ID: 449546
Cookbook: browseurl.jbs
Time: 20:48:41
Date: 15/07/2021
Version: 33.0.0 White Diamond

Table of Contents

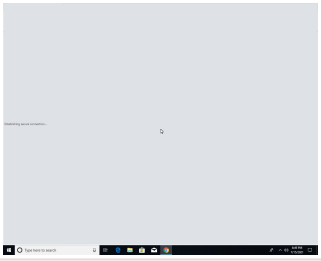
Windows Analysis Report https://www.grainger.ca/fr/co…

Overview

General Information

Sample URL:	http://https://www.grainger.ca/fr/content/covid-19-recovery
Analysis ID:	449546
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

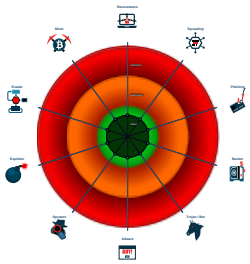
Detection

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: 5428 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.grainger.ca/fr/content/covid-19-recovery' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3228 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1576,8722109470797325843,6740444566604102159,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1712 /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

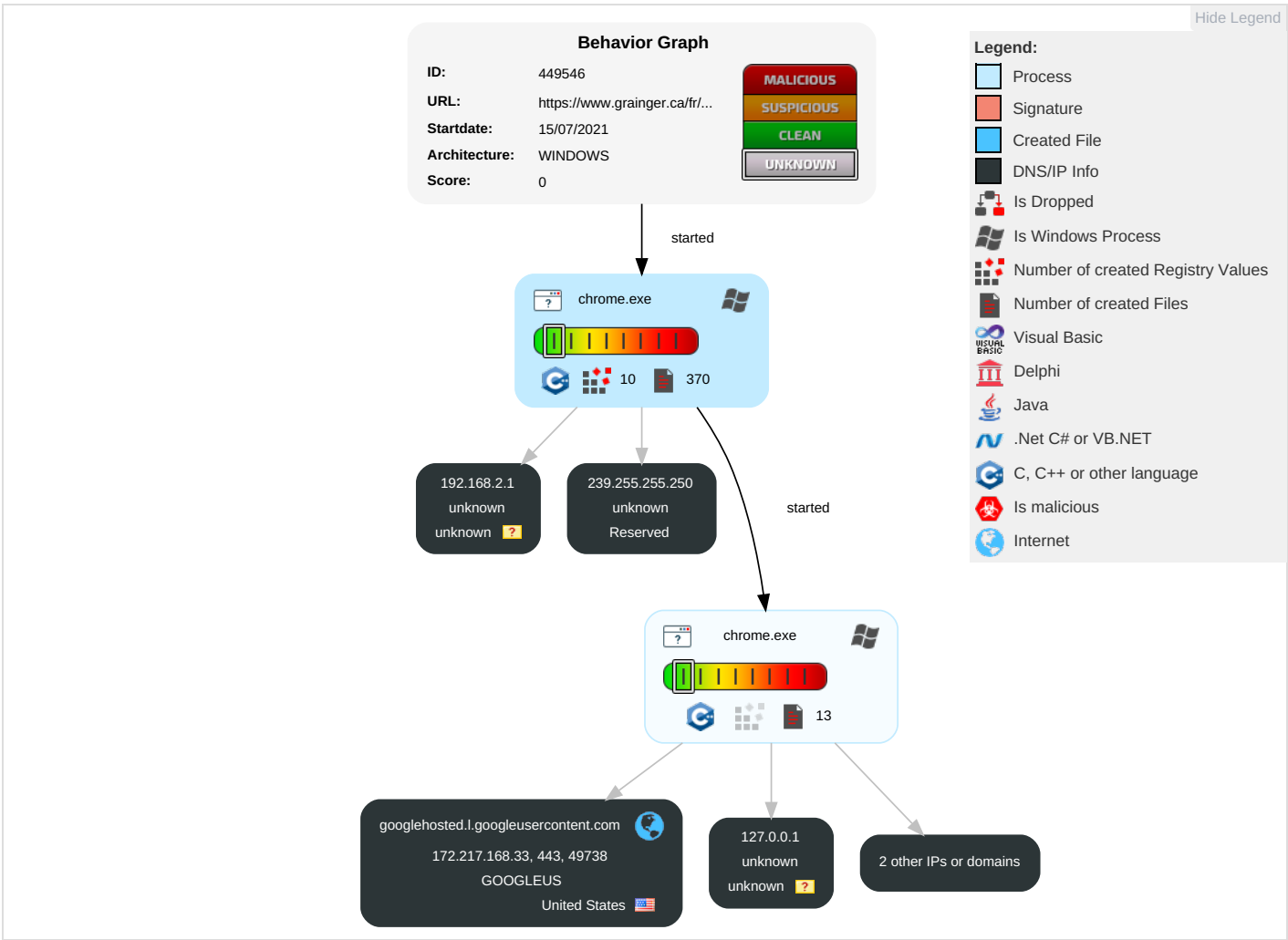
Click to jump to signature section

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

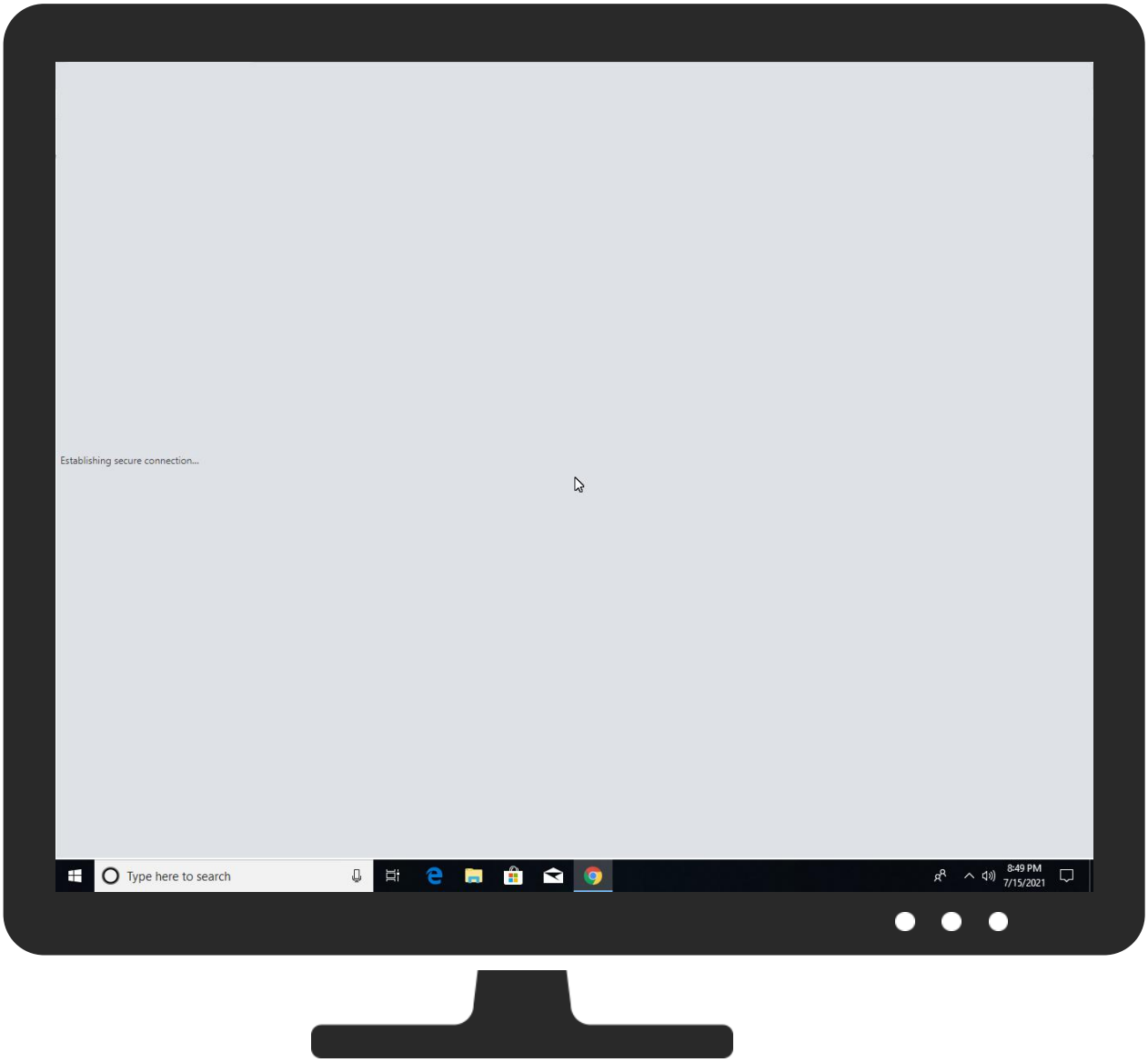
Behavior Graph



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://www.grainger.ca/fr/content/covid-19-recovery	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://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.grainger.ca/fr/content/covid-19-recovery8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
www.grainger.ca	unknown	unknown	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	449546
Start date:	15.07.2021
Start time:	20:48:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.grainger.ca/fr/content/covid-19-recovery
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.win@27/147@2/4
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
20:49:38	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{..,."':o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.139205445116623
Encrypted:	false
SSDEEP:	6:kK3f8EdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:ff8U5kPlE99SNxAhUe0et
MD5:	57965E1325F78611529F513D188FD62B
SHA1:	5F1B1CB8886D080F11EFEF830562D157BF95121B
SHA-256:	F27CB04DC621C29456AB88E2F9F2E62E8F938043E6C34E02A075ADB65DEE835E
SHA-512:	502357972921C6DBBFFBF9AEF31423837A6A8E55009337DCC45089F0C001E69788E8C63653991844357FDDB510325461CC5CFF6842E7C00251072E7E0ACDC0A7
Malicious:	false
Reputation:	low
Preview:	p..... .....'...y..(..... .....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\4f25f9cd-7214-495e-a570-101c1920fd4b.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):	364461
Entropy (8bit):	6.015186023351115
Encrypted:	false
SSDEEP:	6144:AdaiWKY35OzLUjSJ4p8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/di:AdoKO5ALtJzxzurRDn9nfNxF4ijZVti8
MD5:	A9D5C3DC72C72DC3D406E7FE3963483E
SHA1:	38834CE0E1A321FF264DCCA08953DFCC3A2BA952
SHA-256:	B1946770B5F6922AA312908FBDF143E01EE9407B26D9604146E6458C21EC919A
SHA-512:	ECC347934C5709494985D31339FD8F95E14B8C977CEB0E510E1AFE1F3EBB71BD2B5DCAF3BA7007C11DCB2B795B6D4431FB7C9327F62F29EB646830BAFE1C10C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\4f25f9cd-7214-495e-a570-101c1920fd4b.tmp	
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":1.626407376993742e+12,"network":1.626374978e+12,"ticks":6600169106.0,"uncertainty":4662628.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1Qfj oKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP0 5zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327088097370

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
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\3a74a108-5304-48e7-9799-89585014dbf1.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):	5.561170510749199
Encrypted:	false
SSDEEP:	12:YdDZ6Hk3O+UAnIvld06cY8rNgmh4r+UAnIEllWcNnYj+UAnIECm3N4R7N+UAnIEz:YT6H0UhHPkG1KUe9aUeCP7wUKRUeIQ
MD5:	947F1C1934FB10187D823B4A497644E5
SHA1:	814F8F04E775973A2CBDFD9195704ED4F58B6E3F
SHA-256:	FCC45B2503D1217538E10869674414A3AB01FBABD22A76A169E71C5D2C16421F
SHA-512:	CA38D048748EC3124041DBD3FE5AAEDA7F4E35529B644753983A1FC3ACC72526821C10D21A50894C3E69488D5CE5019FE670F7505B9D526AAFDB7F42D13CC53
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":1657943378.592874,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626407378.592878},{"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\9af6c785-10fb-45c2-8eb5-fd4683da394d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577290040639218
Encrypted:	false
SSDEEP:	384:HyttrLlz3X91kXqKf/pUZNCgVLH2HfDurUsCKCGz40:GLlb91kXqKf/pUZNCgVLH2HfyrUsVnzz
MD5:	089814FBDB0BD209227EBC6A5D731CBD
SHA1:	F3ED0E0B5479FDE73DC572EA9DC3D452014B2C0D
SHA-256:	8A6F0F8C972A9B587FB64C25573BDC55266D7DA88AAD78C9CF41E94E4AC76773
SHA-512:	3F4ABEF83AB02BC0619BF11413F9705B33FC5DD3BE2B297D4E0840C4C6DA92ECCB5F43C32F5674FD18F170B460E36D7DC620169C7327FA223B577BE9E7DE739
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":"13270880973783251","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9af6c785-10fb-45c2-8eb5-fd4683da394d.tmp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9d9855b2-212b-4336-9d7e-06f1a8cdb372.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
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\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.190800930759596
Encrypted:	false
SSDEEP:	6:mV+QcROq2P923iKKdK9RXXTZIFUtpo+Q5UEZmwPo+QpEkwO923iKKdK9RXX5LJ:5QgOv45Kk7XT2FUtppQb/PpQpE5L5KkT
MD5:	1842A5E5DD37445BC2ADC938BAFD33A3
SHA1:	53CDAC531F40C750E3B04074C15BFB29D6F7D30E
SHA-256:	E3AE43AEF33AF15931D8F846ED4E681779CE7AD6B9DBA42191361B1E98C30DA1
SHA-512:	F338C914E9AD37BC0D6F4A9248777821D9CDB55843756D5D185F5B8B2C809D45D3F2793E22334C4765E8EDD94E6C3EAC656437984A083CBB4F426E88A68B336
Malicious:	false
Reputation:	low
Preview:	2021/07/15-19:01:41.605 1b14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/15-19:01:41.608 1b14 Recovering log #3.2021/07/15-19:01:41.610 1b14 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):	5.195931701222266
Encrypted:	false
SSDEEP:	6:mV+QBrZq2P923iKKdKyDZIFUtpo+QS9ZmwPo+Q8kwO923iKKdKyJLJ:5QtZv45Kk02FUtppQC/PpQ85L5KkWJ
MD5:	556B6D6E6BA87B45BA150ACE0208562A
SHA1:	454FF04E21E4BED63208658A10430EBF4191FF50
SHA-256:	307AD1345617586D025B66C82E5DD5E304ABB28159607BD0A5DFCDD65ECA0108
SHA-512:	F1ECE42B1F5FA15995703A0077CC73919ECBAF32E603E9F1FD50C58A3605796F308BEB6AD7B822DA9D67DB48F77AE7E680DC78B3FF112341C1D53AD9E3A8E40
Malicious:	false
Reputation:	low
Preview:	2021/07/15-19:01:41.517 1b14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/15-19:01:41.526 1b14 Recovering log #3.2021/07/15-19:01:41.528 1b14 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
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9696748372426434
Encrypted:	false
SSDEEP:	24:GIL4rtEy8PqLbJLbXaFpEO5bNmISHn06UwZ68:GI+qq5LLOpEO5J/Kn7UQ68
MD5:	340AC290ED491AAB217C295036C9F13C
SHA1:	8F28003E15EEBB098DC1D417CFA00BD3B7D1DAE0
SHA-256:	196EEF0DE42BFAF0008300F450AF7D6D81FF2B56B746AFF23712F2D538C185E0
SHA-512:	39B40D17013D2BF13B492EC91AA113B8DFB19E2300E4CD6E22B282B486760C412179B0DE8E1CDF23745D90855080BC2159859BE06672ACC049555774EED786CE
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	995
Entropy (8bit):	3.410202290455497
Encrypted:	false
SSDEEP:	12:3olydJhIRsKXm3ZvPlpxlpNXGJyII0kjKs/aerlW8evVuCBlpl:34SisKXm3JlrlCJc0kjKspxW8zCBlL
MD5:	BF61C2836A0F9BF26FCA21CCDE991B81
SHA1:	DC14FA3D38349E2EEC2E52ACFAC66C7ED16A6C4F
SHA-256:	187DD82DFCC1B3AF0D344696ED9C131A122E846824AEC35DF56562B45A7DE2C5
SHA-512:	5278C623D37F28C7FCCF7CDE72D1E9A9D35E74264733F25F45B0116A3FA23DFAE6C11C6249B342C3A88A5979301116FF1FA2E0604AC9811554E043AAB80467B4
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...8d706e24_bee3_46f6_befa_e6a1af9fc4ef.....9..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....|.....4...https://www.grainger.ca/fr/content/covid-19-recovery..... .....h.....`.....q.z5....q.z5.....(.....p...4...h.t.t.p.s.:././.w.w.w...g.r.a.i.n.g.e.r...c.a./.f.r./.c.o.n.t.e.n.t./.c.o.v.i.d.-.1.9.-.r.e.c.o.v.e.r.y.....8.....0.....8..... .....4...https://www.grainger.ca/fr/content/covid-19-recovery....8....%/.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.209121683628905
Encrypted:	false
SSDEEP:	6:mHEi+q2P923iKKdK8aPrqIFUtpGv2WZmwPGv9VkwO923iKKdK8amLJ:Bi+v45KkL3FUtpDW/P2V5L5KkQJ
MD5:	4966A6D8C5B040784CCF3B752A7FF0E7
SHA1:	0848411CBDA0C35E8B65D62D31346986D4B8D02C
SHA-256:	E7952F281E59EF9DF195889CBE8BD8CDCAFCBB8BC15A419DA6AAF816B22D7707
SHA-512:	7F823674A39BBFB28C8830EEB7B69D8E51E4C585204F567CFCC0121E2F7656210550ADCFE9922A8365C4920D74CD3F42DB0544048BF52BF0473F6972CB5A9A63
Malicious:	false
Reputation:	low
Preview:	2021/07/15-20:49:34.143 f3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/15-20 :49:34.145 f3c Recovering log #3.2021/07/15-20:49:34.145 f3c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................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):	322
Entropy (8bit):	5.241597434330318
Encrypted:	false
SSDEEP:	6:mHq7SVq2P923iKKdK8NIFUtpGqTlTlgZmwPGqTO0IkwO923iKKdK8+eLJ:BSVv45KkpFUtpVlBg/PVO0I5L5KkqJ
MD5:	EE9100C29C8576F761DE79A776629DB1
SHA1:	101DDDEF2C7D14CE6909D7F6D3B3EF133AC4AA0F
SHA-256:	8060D513F51680770C5A9414E9B271ED5547234A751C946DE115031F99862321
SHA-512:	B56B2F0E0111A8FE0CD260B010ACDA08150C49D9E251C52F748A876232C3DB3A5073717EA023726142B96CB2E9A3CEF8A06C865AAF2F1FEACC62A696DF72CF9
Malicious:	false
Reputation:	low
Preview:	2021/07/15-20:49:36.559 1674 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/15-20:49:36.561 1674 Recovering log #3.2021/07/15-20:49:36.563 1674 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
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=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/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):	5.243306564488686
Encrypted:	false
SSDEEP:	6:mV+Q+q2P923iKKdK25+Xqx8chI+IFUtpo+QR09ZmwPo+QUIEkwO923iKKdK25+Xc:5Q+v45KkTXfchI3FUtppQC9/PpQq5L5G
MD5:	39A0413800C3E7439403436375B5E286
SHA1:	267BE249A501FF2AB9DB234DCBC23D6612B222F4
SHA-256:	D3F332AF15FB5C5E3AD6AD7C24A8C757E455E08CE712006EC1521AE9901D6AC8
SHA-512:	8D54F1BC13642F58D090246F8EEB07BCC189B9122EAAF74C30EBFF3336BCEEA279723EAF179CCC84AB031848C91E9232DBBC99698BD8222FC5C8DBB18180A2E5
Malicious:	false
Reputation:	low
Preview:	2021/07/15-19:01:41.266 1b14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/15-19:01:41.269 1b14 Recovering log #3.2021/07/15-19:01:41.272 1b14 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):	5.209286335625319
Encrypted:	false
SSDEEP:	6:mV+LGwq2P923iKKdK25+XuoIFUtpo+QUZmwPo+Q6PkwO923iKKdK25+XuxWLJ:56wv45KkTXYFUtppQU/PpQ6P5L5KkTXp
MD5:	BA2A84A534A0B12130D7D7CBE31B8430
SHA1:	97E295357B5503952B617D931E850D0EFBFC6CBB
SHA-256:	155862B8B0680D5160E7AF2D50FE512BB586AD958D73841612DB853513842078
SHA-512:	776DAE6F5818742D996F4138473F79C4DCD822D71E8E612DA65DA35E26D3E1104DD0238922B531655F88169E1A493F8C9BD7E35CD3BB996361B832F68A84BD44
Malicious:	false
Reputation:	low
Preview:	2021/07/15-19:01:40.627 1b14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/15-19:01:41.094 1b14 Recovering log #3.2021/07/15-19:01:41.184 1b14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.229882524098286
Encrypted:	false
SSDEEP:	6:mV+L9q2P923iKKdKWT5g1IdqIFUtpo+L6ZmwPo+LzEkwO923iKKdKWT5g1I3ULJ:5pv45Kkg5gSRFUtppG/PpE5L5Kkg5gSu
MD5:	2CDA6663044231FFC946689B34DFB14E
SHA1:	88B63DED9C089AADB196E051AA241F865D9ED8A7
SHA-256:	B9039CCEDB8EE4776A67F7993865A929D34B7CB3DB356F9414E4FD9E7A26A585

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
SHA-512:	6F264AC914A8A8EDD430618B67FBCED81361CEACD91CDA674563E74B26739C9AAE3C3E18B3C2B64B071792892CCF6B149CA41360DDC637CA3AD8D2A15570C07
Malicious:	false
Reputation:	low
Preview:	2021/07/15-19:01:40.595 1b14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/15-19:01:40.614 1b14 Recovering log #3.2021/07/15-19:01:40.616 1b14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.227504140303365
Encrypted:	false
SSDEEP:	6:mHKRXQRGSQ+q2P923iKKdK8a2jMGIFUtpGKf3pgZmwPGKfaQVkwO923iKKdK8a23:XGRGSQ+v45Kk8EFUtpnfZg/PnfaQV5Ls
MD5:	41BA6916FC9D1AC71E6C4711CE8F800A
SHA1:	C9F3B5A0D55C237055DF3E2C11DE786A2875ED51
SHA-256:	8552332629A213695828797F2EF1BD5F10B94502E91BBCCF362087E1D80FC90B
SHA-512:	ED07D9EF6EE31D0F39CE327AA346F19969832D57675ABF831F9E11907EF8FB8281C181A6E5098CCD1CB2570EEA9B99FCC5BB376E716CCCBF65FB9E9693DCAA17
Malicious:	false
Reputation:	low
Preview:	2021/07/15-20:49:33.863 154c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/15-20:49:33.880 154c Recovering log #3.2021/07/15-20:49:33.883 154c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.202525515791682
Encrypted:	false
SSDEEP:	6:mH5SQ+q2P923iKKdKgXz4rRIFUtpGRgZmwPGRQVkwO923iKKdKgXz4q8LJ:oSQ+v45KkgXiuFUtpeg/PeQV5L5KkgXS
MD5:	017D3E7C3D936EBC89ADA489D27CB1C4
SHA1:	1B932B124FB34711A2F3C57411711F5154A2022C
SHA-256:	332AEB872CE82595800FF7068C3D2EEB8702ADF61D50FD60C0511E0FE5B041AA
SHA-512:	CD089ABA2C72B284F2F9F01223D487826D93E598050A6F121411B0D13E88333C8293F653A8A1F38A4DCF58DC44255E98088C87CD3BED5C18F1BC6EE7771F7E8
Malicious:	false
Reputation:	low
Preview:	2021/07/15-20:49:34.171 154c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/15-20:49:34.174 154c Recovering log #3.2021/07/15-20:49:34.174 154c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	1.0116363507219235
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoj:wIElwQF8mpcSJ2Y/1
MD5:	7C43C7D37ADE15C5B7A2548F1F902487
SHA1:	0C81EE0FE2B03869B68F32A186A3A953BAB2C9BB
SHA-256:	34413CAA2D1D6680A2D9DAB0FC7105F2F4FAE0F720A592FBDB974CF6E805B20C
SHA-512:	5AA7CFF7DD51CF2A7E383DA304DC3BAA751D6642D961122CD5884A624C2D455CF61830D358275AE4F07D1724C2665E5D550AE717F4D1410E6993021F580E1B9
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):	0.8255198231026499
Encrypted:	false
SSDEEP:	48:dIvqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUb8t6:dIvhIElwQF8mpcS/8w
MD5:	F3445124D19298430508B56A52E05969
SHA1:	9312A786F356E4FCC0BD7932D4E0B5CEFDE5E99A
SHA-256:	D04D8FCCF4EC6DDE71C712168504397FCB671BC784FE06F4368E995CDB57974D
SHA-512:	332CA0D36D6A4B4FB1D69C6083DE3CEFBE6C9B982F191DD61F3A0E7CEA496D7EAD4C2F995BE16B0F8360D4DD49BAAAE8D59179CA17F7D4668B8D5D446E09(A48
Malicious:	false
Reputation:	low
Preview:	.....7..... ....

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
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):	5.161467199306507
Encrypted:	false
SSDEEP:	6:mHB7+q2P923iKKdKrQMxIFUtpGD5yWZmwPGiBFNVkwO923iKKdKrQMFLJ:u+v45KkCFUtpscW/PlzNV5L5KktJ
MD5:	BAD8EF6D5FD282F5F8DF497598E61768
SHA1:	AEAA724D00720B4B1611CA7D1C4585A4EC1AEBFC
SHA-256:	CC824A0CE4C74737614B5D22EF1725BAD52A8830D772010E508B627E29A970A4
SHA-512:	A431BA05C7FB9C687C74C4B3804B075660D54069075089FCA500825D121AE8B67318A92A8FDCED53B283894DB4145DBD9DA811FAE8C7BE1EA18C8476497F653
Malicious:	false
Reputation:	low
Preview:	2021/07/15-20:49:34.071 f3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/15-20 :49:34.073 f3c Recovering log #3.2021/07/15-20:49:34.074 f3c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	347
Entropy (8bit):	5.208705737400781
Encrypted:	false
SSDEEP:	6:mHKX8Iq2P923iKKdK7Uh2ghZIFUtpGKXeZZmwPGKVezkwO923iKKdK7Uh2gnLJ:XXFv45KkIhHh2FUtpnXeZ/PnYz5L5Kks
MD5:	D55CD06FBF064367485CDDC00864DBE2
SHA1:	549E716D688BE4BEBFA7E7C3B8E3AFF728B89295
SHA-256:	037C3CA0A18834D7D371FC7BE24D4B0C9B8F6F4581C684AC01257CA976C5303D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SHA-512:	2FCA69A37A1FE18D2C0C46CEEB6CCE736B28F2CE6F3A451D2F4F6B0E167C24609C5F04D1F7171ECEF2E285896B3DB8EFB14BFC228A1A5FAF3B6E128E1FFCB1CE
Malicious:	false
Reputation:	low
Preview:	2021/07/15-20:49:33.800 1d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/07/15-20:49:33.806 1d4 Recovering log #3.2021/07/15-20:49:33.826 1d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\0c349248-2579-4279-9c09-1b1ace5f1999.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\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.290026424895814
Encrypted:	false
SSDEEP:	6:mHdN+q2P923iKKdKusNpV/2jMGIFUtpGZFZZmwPG+VkwO923iKKdKusNpV/2jMmd:/v45KkFFUtpQX/Pd5L5KkOJ
MD5:	2AC5C9878219EFC2B0778BC655759BE7
SHA1:	540FAC59E72321A4B06016A2AA07B2EFC35ACE34
SHA-256:	6E115E8FA32F9FE29E743C0FA31747D95FD4E931DFEEF3D0C475EC65D3874F75
SHA-512:	2752620646D8B7B17841D5B5F3BC8D3858EB17CE437E217EE34739DAE129312767DFE67A48A36C5F0E76A02C5E9029D0AF7E46F3E6E1C6EF0E7A928BED0BB882
Malicious:	false
Reputation:	low
Preview:	2021/07/15-20:49:34.114 1548 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/07/15-20:49:34.116 1548 Recovering log #3.2021/07/15-20:49:34.117 1548 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.308534091959429
Encrypted:	false
SSDEEP:	6:mHEVq2P923iKKdKusNpqz4rRIFUtpGogZmwPGoIkwO923iKKdKusNpqz4q8LJ:TVv45KkmiuFUtpPg/PPI5L5Kkm2J
MD5:	A7DF9646AA88EB47E2841F914458F9D2
SHA1:	ADA9803A6A9A2CF4C861A75527D7196E151517C5
SHA-256:	3850D4B1A5BAB50035ABACE1CB68884C62C5282D508D9ECC9AB0F86101741A0D
SHA-512:	59C9C9DCDD7E93CF8B64143C8E082D029D6F21F768D8A275A46899632AA20A859E84AE072E0823A25E2E86D89C6D1D4B125A624131E9CCF7E4420CA20C62379
Malicious:	false
Reputation:	low
Preview:	2021/07/15-20:49:34.172 1674 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/07/15-20:49:34.176 1674 Recovering log #3.2021/07/15-20:49:34.176 1674 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\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.226627929634122
Encrypted:	false
SSDEEP:	12:5fOv45KkkGHArBFUtppF/Pp+5L5KkkGHAryJ:5E45KkkGgPgfPoL5KkkGga
MD5:	7832532E1F15C1D5FD99F7BD9B8E6A8A
SHA1:	CC34F339D3B246A710E3BD702D04E2BF7326E90B
SHA-256:	D84707092B50FA1F7A3873069AF7589D737C8ABB4539A60D4A8EE6893C5E906C
SHA-512:	E34C65276DD52AB7D0E3433AD573B4D029C4CCA8AF7932A698FF39416624F69250CC5D54EB9CA89E898BF9F3F8FA1CE635749124DEDAE5DCA01DB263A137502
Malicious:	false
Reputation:	low
Preview:	2021/07/15-19:01:40.644 1548 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/07/15-19:01:40.646 1548 Recovering log #3.2021/07/15-19:01:40.647 1548 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):	5.206237694316578
Encrypted:	false
SSDEEP:	12:5lv45KkkGHArqiuFUtppS/PpR5L5KkkGHArq2J:5645KkkGgCgfODL5KkkGg7
MD5:	DA201B08C978D65735DDEB62CB3E7A26
SHA1:	BC36C3991C30B5264AEC5B026037DAE512D45597
SHA-256:	8AD0661F57D063F9BB51EB8C8F438408B198D8096045130E5E5C082D6BE77E23
SHA-512:	39A01610825BD5864A4E21E389E296494CB13B1085D1675E3943DDA35E28B0810690539D5525E5476E3C58F2F9301B2C25BEA94F083824412738C0038E4C1308
Malicious:	false
Reputation:	low
Preview:	2021/07/15-19:01:40.643 1d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/07/15-19:01:40.644 1d4 Recovering log #3.2021/07/15-19:01:40.645 1d4 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):	323
Entropy (8bit):	5.271756010222749
Encrypted:	false
SSDEEP:	6:mHKTKL+q2P923iKKdKpIFUtpGKYz1ZmwPGK/jLVkwO923iKKdKa/WLJ:XTe+v45KkmFUtpny1/Pn/3V5L5KkaUJ
MD5:	23839646CD28A27AC8A0FA2B657A9EF9
SHA1:	3C36EC5CC28A3FA6BC4D7169C661FBF39EA5020C
SHA-256:	A9ED7228F0CDC0805A9BB31F1E273E0F4822DFC594BB61FC6DB25C53D93E76C8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG

SHA-512:	8440B55BAD61F5AE8C555998520E2A6CE34F4FAECFBBAF27E8584C4C13F1E6FA9FBC1541E664707251DECA471916675188900BDA10EF7BBDD909DB012129FBE F
Malicious:	false
Reputation:	low
Preview:	2021/07/15-20:49:33.849 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/15-20:49:33.854 87c Recovering log #3.2021/07/15-20:49:33.857 87c 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:	modified
Size (bytes):	401
Entropy (8bit):	5.307763959579279
Encrypted:	false
SSDEEP:	12:5JCv45KkkOrsFUtppJb1/PpJU5L5KkkOrzJ:5JI45Kk+gfJbfJeL5Kkn
MD5:	A02789255A7DC3006711DF792054FA7B
SHA1:	2075DD8A3BA4DB6D89D25F1BF98C96D52FC51274
SHA-256:	6BD621978BB3F1F45DDE0BE52053CBEFBA20ACE87089FEDF61777514C5B1AC1A
SHA-512:	39B991FCD39B2063E1F9FEA5B3A7277289F507D11C7F4C9B00AA721A9DF28B3981ABF7BDE43AA2BD12AA73CA3AC0A6E7EB6E11B5B8141A14FC55A2C53FED9 C79
Malicious:	false
Reputation:	low
Preview:	2021/07/15-19:01:42.114 3e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/15-19:01:42.116 3e8 Recovering log #3.2021/07/15-19:01:42.117 3e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cd2515be-85df-4552-9f7c-9a30c6d411c1.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d3b4f4d6-622d-4fe4-a5ec-4d3e478e0c25.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):	4778
Entropy (8bit):	4.94051992711574
Encrypted:	false
SSDEEP:	48:YcClklSiklqecBqAJdqTlYclQKHoTw0h1aPc8C1Nfct/9BhUJo3KhmeSnpNGz0sQ:n/r1oGMpSKIEIk0JCKL8xpbOTQVuwn
MD5:	32BB78BD914217CAFC075CD992E42163
SHA1:	1BD7073688160F8BA7DFABDD4C77268DE6FA8DE3
SHA-256:	EC1F505281CF725A0BEA837320394AD3712AD3FF3558F08CD70842AE08DDE2CE
SHA-512:	3C2C6ED3C352B360920B41C94DF51446AF19F6C779E6AA1079AAF3050FCC1DE97E4DDA61364FF790B64157222BC1917D1FEFE1C1A447889ED7E1E9C0C4EA44 9
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270880974135867","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","1538886"],"daily_received_length":["0","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\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.537850386961684
Encrypted:	false
SSDEEP:	3:tUKgVN2SgZmwv3GV1cR70V8sGV1cRQQFO0WGv:mHjZgZmwPGDA0VvGDvX0tv
MD5:	6229C7D9BA8FCF55447D7A7CEA6A0DAE
SHA1:	278638682D7A2D8880EFF5EA40B10CE097F60D23
SHA-256:	5EBC1B186D6853A6FFCBDFB7EC2A33EF9BB6C9D1122561CB00BBF48005C60C73
SHA-512:	590CC94FFB52ED95DFF438DFA55CE5DB543C07E5D866FC3906C15B81DEAEB0F16593F159838D0823054E3C2E1363BECB5F75D2E63D0F75EB89502C294F2C71 8
Malicious:	false
Reputation:	low
Preview:	2021/07/15-20:49:48.681 1228 Recovering log #3.2021/07/15-20:49:49.944 1228 Delete type=0 #3.2021/07/15-20:49:49.945 1228 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	337
Entropy (8bit):	5.237086807408815
Encrypted:	false
SSDEEP:	6:mV+Q/jL+q2P923iKKdKfrzAdIFUtpo+QHFz1ZmwPo+Qas4jLVkwO923iKKdKfrzS:5Qmv45Kk9FUtppQH11/PpQ54F5L5Kk2J
MD5:	E1C4D8A17C155CFC3E481B90682E57CA
SHA1:	C61FFE3D38E544DAC964989FAF91C33263B73BFE
SHA-256:	7560F2EA209C49AD94D721270FFCB4103B2B2761AAAFBFDC523D26FE37AA7EFF
SHA-512:	9413E64B7FF0B41038A630AD93D88C5685FD850BD115E22907C5AAC533A9D8A434A38FA6335BB64CBB71BA03AE815ACF5536DA163BF1C3C973F7652F40CF712
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Reputation:	low
Preview:	2021/07/15-19:01:41.446 3e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/07/15-19:01:41.464 3e8 Recovering log #3.2021/07/15-19:01:41.465 3e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Temp\2750ee0c-a433-4add-a1ee-e1c4fbc1b59c.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\94cd6afc-499f-4d1b-8dc2-c8cfaa757483.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

C:\Users\user\AppData\Local\Temp\94cd6afc-499f-4d1b-8dc2-c8cfaa757483.tmp	
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):	6222
Entropy (8bit):	4.644405279037576
Encrypted:	false
SSDEEP:	192:KXCXgy+dkX7XQXlkfe2HfYyWysDidjJj4GEM:jI9kG2HfYyHysjl3
MD5:	BDA2E1A370A6DB80B30847DED02D38D9
SHA1:	9232FCF7AB442732CDB11DEE8892D812F434412A
SHA-256:	BF4A801AF75B18A40413B34B73F1E100371A9CC67FFCF07C5D935962EEE1C855
SHA-512:	D85345D8F538BAE91329E4F22250F888AFB4A50597C9AB0CD487A52C7846ABF0707C618C30736A80B0496C296788D15FFB53676DEEAC0E90FBD40B900FA0E347
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET f51c23192e4dcfbb7c33693f081ad7df9237b0aa780505dc20817b12e55c7222 836bc84e8c43c6b21a9f67eb47fae50fa592ad2cfebcd6e48631ce7fcc7c6af4.SERVER_HANDSHAKE_TRAFFIC_SECRET f51c23192e4dcfbb7c33693f081ad7df9237b0aa780505dc20817b12e55c7222 0f77b38353de2ab64f8d11a216fa7ed4b72f4714ce811ddfa925c3e2f3ecfe76.CLIENT_HANDSHAKE_TRAFFIC_SECRET 9f6ff44fdb78c50509299075470448f2410ddae0ac9c775906e23903314f21e6 b4a5f5ea5f1bf1cad560fde1bafd5f57de2e7c7c471af837db231af4cdf26ba1.SERVER_HANDSHAKE_TRAFFIC_SECRET 9f6ff44fdb78c50509299075470448f2410ddae0ac9c775906e23903314f21e6 1e0c404fa44a49e40cf3c446670329e464384d40501c00053944c77f73ffef58.CLIENT_HANDSHAKE_TRAFFIC_SECRET ccf0a3280b4abde05f4e3a8438e7ecbde7fe0fde09edf42e953fd758b0a472fa 6dc4a5486977cf4d8a6cb3c5f95f2a1671dd1dc3af304c5bf16d551461a08206.SERVER_HANDSHAKE_TRAFFIC_SECRET ccf0a3280b4abde05f4e3a8438e7ecbde7fe0fde09edf42e953fd758b0a472fa e169783b4a5db9d8b1d30bb89f0c576ee9d25fc7d3ca6a90778ee14b59597718.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\eb6f4f72-ac3f-4664-a6f7-9c111c23d08a.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.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\eb89fec9-2c10-4d28-8437-9db3dbaee116.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
Malicious:	false

C:\Users\user\AppData\Local\Temp\eb89fec9-2c10-4d28-8437-9db3dbaee116.tmp	
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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_dir5428_1093469420\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".. },.. "craw_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 completed.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\ja\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome ....."... },.. "app_name": {.. "message": "Chrome ....."... },.. "craw_app_unavailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "....."... },.. "iap_unavailable": {.. "message": "....."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Chrome ....."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome . ... .."... },.. "app_name": {.. "message": "Chrome . ... .."... },.. "craw_app_unavailable": {.. "message": ".. .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....."... },.. "iap_unavailable": {.. "message": ".. .. .."... },.. "jwt_retrieve_failed": {.. " message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Chrome. ....."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\lt\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):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344 4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema"... },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema"... },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima."... },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo."... },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome.."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\lv\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):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma"... },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.ma"... },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama."... },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu."... },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami."... },.. "jwt_retrieve_failed": {.. "message": "The transacti on could not be completed."... },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\nb\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\nb\messages.json	
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCE
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app _unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap _unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\nl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A A7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\pl\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):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfiIu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOfIC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B7 77
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be com pleted.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\pt_BR\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):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\pt_BR\messages.json	
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw _app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.".. },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede.".. },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\pt_PT\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):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTnPlOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F 4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\ro\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):	4.61125938671415
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hI3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "cr aw_app_unavailable": {.. "message": "..n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be c ompleted.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\ru\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):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSl3ZGG7OJHZMSl3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjT03On:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F6 2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\ru\messages.json	
Preview:	{.. "app_description": {.. "message": "..... ....-..... Chrome".. },.. "app_name": {.. "message": "..... ....-..... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "..... . .....".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... . Chrome.".. }.. }..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\sk\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):	4.640777810668463
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOfTYCUAi0D:1HEl4G8WYpetPmD8ZpcH7aOGAOfzUeD
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E595D
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": "Aplik.cia moment.lne nie je dostupn..".. },.. "craw_connect_to_network": {.. "message": "Pripojte sa k sieti.".. },.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\sl\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):	617
Entropy (8bit):	4.5101656584816885
Encrypted:	false
SSDEEP:	12:1HEJGcyvmbZGGGcyvmbZ+WYpU34OBOEtf+dgca1ZO8ZpU34GcQArERff03OyZnLh:1HE4cyY4TcyY8WYpNoWa1w8ZpQcQ6AfK
MD5:	3943FA2A647AECEDFD685408B27139EE
SHA1:	0129DD19D28373359530B3B477FE8A9279DABB7D
SHA-256:	18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
SHA-512:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DECD
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailable": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prijavite se v Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\sr\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):	743
Entropy (8bit):	4.913927107235852
Encrypted:	false
SSDEEP:	12:1HEJssbdOGGssbdO+WYpU347xBP+dgcucO8ZpU34s1muP03OyZnLAOfTYzDYD:1HEKsb59sbTWYplx4Xud8Zpy1mNOGAOv
MD5:	D485DF17F085B6A37125694F85646FD0
SHA1:	24D51D8642CDC6EFD5D8D7A4430232D8CDE25108
SHA-256:	7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818
SHA-512:	0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E7
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_dir5428_1093469420\CRX_INSTALL_locales\sv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\sv\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	630
Entropy (8bit):	4.52964089437422
Encrypted:	false
SSDEEP:	12:1HEJJMkbGGJMkb+WYpU34OACwz+dgNPGFZO8ZpU34JgpXLSb03OyZnLAOfTYLdID:1HErMkaqMk6WYpTOcb8ZpDgdZOGAOf8Y
MD5:	D372B8204EB743E16F45C7CBD3CAAF37
SHA1:	C96C57219D292B01016B37DCF82E7C79AD0DD1E8
SHA-256:	B8BA77E0089B0676545EC16D32468B727812B444F90B33A7A5B748E6C36C4388
SHA-512:	33640529E0D5DCC5CA4BDB0615A2818E8D26C6FCB7B3474C08AC3EB67B9DB40E1F0A79954ED20728CD47A686D2533DCBC76ABCBDB917F8530C8DE8BBA6873 2E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "BetaIning via Chrome Web Store".. },.. "app_name": {.. "message": "Betalning via Chrome Web Store".. },.. "craw _app_unavailable": {.. "message": "Appen .r inte tillg.nglig f.r tillf.llet.".. },.. "craw_connect_to_network": {.. "message": "Anslut till ett n.tverk.".. },.. "iap_unavai lable": {.. "message": "Betalning i appen .r inte tillg.ngligt f.r n.rvarande.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logga in i Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\th\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):	945
Entropy (8bit):	4.801079428724355
Encrypted:	false
SSDEEP:	24:1HEKa1dDa1/WYp6UFi72SmlG8ZpyactrW2SAOGAOfvSLD:WK2DNYp6U4y3bpyLxwGFW
MD5:	83E2D1E97791A4B2C5C69926EFB629C9
SHA1:	429600425CB0F196DDD717F940E94DBD8BFF2837
SHA-256:	2FECA577F43D97BAEEA464741D585892103585208FD0A935B810A03BDCE83C88
SHA-512:	60A5928DAA8CB4341487F477C56B5A98B83EDE50E5F4F55A802E01FDDAB86F3E795D391953D3D9214552D14D3F58C5A183693C613720FC12FC387D7B8F9B9AB
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_dir5428_1093469420\CRX_INSTALL_locales\tr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	4.710869622361971
Encrypted:	false
SSDEEP:	12:1HEJ9Y8GG9Y8+WYpU34wWT+dgGb0GO8ZpU34wryd7T03OyZnLAOfTYGbPKG:1HE0jWYpyRnG8Zpyr/OGAOfFPn
MD5:	2CEAE0567B6BB1D240BBAD690A98CA3B
SHA1:	5944346FBD4A0797B13223895995CAB58E9ECD23
SHA-256:	A7CB86F30C9C31FE5540282C308BA96ADB4EC16EF98C87129EB88105E5BEF5FC
SHA-512:	108A07C6D03D7178E8D0FFEF5349E0249A898D864964FED8757BD8A08BC1C6D9613F2A6C01AA34A6606127D1C6CE14C229FA02586677DBB060B85E3E845950E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "app_name": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "craw_a pp_unavailable": {.. "message": "Uygulama .u anda kullan.lam.yor.".. },.. "craw_connect_to_network": {.. "message": "L.tfen bir a.a ba.lan.n.".. },.. "iap_unavail able": {.. "message": "Uygulama ..i .demeler .u anda kullan.lamaz.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.tfen Chrome'da oturum a..n.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\uk\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):	720
Entropy (8bit):	4.977397623063544
Encrypted:	false
SSDEEP:	12:1HEJ7wILkSlXZGG7wILkSlXZ+WYpU34zb1Oy2P+dgSV1EjiTO8ZpU347qtfP2CTW:1HElwEkK4uwEkK8WYpd/dTV1e8Zptq5S
MD5:	AB0B56120E6B38C42CC3612BE948EF50

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\uk\messages.json	
SHA1:	8B3F520E5713D9F116D68E71DAEED1F6E8D74629
SHA-256:	68ABA284751EB9C856032062EF9B1651E2A1E5CE5FDA0977FFC97D63BA7BED9E
SHA-512:	CD852A58217F739C1CD58567FF432D31A7AD3F68C884ABBA1DA95799BCD1545C6A5D3B06F319681C12B78AD0A709828DE4B22736316F148D21F5DB76A5BCCB F
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_dir5428_1093469420\CRX_INSTALL_locales\vi\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):	695
Entropy (8bit):	4.855375139026009
Encrypted:	false
SSDEEP:	12:1HEJMAZrSFZGGMAZrSFZ+WYpU34WFHoz+dgdklzoO8ZpU34NFHoz03OyZnLAOfTU:1HEl4B8WYpAKytFZ8ZpXKMOGAOfd6D
MD5:	7EBB677FEAD8557D3676505225A7249A
SHA1:	F161B4B6001AEAEAB246FF8987F4D992B48D47BE
SHA-256:	051F96ED874C11C4A13589B5F68964E4F5B03B52DDA223D56524F2CA23760C04
SHA-512:	74FD267CF7E299FB8E7054605C3F651F057F676FF865082FA24F4916755456768DB0DA62DBC515D829B48AB1F9CFC8AD3E841DCBF1F194D5CB14C5335A192A0
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Thanh to.n tr.n c.a h.ng Chrome tr.c tuy.n".. },.. "app_name": {.. "message": "Thanh to.n tr.n c.a h.ng Chrome tr.c tuy.n".. },.. "craw_app_unavailable": {.. "message": ".ng d.ng hi.n kh.ng kh. d.ng.".. },.. "craw_connect_to_network": {.. "message": "Vui l.ng k.t n.i v.i m.ng.".. },.. "iap_unavailable": {.. "message": "Thanh to.n trong .ng d.ng hi.n kh.ng kh. d.ng.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be compl eted.".. },.. "please_sign_in": {.. "message": "Vui l.ng ..ng nh.p v.o Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL_locales\zh_CN\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):	5.210259193489374
Encrypted:	false
SSDEEP:	12:1HEJ01GG01+WYpU34zeHz+dgfO8ZpU34YKiO03OyZnLAOfTYB6U:1HEplWYpISv8Zp+JOGAOfa6U
MD5:	BB73BF561BB79F89D9BF7C67C5AE5C65
SHA1:	2FADD3A1959B29C44830033A35C637D0311A8C9C
SHA-256:	D804F2A040D21D7511EFD5213D8E1721D64964A1A0DBB48E21622CEEDC9D967E
SHA-512:	627D44CEF1FE5C5ABD598BD47FF5E22B9EFC1CF98DDE3868FA9E5896C134A0C9C055AC34EDDADAE56B6690E51AEA89965D38F770552A85C732CC796795DC6 D2
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_dir5428_1093469420\CRX_INSTALL_locales\zh_TW\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):	634
Entropy (8bit):	5.386215984611281
Encrypted:	false
SSDEEP:	12:1HEJ2j62GG2j62+WYpU34m7T+dgc8nOO8ZpU34mvIO03OyZnLAOfTYAuH:1HEuSZCWYpsStwP8ZpROGAOfCH
MD5:	5FF50C673CC0C661D615F0CFD0E6DCA0
SHA1:	60DFF98DEAB9C4746B288BDD9C94B3BCAE5EAA85
SHA-256:	C6F8C640F3353A7B9B1432A0C139C1AEEC40133800E6C9B467B63991AD660308
SHA-512:	361D62D91F4931C5F34092C9F2C6A5323D5EEB82A24E7ABE11F7817D8D66341C0ECAD4DCB4B10873920C8D6A3CC9F5704889E178EB2549001A9F62BEDF6C801
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_dir5428_1093469420\CRX_INSTALL\images\icon_128.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4364
Entropy (8bit):	7.915848007375225
Encrypted:	false
SSDEEP:	96:YjlLDJjTvXUtNvX8dgb9HT6y8nviyHG5iCRYtIP:YtNTfUzvX8KM+MGRsIP
MD5:	4DBC9F9E6F5A08D299BAC9E54DF07694
SHA1:	BB38F5DE34B1E0BE1109220BA55271087A4D9EA5
SHA-256:	91C2718DD23B4356D71F88F6146868369033291086DF327534546DFA459BEB0E
SHA-512:	A5F2B1F47502836130D8083F757B7773C1E1CB36B76AD298CC29AB2B428C8002D2F15BD839838FC326DAC3681C2F48AB25A3E7631D33726C4B25E8EC14170912
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a.....IDATx..yp.....gF#.:.[H.l.l..8...`/.k....,!a7Km...E...Te..T.....J...p....%.(....+...3....eY.e...L.o...5....h4...\....{?....~.u.`0.....`0.....`0.....`.Y.....[(.....).4....a i..w38.+....Bf././..]...{.....8...3.....3W~OJ.. /...u6V.C..U.0.+._=.c..9.X.?....L....S@.L...m.0..>.C...L|TF.p5..f4M.,.V....8..a.<...RP..@)E,..E"...h.....!...-....,I..T.....m..._[[{w{{.... {*.^.....M.x..h4.h.....\.R.E....j).7.....h4.A.E....,. ...iii.Vj?2...=/.B.FK9P..@)=Rj..D".Y...2.B..x.}0...&J...2.....f.O..e.H.....!.J)'I..R....B.....QJ;K..L...L.l".L~mhh.R.@).FFF ~.L&...~.B.....u.....}.....~.....f..yUU.....^M...6.....].,w.e..~.!$.C.R.....E(%e9.,....k..@...W8.....@.....O..@%.~..@.S..P.....`Tp...."...?ME..c.....s...`..S1...7.b..aNE..k...3 .yP.}.Ch.}.....B.....IPE..C.<....T....k.....Z..o_.....g.....P..A=y.J.)h..@.q.-.*].AU.4...F.M.....y%B]+ .\.~..9.....:.=...r.....E].o...F..P.....i...|....

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL\images\icon_16.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	558
Entropy (8bit):	7.505638146035601
Encrypted:	false
SSDEEP:	12:6v/7vyVgSKYsfFzXxXsrPfA+b0YX+5IOUWCQKznuow7:6yVnKYsfFzhXsrIq0YXmgQGn6
MD5:	FB9C46EA81AD3E456D90D58697C12C06
SHA1:	5FC450F7D73CCFAC8F0D818CB3392BA4D91B69DE
SHA-256:	016CA659BA080E194FBFC0929602B16506ED60AA6019FAA51410C4FD93B583E8
SHA-512:	ADD810EE9EB7CAEC505B5FD90A1F184CE39D8F8C689DCC240F188FE353B9575489492E07D572A3B1C11A1555CE66AFCA5134903E4C1AA3D54BC7C5ED3E65B 0C
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDAT8...Mk.Q...;... .....F..QW.....F....J.?.w..7~.....'.Q..B]... .QS...M&_w..b&.|`.....p...f.?.D$.y^.....y*...\..Z..t6..oRj.@&.u..G.qN).t.-V*.>(.N .Ep]wFk.60o.]0.`Y..cT..Y.Tb.`DF.d..s.Z..E..9.4._C..._...%..*.^....4.I...Y..X..R..../...Wj+w0[.]..._B.k.${.\.>.%.....lz .w.ALxo.2;..a...".p..S..&..uXS...<..6..[..zD.._.N+w.WbM7y e6X<...'(,=.r}.....$f..5..P....k..."..8.s.<zgSm@.....).Y.....:e..\|.....F...I..A$.....T?.....m....8.....N...z.....V..vd.h'....C.?.....H.;]..C.M.....9.b.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\CRX_INSTALL\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1322
Entropy (8bit):	5.449026004350873
Encrypted:	false
SSDEEP:	24:1HEis7ViC/yox/fiqeUoLFlmF1s80FKrGfd0d3NZNZx1Fq7eY7nfj1B:WL7V2opiV1mvs8rxTZRczhB
MD5:	01334FB9D092AF2AA46C4185E405C627
SHA1:	47AD3C0E82362FFE5B881DF8D71D6F79AB7F5796
SHA-256:	F52714812D68C577A445169D11E84DF6751C2D6886BC429643072BB5D61C6C27
SHA-512:	888D96ADB7A847ABE472145258C8C46950EB2FA3BA7D596C2E90A17C8FB06FD0155C56CC8ABA5D076D89368417464BCB2D236F9E40E53241950A01F9F8ED548
Malicious:	false
Reputation:	low
Preview:	{.. "app": {.. "background": {.. "scripts": ["craw_background.js"].. }.. },.. "default_locale": "en",.. "description": "__MSG_APP_DESCRIPTION__",.. "d isplay_in_launcher": false,.. "display_in_new_tab_page": false,.. "icons": {.. "128": "images/icon_128.png",.. "16": "images/icon_16.png".. },.. "key": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrKfMnLqViEyokd1wk57FxJtW2XXpGXzIHBzv9vQI/01UsuP0IV5/lj0wx7zJ/xcibUgDeIxobvv9XD+zO1MdjMWuqJ FcKuSS4Suqkje6u+pMrTSGOSHq1bmBVh0kpToN8YoJs/P/yrRd7FEtAXTaFTGxQL4C385MeXSjaQfiRiQIDAQAB",.. "manifest_version": 2,.. "minimum_chrome_ver sion": "29",.. "name": "__MSG_APP_NAME__",.. "oauth2": {.. "auto_approve": true,.. "client_id": "203784468217.apps.googleusercontent.com",.. "scopes": ["https://www.googleapis.com/auth/sierra", "https://www.googleapis.com/auth/sierrasandbox", "https://www.googleapis.com/auth/chromewebstore", "https://www.goog leapis.com/auth/chromewebstore.readonly"].. },.

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\eb89fec9-2c10-4d28-8437-9db3dbaee116.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

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1093469420\eb89fec9-2c10-4d28-8437-9db3dbaee116.tmp	
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir5428_1184234559\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1184234559\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0lprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "1282768764603190 75": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1184234559\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1184234559\CRX_INSTALL_locales\bg\messages.json	
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "1550904064710828958": {.. "message": "......".. },.. "1636686747687494376": {.. "message": "......".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir5428_1184234559\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:IPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 15, 2021 20:49:38.094572067 CEST	192.168.2.5	8.8.8.8	0xaeb4	Standard query (0)	www.grainger.ca	A (IP address)	IN (0x0001)
Jul 15, 2021 20:49:49.991151094 CEST	192.168.2.5	8.8.8.8	0x83fe	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 20:49:38.128114939 CEST	8.8.8.8	192.168.2.5	0xaeb4	No error (0)	www.grainger.ca	www.grainger.ca.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 20:49:50.022309065 CEST	8.8.8.8	192.168.2.5	0x83fe	No error (0)	clients2.google.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 20:49:50.022309065 CEST	8.8.8.8	192.168.2.5	0x83fe	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5428 Parent PID: 4992

General

Start time:	20:49:32
Start date:	15/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.grainger.ca/fr/content/covid-19-recovery'
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: 3228 Parent PID: 5428

General

Start time:	20:49:34
Start date:	15/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1576,8722109470797325843,6740444566604102159,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1712 /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