FE18F59A5D35E689B38C64F
SHA1:	435FDC3602DF333B6D9DD660D8D2D36A0B812A24
SHA-256:	96E26076D30A00A3E07A22486F60C8BF16FB822510B4A851C71AC4AEEF251532
SHA-512:	0E200F204538E200EFF1F41715E6CA10AA8CACEEF9C7E1344057F5B7019068C7F91296834056620D67956F8EE1757BDBE005BF4EA8395B3A26236B5FD73B2E69
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:40.012 1c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:57:40.017 1c8 Recovering log #3.2021/08/26-07:57:40.019 1c8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.201227296631704
Encrypted:	false
SSDEEP:	12:aYyv45KkkGHArBFUtpKjPJ/PKXR5L5KkkGHAryJ:BY45KkkGgPgaQDL5KkkGga
MD5:	588B88E91FE18F59A5D35E689B38C64F
SHA1:	435FDC3602DF333B6D9DD660D8D2D36A0B812A24
SHA-256:	96E26076D30A00A3E07A22486F60C8BF16FB822510B4A851C71AC4AEEF251532
SHA-512:	0E200F204538E200EFF1F41715E6CA10AA8CACEEF9C7E1344057F5B7019068C7F91296834056620D67956F8EE1757BDBE005BF4EA8395B3A26236B5FD73B2E69
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:40.012 1c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/26-07:57:40.017 1c8 Recovering log #3.2021/08/26-07:57:40.019 1c8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	5.190965930586822
Encrypted:	false
SSDEEP:	12:a+v45KkkGHArqiuFUtpKg/PKh5L5KkkGHArq2J:n45KkkGgCgML5KkkGg7
MD5:	6F5017FD934423957A70817BDF902BE9
SHA1:	9C076CC6D64652BD56B1A398068C815D372E576B
SHA-256:	588D9D7EBCA03E6470FE18E7C741F339BFD84EC2B155141D451B6433A37E2D0E
SHA-512:	ABBB9E566F8599A930D7775714AC06D65F9A126ECFF025F9D8E8FCCA50FC98CC19E1115DF3B9ACC154D0AAF33713651711D542B67BBC8284B7AEF991DEA3561
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:40.024 d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/26-07:57:40.027 d04 Recovering log #3.2021/08/26-07:57:40.028 d04 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.oldg (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	5.190965930586822
Encrypted:	false
SSDEEP:	12:a+v45KkkGHArqiuFUtpKg/PKh5L5KkkGHArq2J:n45KkkGgCgML5KkkGg7
MD5:	6F5017FD934423957A70817BDF902BE9
SHA1:	9C076CC6D64652BD56B1A398068C815D372E576B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.oldg (copy)	
SHA-256:	588D9D7EBCA03E6470FE18E7C741F339BFD84EC2B155141D451B6433A37E2D0E
SHA-512:	ABBB9E566F8599A930D7775714AC06D65F9A126ECFF025F9D8E8FCCA50FC98CC19E1115DF3B9ACC154D0AAF33713651711D542B67BBC8284B7AEF991DEA3561
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:40.024 d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/26-07:57:40.027 d04 Recovering log #3.2021/08/26-07:57:40.028 d04 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:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.228938447027757
Encrypted:	false
SSDEEP:	6:mJZh4q2P923iKKdKpIFUtpuZBeVLJZmwPuZrDkwO923iKKdKa/WLJ:Lv45KkmFUtptV9/P05L5KkaUJ
MD5:	67CCC181A2EA1E64B7CCBCA9CC113D7A
SHA1:	ABC732EE0A3BDB78B2EF7AC4CBB5D5DB732BA3AC
SHA-256:	BC271430D8DC1D05FE4B4A3EEA5D30454EBA1A9BEE29A3F71DE8240E60862A99
SHA-512:	F09BC70CA1AD2B0617203B42A1BF7B838C9F9F39FC0FFCBBAC5943839DC13D76FD5709E667D71E6855DF125C2CCD777BE73456E7CC32C77BA2F44F1B222A9CE6
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.143 1404 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/26-07:57:30.151 1404 Recovering log #3.2021/08/26-07:57:30.152 1404 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):	326
Entropy (8bit):	5.228938447027757
Encrypted:	false
SSDEEP:	6:mJZh4q2P923iKKdKpIFUtpuZBeVLJZmwPuZrDkwO923iKKdKa/WLJ:Lv45KkmFUtptV9/P05L5KkaUJ
MD5:	67CCC181A2EA1E64B7CCBCA9CC113D7A
SHA1:	ABC732EE0A3BDB78B2EF7AC4CBB5D5DB732BA3AC
SHA-256:	BC271430D8DC1D05FE4B4A3EEA5D30454EBA1A9BEE29A3F71DE8240E60862A99
SHA-512:	F09BC70CA1AD2B0617203B42A1BF7B838C9F9F39FC0FFCBBAC5943839DC13D76FD5709E667D71E6855DF125C2CCD777BE73456E7CC32C77BA2F44F1B222A9CE6
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:30.143 1404 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/26-07:57:30.151 1404 Recovering log #3.2021/08/26-07:57:30.152 1404 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):	401
Entropy (8bit):	5.334859410924718
Encrypted:	false
SSDEEP:	6:mJrBiq2P923iKKdKks8Y5JKKhdIFUtpuFpZmwPuyzkwO923iKKdKks8Y5JKKTLJ:oYv45KkkOrsFUtpG/PV5L5KkkOrzJ
MD5:	6BE816E7E319D399F0F06BDA4399F487
SHA1:	B15DAB8B94060CA426C263E5720BAE6E42D90814
SHA-256:	90757E633B57AD6370E2789922DE7FB584424BE3E48B15A219D9681B8985CD6D
SHA-512:	BA69136FD40912519EFFAE72AAC6478708EAD657219ABACD4DFCA069BA2FD69D5B4CD4A91A62388C56A3A00E022B2FB2F90FD5AE1604926F63C9AFE4D2B214 59
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:41.416 d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbm eomcjbeemfm/MANIFEST-000001.2021/08/26-07:57:41.418 d04 Recovering log #3.2021/08/26-07:57:41.419 d04 Reusing old log C:\Users\user\AppData\Local\Goog le\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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	401
Entropy (8bit):	5.334859410924718
Encrypted:	false
SSDEEP:	6:mJrBiq2P923iKKdKks8Y5JKKhdIFUtpuFpZmwPuyzkwO923iKKdKks8Y5JKKTLJ:oYv45KkkOrsFUtpG/PV5L5KkkOrzJ
MD5:	6BE816E7E319D399F0F06BDA4399F487
SHA1:	B15DAB8B94060CA426C263E5720BAE6E42D90814
SHA-256:	90757E633B57AD6370E2789922DE7FB584424BE3E48B15A219D9681B8985CD6D
SHA-512:	BA69136FD40912519EFFAE72AAC6478708EAD657219ABACD4DFCA069BA2FD69D5B4CD4A91A62388C56A3A00E022B2FB2F90FD5AE1604926F63C9AFE4D2B214 59
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:41.416 d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbm eomcjbeemfm/MANIFEST-000001.2021/08/26-07:57:41.418 d04 Recovering log #3.2021/08/26-07:57:41.419 d04 Reusing old log C:\Users\user\AppData\Local\Goog le\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecuritye (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):	874
Entropy (8bit):	5.561713251441355
Encrypted:	false
SSDEEP:	12:YdDZ6Hk3O+UAnIvld06cY8rNgmh4r+UAnIEllWcNnYj+UAnIECm13R7N+UAnI3L0:YT6H0UhHPkG1KUe9aUeCwB7wUWRUeIQ
MD5:	A58DB42A13D916CB1BB0C2347F218AB9
SHA1:	2CF80A8F1EC054544D6B61C00BAFBEC7C5A5EE89
SHA-256:	A8BE81843C9C12F4C1CEE879FA7D00076DEB2260E988B6C19658D9EF648D93A9
SHA-512:	09D3464DACA7E5B43C46131F47224B0984A20CB7B3814CF49533ED75563B59738BCA9E3BAB062FA0EAB27AFBB17FA6C6F2947FCF0AF6B07B028D6C5AD145475 4
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1601477028.822838},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_in clude_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=", "mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1661525856.342144,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C 5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629989856.342148},{"expiry":1633013028.952627,"host":"+ccWXqaoHJ 9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.95263}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c1aff6af-05dd-47aa-becc-0e314feb084f.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):	18940
Entropy (8bit):	5.568751349618025
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c1aff6af-05dd-47aa-becc-0e314feb084f.tmp	
SSDEEP:	384:ZQ9t8LlHYXW1kXqKf/pUZNCgVLH2HfDxrUFHGr0VK4JB:NLlCW1kXqKf/pUZNCgVLH2HfdrUZGYVB
MD5:	CE2BFC4472EC25A9809A130E364D2BFE
SHA1:	F947381FAE7136BBBB12590EA7646090FC5BCADA
SHA-256:	83E682CBD80B3F79DA41E12FCB8312BFF737CE0FA499FA8D3B3F8592A4EA2B16
SHA-512:	87BBAECA5889CE8BE67F09EFB0CE75412F8ED88BC37AE65279F1D937DFD0EF00A2C52567A45B1A7C749B579FDFF5376DD4DFC8D068ED5C8E5FB7B2BFC4B08 671
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13274463450145791","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cff21966-e84c-4b64-a6dd-f53fd0429396.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):	4785
Entropy (8bit):	4.936317417564759
Encrypted:	false
SSDEEP:	48:YcmiklSiklqQqAPqqTlYclQKHoTw091aPc8C1Nfct/9BhUJo3KhmeSnpNGz0s6F5:nmdrLY9pSKI0Ik0JCKL8xpbOTQVuwn
MD5:	FB24375E481BA0FE25B3500E9A62FB02
SHA1:	A074CC19674FD21371358D9BAD00C713E7CF8FFA
SHA-256:	622A5E9AB6FB79EB25EFF5ACF27EEAB648A31EBDE549FAD50AD3145AADD91C92
SHA-512:	3E2E02C6FDFB65AD535FDF448857DF2EE74CC495F4ED6D859BE86A7E3E2E8148DBF6D531374F65A0D454DBBF409E88AEF9026EB58CF25CA6CFCAF8AC23EF0 EDF
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13274463450428760","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245950640095768","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","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.533261589702817
Encrypted:	false
SSDEEP:	3:tUK6jvOzbVN2WZmwv3ljvLHhR1V8sljvLHhR1WGv:mJMxXZmwPuTB7VvuTB7tv
MD5:	0F0C90DFF5E9CBD4B9245BE4886429D9
SHA1:	B18FDE5B2D4C3B2691FBC0226213D84DF95C799D
SHA-256:	5A07C9608B867C282D2C2C6F20D473356B59E90DE3577F6DD71F342BA12002F5
SHA-512:	E88544D457C3D1FE3F9C82086F2784C1B1470BA4F475AE91683F95BC0A637C157367BE53430F6B2434A16938496FD44479223C9419B15207D9F3CFE5B6415D4D
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.127 1390 Recovering log #3.2021/08/26-07:57:39.175 1390 Delete type=0 #3.2021/08/26-07:57:39.175 1390 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old3c (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.533261589702817
Encrypted:	false
SSDEEP:	3:tUK6jvOzbVN2WZmwv3ljvLHhR1V8sljvLHhR1WGv:mJMxXZmwPuTB7VvuTB7tv
MD5:	0F0C90DFF5E9CBD4B9245BE4886429D9
SHA1:	B18FDE5B2D4C3B2691FBC0226213D84DF95C799D
SHA-256:	5A07C9608B867C282D2C2C6F20D473356B59E90DE3577F6DD71F342BA12002F5
SHA-512:	E88544D457C3D1FE3F9C82086F2784C1B1470BA4F475AE91683F95BC0A637C157367BE53430F6B2434A16938496FD44479223C9419B15207D9F3CFE5B6415D4D
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:39.127 1390 Recovering log #3.2021/08/26-07:57:39.175 1390 Delete type=0 #3.2021/08/26-07:57:39.175 1390 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/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e6c4b7a7-4176-49a2-bbcd-67abdbe9e136.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):	2693
Entropy (8bit):	4.871599185186076

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e6c4b7a7-4176-49a2-bbcd-67abdbe9e136.tmp	
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

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):	334
Entropy (8bit):	5.212856916159683
Encrypted:	false
SSDEEP:	6:mJzH4q2P923iKKdKfrzAdIFUtpuzbgZmwPuzZkwO923iKKdKfrzILJ:aYv45Kk9FUtpKbg/PKZ5L5Kk2J
MD5:	FFCF4328C295CA7F8C886895FEE3BBA1
SHA1:	A8EDCA64C1CCC043FE75EC4FF0A2B6A912FEACBD
SHA-256:	EFDEEE32A714AF7AC62BDBCD61323B00B506BE919AF05B1F995DDA12299FEB27
SHA-512:	7C734AFDA8B5972B289F35B263FD80451AF84848FC56703C9B55B4819E8CCFD98E9C633295A36E4C36633637F18992B2810181959B4DD8DC39EE28024C88E48E
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:40.127 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/26-07:57:40.128 f0 Recovering log #3.2021/08/26-07:57:40.129 f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.212856916159683
Encrypted:	false
SSDEEP:	6:mJzH4q2P923iKKdKfrzAdIFUtpuzbgZmwPuzZkwO923iKKdKfrzILJ:aYv45Kk9FUtpKbg/PKZ5L5Kk2J
MD5:	FFCF4328C295CA7F8C886895FEE3BBA1
SHA1:	A8EDCA64C1CCC043FE75EC4FF0A2B6A912FEACBD
SHA-256:	EFDEEE32A714AF7AC62BDBCD61323B00B506BE919AF05B1F995DDA12299FEB27
SHA-512:	7C734AFDA8B5972B289F35B263FD80451AF84848FC56703C9B55B4819E8CCFD98E9C633295A36E4C36633637F18992B2810181959B4DD8DC39EE28024C88E48E
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:57:40.127 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/26-07:57:40.128 f0 Recovering log #3.2021/08/26-07:57:40.129 f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
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 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):	369033
Entropy (8bit):	6.015161835361297
Encrypted:	false
SSDEEP:	6144:vP8oPjxD8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB0:XRjxwxzurRDn9nfNxF4ijZVtilB0
MD5:	50B0F4936D143DC1BAE9FE58361BD7C9
SHA1:	E8DE1CBC6FDF23BE9732EC6101C02BC26D879391
SHA-256:	813197B0DF62785619A8FC8DEEFA403426A0C4AE00212461094075F8B5FCD065
SHA-512:	B88258675D406A3194566C0FE191C01A90301A9D5496AD95B4FC7458927AAA2AFC4612CDAD13C7941000B14A977D8EAA49BF8082B2F16619EC50FDCDEFE9851
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":1.629989854462247e+12,"network":1.629957456e+12,"ticks":3939768103.0,"uncertainty":4956536.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327446345007

C:\Users\user\AppData\Local\Temp\0dad7087-158e-4fd7-9ae4-a315a170d0ea.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L]....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\1ae382d8-7f81-4945-b807-cf3776b963c5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\1ae382d8-7f81-4945-b807-cf3776b963c5.tmp	
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\4903bf7a-e852-4da0-a450-3929968fb8e5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\b6ba01d9-f118-4f1c-b6d6-408101a16f8b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	4992
Entropy (8bit):	4.646498147325179
Encrypted:	false
SSDEEP:	96:ex2F3g+/b++b0ReltUC3vTSfUhRlZphRtUltUftU4EtUG7RtUM:N3gCb+nenL2fUrl/hREeYZB
MD5:	06854A7FE118304BE2A99EAD51F99B57
SHA1:	A46E2F10F88858B156C001251E99D448E5FA5B02
SHA-256:	3C7A498D8E0E1F31AD69B015DF09922A4EDD91C03EA91F06ADFCAF2BFA6FEB0F
SHA-512:	2781808BF73CE6D29374E0352DCF76C9442EA0C586276C9008953CC5B1B49FB303FC74812B9F0AB63F77889AB390B5970DEA6773FC9EEB692B9B67C6D38ECA8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET c5647263c9a78c0dc059e03d4310580758c9c1c38924a6b2cb6197196eff8f2a e32086ee012cc2187d6d623c954cfaccc 25be96232fc7df6a075724f5b5bd5a3.SERVER_HANDSHAKE_TRAFFIC_SECRET c5647263c9a78c0dc059e03d4310580758c9c1c38924a6b2cb6197196eff8f2a 8 710d2db36bf0b3d326d76eedd283b9b550b8b4e1a4121480fe12ec8a78a2fdd.CLIENT_HANDSHAKE_TRAFFIC_SECRET 53c9677cf595ad1d3242b63708ae868b3b 9775976c75dabd20baf86f01d973bb 7ccb9e4a169cfc0b2a98ddd052a114c50a3c204a784c2116c356110143247c1d.SERVER_HANDSHAKE_TRAFFIC_SECRET 53 c9677cf595ad1d3242b63708ae868b3b9775976c75dabd20baf86f01d973bb 09e7d60f686c54574d44105e9f01d919cf05644124052b5627d09d48b4212689.CL IENT_HANDSHAKE_TRAFFIC_SECRET 3b906f1270d772deddda4529c241acae1924976e29829f24b5a2d927474353dd 73930d34c78167ab07d835c8be81d5364e9 167245da3270d1acf8bdaa1c0751e.SERVER_HANDSHAKE_TRAFFIC_SECRET 3b906f1270d772deddda4529c241acae1924976e29829f24b5a2d927474353dd 759 44e3d9e6193307c013df5080f836f8032da34b631eef185fa724e11983515.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\ca0680fc-385c-4de2-be0f-f74336146d08.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..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6.. @?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\eda03c05-6b6c-4bd5-a730-75d34e692ce1.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...I.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_dir5916_100679197\0dad7087-158e-4fd7-9ae4-a315a170d0ea.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_dir5916_100679197\0dad7087-158e-4fd7-9ae4-a315a170d0ea.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_dir5916_100679197\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_dir5916_100679197\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:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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_dir5916_100679197\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.".. }..}..

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 07:57:36.301886082 CEST	192.168.2.5	8.8.8.8	0xf937	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:57:36.307468891 CEST	192.168.2.5	8.8.8.8	0x6f7f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:57:36.309520960 CEST	192.168.2.5	8.8.8.8	0xd34f	Standard query (0)	clapham.allow.me	A (IP address)	IN (0x0001)
Aug 26, 2021 07:57:39.655853033 CEST	192.168.2.5	8.8.8.8	0x4c2	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 07:57:36.334465981 CEST	8.8.8.8	192.168.2.5	0xf937	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Aug 26, 2021 07:57:36.349920034 CEST	8.8.8.8	192.168.2.5	0x6f7f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:57:36.349920034 CEST	8.8.8.8	192.168.2.5	0x6f7f	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Aug 26, 2021 07:57:36.463563919 CEST	8.8.8.8	192.168.2.5	0xd34f	No error (0)	clapham.allow.me		52.56.219.240	A (IP address)	IN (0x0001)
Aug 26, 2021 07:57:39.695965052 CEST	8.8.8.8	192.168.2.5	0x4c2	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:57:39.695965052 CEST	8.8.8.8	192.168.2.5	0x4c2	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 07:57:36.543843985 CEST	52.56.219.240	443	192.168.2.5	49686	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 07:57:36.547712088 CEST	52.56.219.240	443	192.168.2.5	49687	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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: 5916 Parent PID: 4304

General

Start time:	07:57:29
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:	0x7ff677c70000
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: 2856 Parent PID: 5916

General

Start time:	07:57:30
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=1624,12626956359303723085,12777355795646735380,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1684 /prefetch:8
Imagebase:	0x7ff677c70000
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