ID: 412647
Cookbook: browseurl.jbs
Time: 20:40:27
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

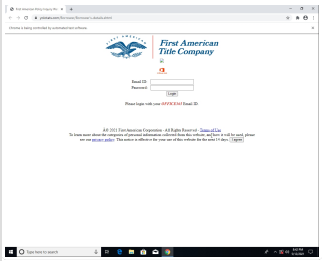
Analysis Report https://yolotats.com/Borrower/Borrowe…

Overview

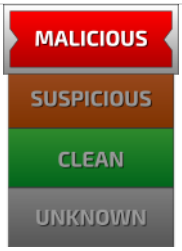
General Information

Sample URL:	http://https://yolotats.com/Borrower/Borrower's-details.shtml
Analysis ID:	412647
Infos:	

Most interesting Screenshot:



Detection



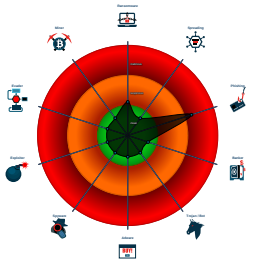
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish10
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 1060 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://yolotats.com/Borrower/Borrower's-details.shtml' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5708 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1704,1686343471565443222,3804912756075544807,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1752 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

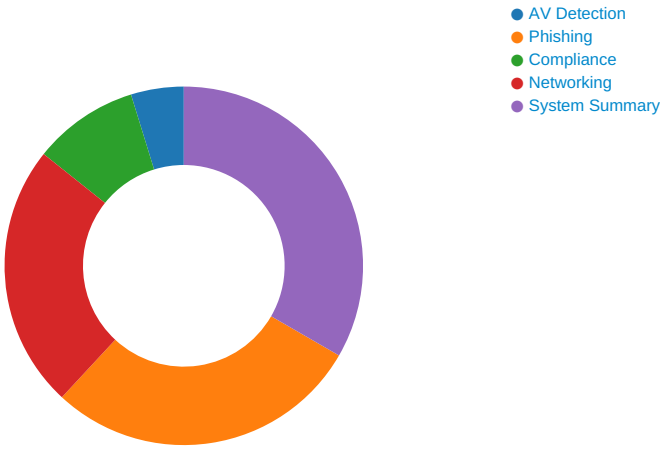
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

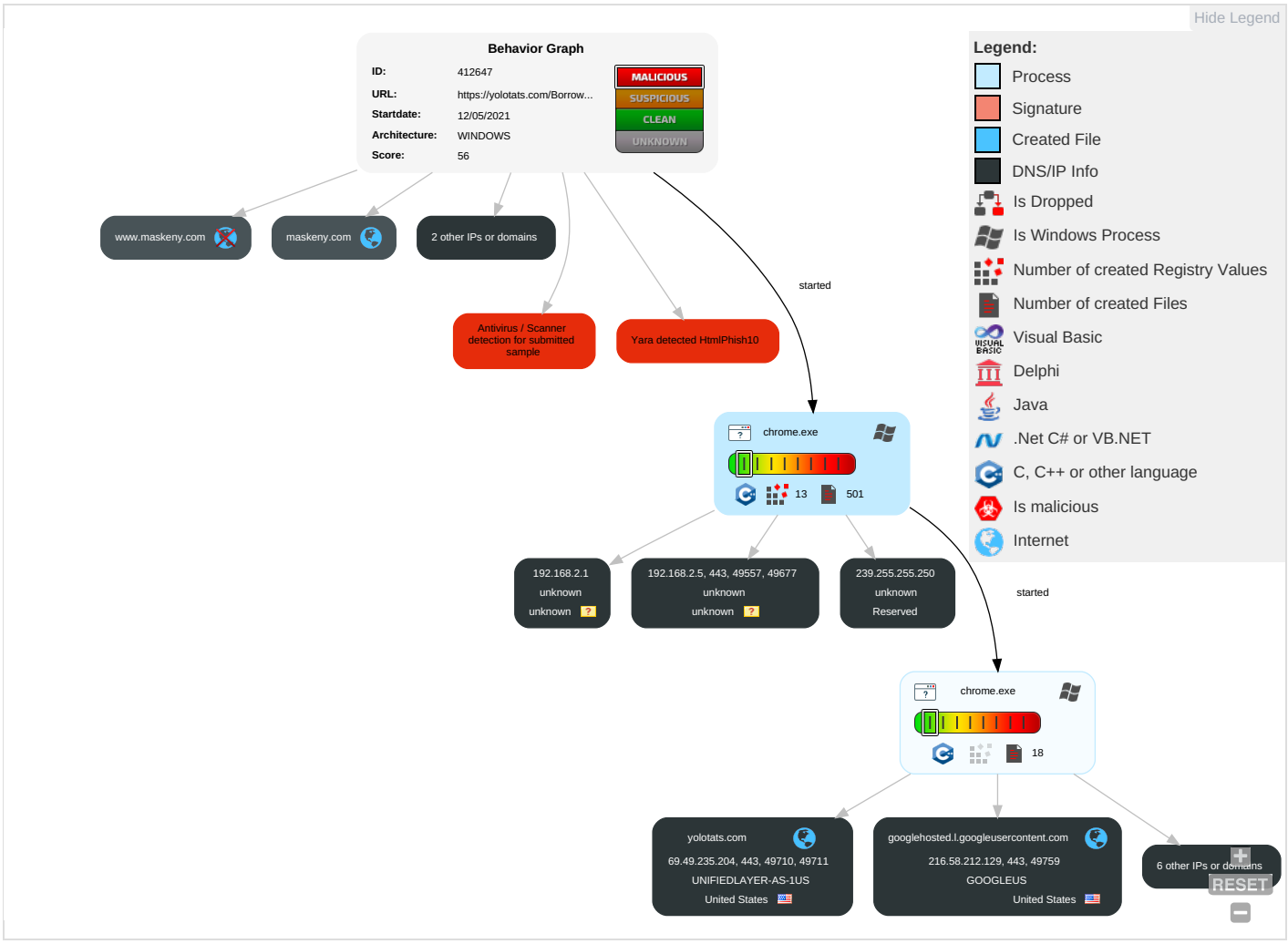
Phishing:

Yara detected HtmlPhish10

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 1	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

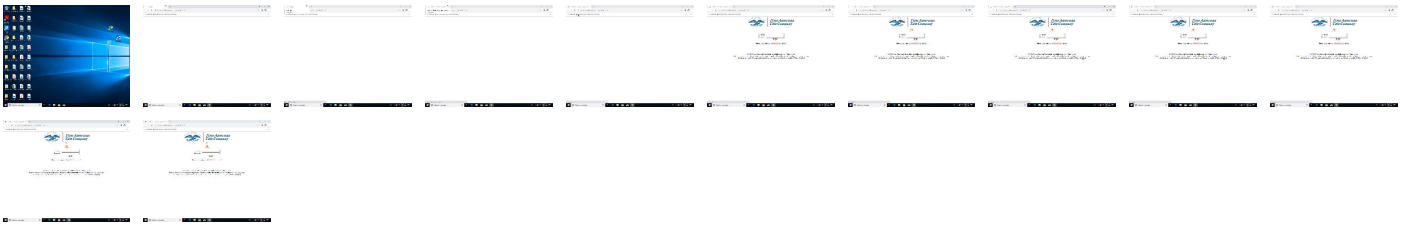
Behavior Graph

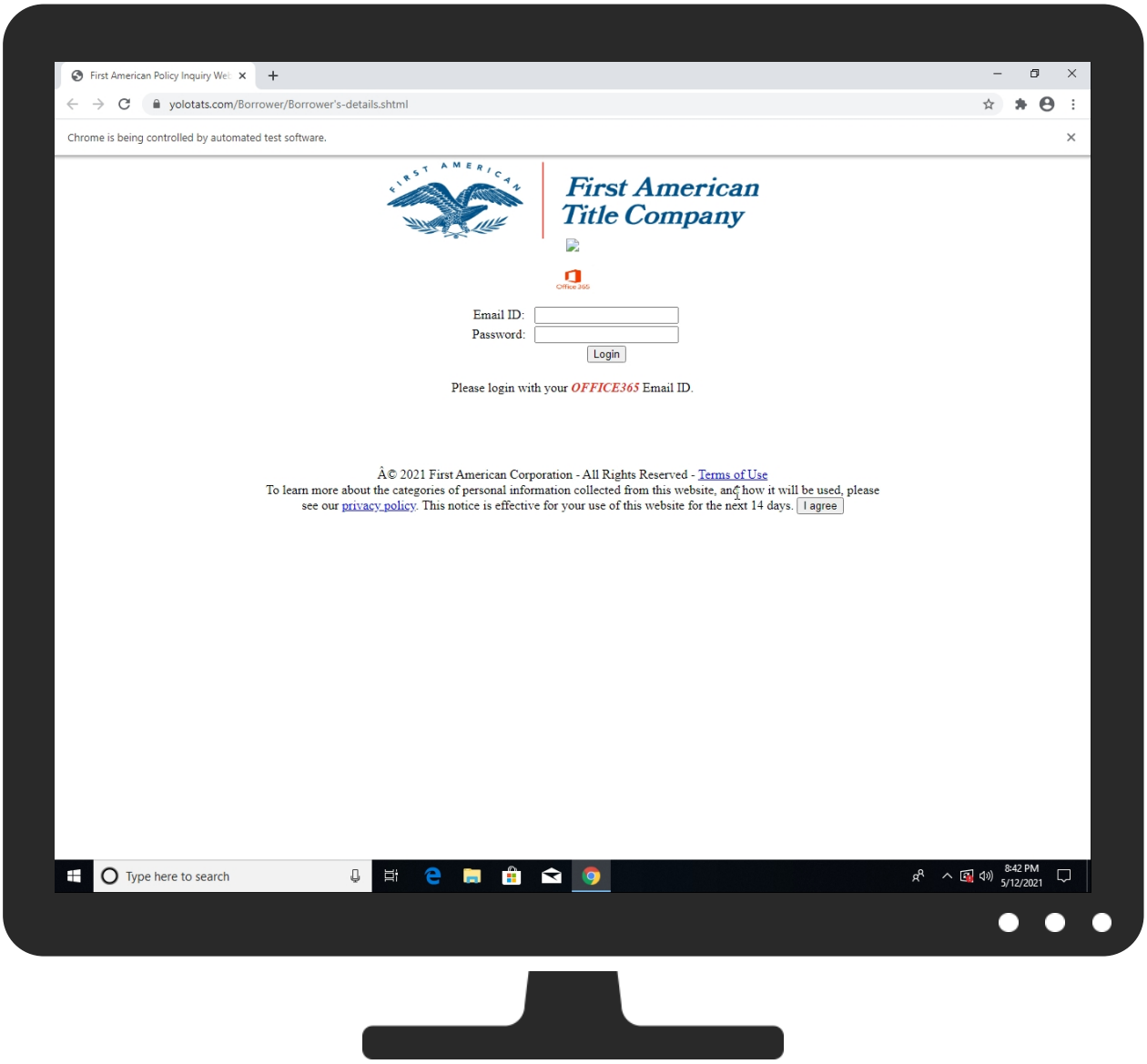


Screenshots

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://yolotats.com/Borrower/Borrower's-details.shtml	0%	Virustotal		Browse
http://https://yolotats.com/Borrower/Borrower's-details.shtml	0%	Avira URL Cloud	safe	
http://https://yolotats.com/Borrower/Borrower's-details.shtml	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://yolotats.com/Borrower/Borrower	0%	Virustotal		Browse
http://https://yolotats.com/Borrower/Borrower	0%	Avira URL Cloud	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://dns.google	0%	URL Reputation	safe	
http://https://yolotats.com/-	0%	Avira URL Cloud	safe	
http://https://yolotats.com/	0%	Virustotal		Browse
http://https://yolotats.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
yolotats.com	69.49.235.204	true	false		unknown
gofirstam.com	104.129.24.42	true	false		unknown
insagent.firstam.com	69.87.16.180	true	false		high
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
maskeny.com	184.175.83.99	true	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
www.maskeny.com	unknown	unknown	false		unknown

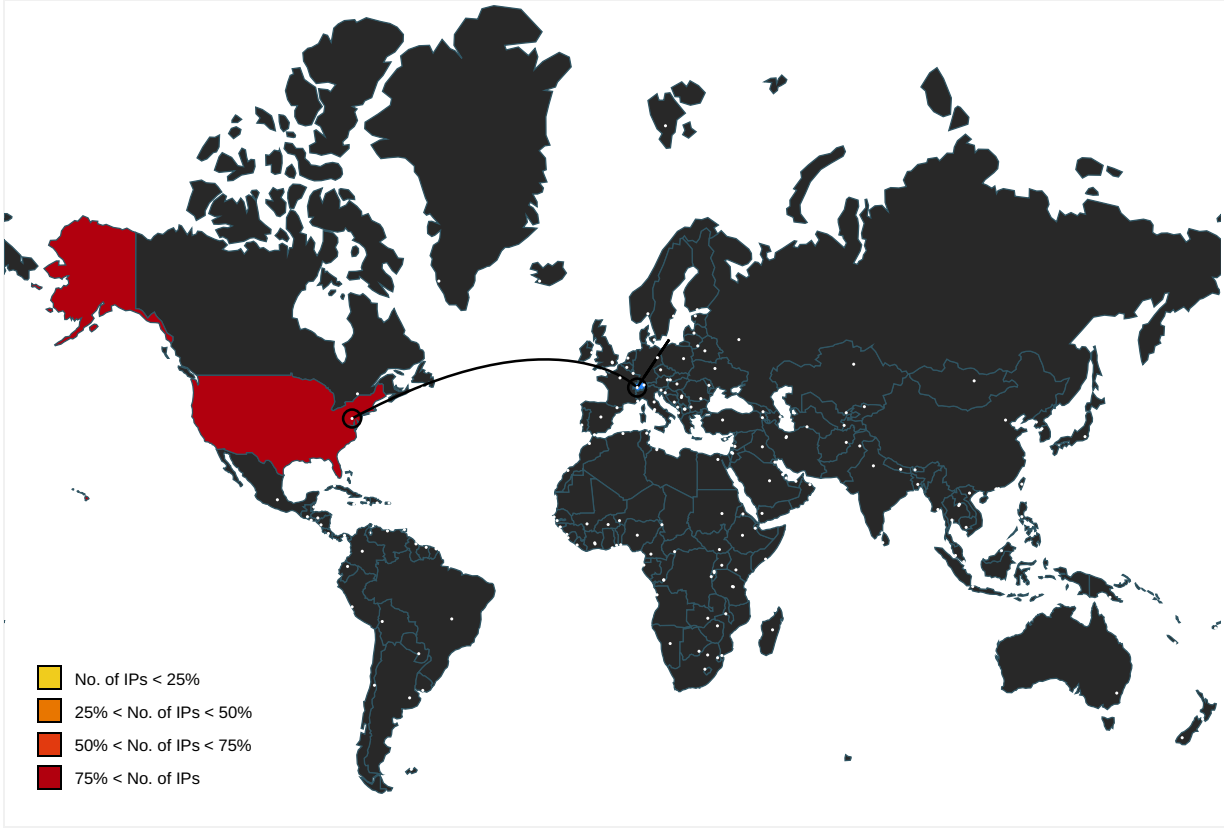
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://yolotats.com/Borrower/Borrower's-details.shtml	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://yolotats.com/Borrower/Borrower	History.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dns.google	7b6f9a58-09a1-4ba0-b1ac-30b1a8005059.tmp.1.dr, 533d441f-2c82-4fb7-b488-51a1d33de4c4.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://yolotats.com/-	080e5d32096294ef_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	7b6f9a58-09a1-4ba0-b1ac-30b1a8005059.tmp.1.dr	false		high
http://https://yolotats.com/	58c452aae925b73a_0.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.129.24.42	gofirstam.com	United States		8100	ASN-QUADRANET-GLOBALUS	false
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
184.175.83.99	maskeny.com	United States		7393	CYBERCONUS	false
69.49.235.204	yolotats.com	United States		46606	UNIFIEDLAYER-AS-1US	false
69.87.16.180	insagent.firstam.com	United States		13782	FAFCOUS	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412647
Start date:	12.05.2021
Start time:	20:40:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://yolotats.com/Borrower/Borrower's-details.shtml
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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@33/211@8/9
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.50.102.62, 13.64.90.137, 52.147.198.201, 92.122.145.220, 216.58.212.173, 142.250.185.78, 142.250.185.206, 95.168.222.144, 2.20.143.16, 2.20.142.209, 95.168.222.76, 142.250.184.195, 23.57.80.111, 142.250.185.174, 172.217.18.106, 20.82.209.183, 92.122.213.194, 92.122.213.247, 34.104.35.123, 172.217.16.138, 142.250.185.106, 142.250.185.138, 142.250.185.170, 142.250.185.202, 142.250.185.234, 142.250.181.234, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 142.250.184.202, 142.250.184.234, 216.58.212.131, 172.217.16.131 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, r1---sn-n02xgoxufvg3-2gbl.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, r5---sn-n02xgoxufvg3-2gbs.gvt1.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, clients2.google.com, redirector.gvt1.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, update.googleapis.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, www.bing.com, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, accounts.google.com, www-google-analytics.l.google.com, content-autofill.googleapis.com, dual-a-0001.a-msedge.net, r5.sn-n02xgoxufvg3-2gbs.gvt1.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, r1.sn-n02xgoxufvg3-2gbl.gvt1.com, www.googleapis.com, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, edgedl.me.gvt1.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:41:19	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
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, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	59863
Entropy (8bit):	**7.99556910241083**

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Encrypted:	**true**
SSDEEP:	1536:Gs6cdy9E/ABKQPOrdweEz480zdPMHXNY/gLHfIZN:GNOqOrdDdJPAX1LHA/
MD5:	15775D95513782F99CDFB17E65DFCEB1
SHA1:	6C11F8BEE799B093F9FF4841E31041B081B23388
SHA-256:	477A9559194EDF48848FCE59E05105168745A46BDC0871EA742A2588CA9FBE00
SHA-512:	AC09CE01122D7A837BD70277BADD58FF71D8C5335F8FC599D5E3ED42C8FEE2108DD043BCE562C82BA12A81B9B08BD24B961C0961BF8FD3A0B8341C87483CDE7
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....b.....R.i .authroot.stl.qqp.4..CK..8T....c_.d....A.F....m"...AH)-.%.QIR..$t)Kd.-QQ*..~.L.2.L.....sx.}...~....$....yy.A.8;....|.%OV.a0xN....9..C..t.z.,X....,..1Qj,.p.E.y..ac`.<.e.c.aZW..B.jy....^]..+)..!...r.X:.O.. ..Y..j.^.8C.....n7R....p!|_.+..<...A.Wt.=. .sV..`.9O...CD./.s.\#.t#..s..Jeiu..B$.....8..(g..tJ....=,...r.d.].xqX4.....g.lF...Mn.y".W.R....K\..P.n._..7.....@pm.. Q....(#.....=.)...1..kC.`.....AP8.A..<....7S.L....S...^.R.).hqS...DK.6.j....u_.0.(4g.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....4E....q.QA.0.M<.&.^*aD.....,..]*....5.....\../ d.F>.V.....,_.J....".....wI..'..z...j..Ds....Z...[.....N<.d.?<....b..,...n.....;....YK.X..0..Z.....?...9.3.+9T.%.l...5.YK.E.V...aD.0...Y../e.7...c..g....A..=.....+..u2..X.~....O....\=...&...U.e...?...z....$.)S..T...r.!?M..;....r,QH.B <.(t..8s3..u[.N8gL.%...v....f...W.y...cz-.EQ.....c...o..n.....D*.....2.

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):	3.1492930417120966
Encrypted:	false
SSDEEP:	6:kK5QpkQSN+SkQlPlEGYRMY9z+4KlDA3RUeSKyzkOt:6phZkPlE99SNxAhUeSKO
MD5:	5526E9B29B807E558D2BA881EE25D2BC
SHA1:	386C6D32047825116957D8A2E085B5204C04DA5E
SHA-256:	C69A0AA7CAC9F66FC8BB06A7C3E4F552546403E61849C00B73E214B608742962
SHA-512:	938BD9AC6FD803C4D172E3238A28B18AB536BE01FDB143B0C0EB3FADFE6BD50433ACB8D06514FE1C00C9DB5179A014AC50ED999B01066EFA71234C8319F682E8
Malicious:	false
Reputation:	low
Preview:	p..... .....6..G..(..... .....Y5.....$.....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...".8.0.f.8.8.3.5.9.3.5.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0a0938a0-2127-4a3f-a7e2-984deed327cb.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):	359931
Entropy (8bit):	6.015385226635916
Encrypted:	false
SSDEEP:	6144:apubslwHRY+8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB+:aAbNxzurRDn9nfNxF4ijZVtilB+
MD5:	E220C13A7C31912DC3E0CD41A86430FB
SHA1:	36B9EEA3A5FD9A891CEB5655F0660A4290A64C69
SHA-256:	E4426D1C539410EBA7E3E1E6485765B6416DF588A141C424E1CB26DDF2B5F748
SHA-512:	6BFE5D9A162405217D314CCB93DD46EC3FF0535FD988349FCE65E3FC1E4F77A7C58ADCFCA07CF72D8E7E1C88C5F454C3DED7A1C5BAD6FC0B4F24B3E59A5F85B
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877279015723e+12,"network":1.62084488e+12,"ticks":106991788.0,"uncertainty":4527246.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"132653508758610

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
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\3cdcdaa6-5a7c-4be3-8122-3615fa41a74c.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):	5.577888163978436
Encrypted:	false
SSDEEP:	384:NbHtJLlzKXM1kXqKf/pUZNCgVLH2HfDwrUKig4x:ZLlsM1kXqKf/pUZNCgVLH2Hf0rUjge
MD5:	25ED9435DCDE8007D24805885E62F5B3
SHA1:	AD84979724E52199D2E7001CFB3BAC18A09086F5
SHA-256:	52D3254B76C3A1B9A8F3E01888B78485542C75ED77ADCB20192165D1CC757306
SHA-512:	2A70B6C44BC7F350EFEBBD329DFB418AF36AA1B7FACD1FBCAD2DD0B4D1E0BD90E80B8ABD1C9ACEF76FAA058D558B9A0ED7343841E55253EC1C5CF4DB535F23F1
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":"13265350875949573","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\40f96ee6-453c-41a2-8c88-eac22213abb9.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):	24055
Entropy (8bit):	5.533971644853065
Encrypted:	false
SSDEEP:	384:NbHtULlzKXM1kXqKf/pUZNCgVLH2HfDwrUPHGEHGYnTLAg4B:ELlsM1kXqKf/pUZNCgVLH2Hf0rU/GIGt
MD5:	7DA2D523823CA553429013A2B9A6F98B
SHA1:	FB7CBBDC021D21F8079A80E70ED806C018AE56F5
SHA-256:	FDCB65B29ACDCA0EDC264F5C9DBFA3FDBF9FF0211E374C00BAFE1E716B48023A
SHA-512:	CBFD96D35379B53964B1A0BA526AA0B6853B59ACD8684681AAC88D4419552ACEF370BB45F35D5A8CD4EF10713F1D895AF6F5196B524EC1ADCE68E842E1BE38E6
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":"13265350875949573","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6829f1b0-75f2-4569-b54b-87abd97e6c87.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):	5037
Entropy (8bit):	4.967070722657073
Encrypted:	false
SSDEEP:	96:nLrvoG2pSVJlk0JCKL83YkE119bOTQVuwn:nLrP2pSLC4KzkEV
MD5:	3DD0CD667BE18F120C360A9904A8E893
SHA1:	FE4A4A3FF5D64FC3AEAFDF74D2E8B4C141AD4DEF
SHA-256:	84C14BF7EC644E270E1ABA994A81792DBE058B188B5DD5B5E450A9BD0158E08C
SHA-512:	E936AA5A8636031A9F1C9B1FD1976CAD4BB4CF71D08D3B953E19721A6BBAD88FF4F4866D7B3CCBA07DE285CA529D415EFA48F67852C41FD8638D3B3CB32F4F54
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6829f1b0-75f2-4569-b54b-87abd97e6c87.tmp	
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265350876161971","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b6f9a58-09a1-4ba0-b1ac-30b1a8005059.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\8fb20792-f4d2-4d73-a979-32b725521c53.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):	5100
Entropy (8bit):	4.969452517943468
Encrypted:	false
SSDEEP:	96:nLrPl/2pSVJzIk0JCKL83DkXMFeTbOTQVuwn:nLrp2pS7C4KwkXR
MD5:	C5F8FEBA95B4739F38287E4278A6106D
SHA1:	2912307BC601F537708E99E6276D5AB6A2F15D40
SHA-256:	70B0E52883BB4CF8FB66FEF4AFA71EDC52788ADB62EFB7B2AEC17D9C6E6EE763
SHA-512:	A51ED388DF972FDF94D79BB095DAF8D5A92EADF261BBFE7DEA2F32E9A3E49D247074A088C7342170B8042958A1C8BF2895D7BFA4EC661B2C2CE3FADA303CB10
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265350876161971","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\954b861d-7a24-4530-a900-ab12cd548492.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):	5085
Entropy (8bit):	4.966459097354303
Encrypted:	false
SSDEEP:	96:nLrvGG2pSVJzIk0JCKL837kqjrnAbOTQVuwn:nLrh2pS7C4KMkq6
MD5:	61EB2A7A780BD899AB0C41D2B9CAF616
SHA1:	8F63DA3A47EF3EFA17DE7C065D60D69B48AB6C0B
SHA-256:	B7A782C443ECCE5742D6D65A0D46113386E9EBF4D86CFDB20BDF5DB62CEEEE28
SHA-512:	5061EDB6D02573ED5C813B4E794FEFE72971E7C3331C46C879B49777195ED9EAEB0FFE3FA4B2D6CD6E579185DD32CFE8F66C892B44F6E3FC83C756692FBAB95
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\954b861d-7a24-4530-a900-ab12cd548492.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265350876161971","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",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9d19e752-659b-4cc2-9a3e-7e0ee7e00a48.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	1041
Entropy (8bit):	5.568045042557709
Encrypted:	false
SSDEEP:	24:YT6H0UhHgHrfwUsdkG1KUe9aUeClVb7wUkRUeIQ:YT6UUhFUkDKUeAUeClpwUoUeh
MD5:	5B63FEC4F52225980114F40F847E4FAB
SHA1:	B65C26C08F63E143BFB0D4E9A255EDA8EBEB6A09
SHA-256:	92E650C9E14541A0A67D6968781C058B40DCF38AF5F9271258C2A23342F80A7A
SHA-512:	34A8465C1A3A5E627769A754BE92AFA5BD0CAC06CD2894C2D4FEB9043103704A0A21B0273854E140CE8BD84500EF5E0CA4C88629B55D286FFC47CA16BEF5A1 E
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":1631763701.849547,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620877301.849552},{"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":1652413279.040318,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620877279.040321},{"expiry":1633013028.952627,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_

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):	5.080301726698372
Encrypted:	false
SSDEEP:	6:mXhD9q2P923iKKdK9RXXTZIFUtp8hDVvZZmwP8hDnUR7kwO923iKKdK9RXX5LJ:shxv45Kk7XT2FUtp8hph/P8hjUR75L51
MD5:	2C3CB2F34A6D9080511CD3C32FE8EFCD
SHA1:	9D1603FE174DC55E9EC32657F26F4874D78A39EC
SHA-256:	F05CDDFBB7FD4181F550FC4BC7799C443BF5CFDF706A96F8E91C8E514A24E649
SHA-512:	E8C9F423D99FEE79D412E982994C7232F08DB8B03E90CE71472C347B1E6006266CA41A6A0DB3FCAA88BA4F40BD379FE1BCD3F9A90EAFCBE91A3A998B21B10F 4D
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:42:10.016 1140 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/12-20:42:10.022 1140 Recovering log #3.2021/05/12-20:42:10.023 1140 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):	5.15377102211155
Encrypted:	false
SSDEEP:	6:mXoIq2P923iKKdKyDZIFUtp8vZmwP8akwO923iKKdKyJLJ:sJv45Kk02FUtp8v/P8a5L5KkWJ
MD5:	D58AA655632A771651B4E033AACBA8D6
SHA1:	37D10910CDF90B166DC645383C4ABC03C29E6148
SHA-256:	6D100097D0B05644F581B1C4A2BBC8FFC69FAC28FA7E729F2DC97A9B9F92E3C0
SHA-512:	62609C6AFCDAF753850EB530407C05B50667E61F9CA6989ECDE36B5EEB991BA3FF51284D2A01581E8B1DEF8728BA33F43C5A19479B601C7304897E35F46CA95
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:42:09.892 1140 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/12-20:42:09.893 1140 Recovering log #3.2021/05/12-20:42:09.894 1140 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\080e5d32096294ef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.48538495928928
Encrypted:	false
SSDEEP:	3:m+lQnls8RzYrSLLiMZJXMLHSm9oWKiRMRictlPD8ell2QGP4fJ8dSD4hm5mv5X/B:mNnYGL+MHMmFyMrgO2CqcGm4PK6t
MD5:	91A3A392C8E05E6779926536145AD3E4
SHA1:	F78218BBC6F52A59B39289042D2CE988701DA1EF
SHA-256:	28728CAAB3C8AED38F043F0A212DA1BF032FB4117CB817183C2E718A3D14AD02
SHA-512:	BE8926F8BD6FD90ED250E8A3C4839884E16216F2356541D38B4C7D6B7F5382AFCC2CA7085C69405C117C596DA47BDD1F8D3AC65E98E930FEE08A69B8A2CF07 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....._keyhttps://www.google-analytics.com/plugins/ua/linkid.js .https://yolotats.com/-.W0. /.....".5..E.c..x.^.#.D..Y.....(.$.A..Eo.....X .....A..E o.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\58c452aae925b73a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.348937091810465
Encrypted:	false
SSDEEP:	3:m+loMD/ll6v8RzYrSLLiMIwJJSWKiRMRx5yhwv/tlPDZtrM+VFi7qSImkZm0HltJ:m8D//6EYGL+MIwJJ8yMswf3TKr0DK6t
MD5:	A770DC19E60BDDD661ABB07E5F866962
SHA1:	CDBE5FCBC3AD2A9A5907DF6D53A1DE5837D5FFFA
SHA-256:	60B462737EC05910F8CC8F91F59D52523B1E620E6C0B274C55F6C33ADB2F1D4F
SHA-512:	1C8C28456455A8E9EBE54D1D5274C60883B816B1DBD35703F7E85E393CCA36BC77F7BB1F97C2DC4EB6B994462CA8B752522942592EFE42112CBE576090E5EF4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....:.&...._keyhttps://www.google-analytics.com/analytics.js .https://yolotats.com/.\S0. /.....C.i[...../)...K.d..5.....X.A..Eo.....f|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	144
Entropy (8bit):	4.3060910556055765
Encrypted:	false
SSDEEP:	3:cmI004l/llWldl9oIghPa7U4KL/lllhuBQ6qKqloVT+:cmIsEJghPrqBQ6YoVT+
MD5:	E2D8FFBCD1761F029FC872876982AB91
SHA1:	A41BB9DFBDA1B580FAC2A7F8A67C40857C006694
SHA-256:	15A7970D9C6A599B5DD365BC7A824C4C1E538AE8ED288B0ACC44898350DEEFE4
SHA-512:	E83823D72A8C4FFFAAEE43FD78386CAC8F569DD807097A1AE31FCEA19F96A104758BE353C32DEDF3886BE39041C0A118829871EC6A28A9572C070A4CABCC3B BF
Malicious:	false
Reputation:	low
Preview:	....a...oy retne.....b.2]....U0. /.....:.%.R.X@gF0. /...../...3...5../.....^}.Np.....5../.....W0. /.

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:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619 F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
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):	0.9701566896430096
Encrypted:	false
SSDEEP:	24:XIL4rtEy8n/qLbJLbXaFpEO5bNmISHn06UwJ8:XI+M/q5LLOpEO5J/Kn7Ua8
MD5:	41C174EFD7E639A9DD603C8E8FAAFA71
SHA1:	E172ACFA8928618F0160AA603E05BF1201FB6AEF
SHA-256:	2A91F53A652199E94359BD503447BF8BBE3A4C7F6DACEBE91917B41623B99CBF
SHA-512:	E76959196F15117059C8DEB1608D7A4B78058A353251035D345EEDBB44B7DB35CDAE459E1A17A5A042DAA1135892DB12CCD067FA860D6E5563C6C932F59A94E
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):	1120
Entropy (8bit):	3.3661407769238174
Encrypted:	false
SSDEEP:	24:34Sue1tlrlCJc00ylGa6DmyzfIZl6DvlLlLlr:34Uxec002aDmOfIpD9RRr
MD5:	F9C1CCC01F1DFD2F49F2BB13FC6C322B
SHA1:	DF45185CF41C66FCEB82AAAC047F84CE3AF14E43
SHA-256:	43BF37331A7BADFA27612B957A9C699B0BBAAD754EADF0A660609FEAEAA0FC6A
SHA-512:	2DD98A3814C6308ED235A6A9DE1FBF675CACDA7B7A29893F6DE6FF30680A63C140FFAEA62FBAF1BEC562655B755A42020CDC8B89A25E11A53127AE7D6820EA 9A
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...c8ba779d_28ec_41bd_88b0_06ba30f6271e.....3..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....6...https://yolotats.com/Borrower/Borrower's-details. shtml.....h.....`.....~.-.....~.-.....0.....t...6...h.t.t.p.s.:././.y.o.l.o.t.a.t.s...c.o.m./.B.o.r.r.o.w .e.r./.B.o.r.r.o.w.e.r.'.s.-.d.e.t.a.i.l.s...s.h.t.m.l.....8.....0.....8..... ....6...h ttps://yolotats.com/Borrower/Borrower's-details.shtml...../. /.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.................F...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.1425003967936584
Encrypted:	false
SSDEEP:	6:mXGHeUQQL+q2P923iKKdK8aPrqIFUtp8GyQG1ZmwP8GTQLVkwO923iKKdK8amLJ:sIFyv45KkL3FUtp8p5/P8BR5L5KkQJ
MD5:	688C39D112D4A963FA45BBEC4F3FDE32
SHA1:	545F3F18BB8A7BC37E5E940B9F295E47E90119B8
SHA-256:	610F5B03A773DF6C80B41C955DEC041EC857E6B203A7B495EB2A7CFF44499FC6
SHA-512:	D2CB2972D3B902C8C62B6C0990306D2BE6482145E82EB14CCB3CC517241A0C6B3E34EDD647F6AE5F13E70A211A393DDBA9F8225E5C9989AF03AE985E3FA2682
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:41:16.208 1418 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/12-20:41:16.209 1418 Recovering log #3.2021/05/12-20:41:16.210 1418 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.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):	5.165023288521567
Encrypted:	false
SSDEEP:	6:mXGpQL+q2P923iKKdK8NIFUtp8GhSG1ZmwP8GnHQLVkwO923iKKdK8+eLJ:sfyv45KkpFUtp8QX/P8qwR5L5KkqJ
MD5:	BA04A006DB8825025657C201BE70A10A
SHA1:	8C8D42F770C907A0605C43EE4C3C257F5D024BF6
SHA-256:	B9D4C3B574561ED6625F233CE99880654D642BAA4719A296D831229FA7C6B9F2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
SHA-512:	5217874212EB6DC9514BD6A68EC27BC0E6FFF5D12723FA576574CF4C7A9307A98566083854E5F8BA26CF63AF1ECF293FB71B9C2B90EDE1563AD743036446C923
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:41:18.456 1418 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/12-20:41:18.457 1418 Recovering log #3.2021/05/12-20:41:18.458 1418 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:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/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=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_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):	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=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	5.214945369738182
Encrypted:	false
SSDEEP:	6:mXWq2P923iKKdK25+Xqx8chI+IFUtp8DZZmwP8GkwO923iKKdK25+Xqx8ch+/WLJ:sWv45KkTXfchI3FUtp8d/P8G5L5KkTXc
MD5:	1338C56B7860AFDE4B5B940B3179293D
SHA1:	5F553D38B2AF2F52355846DB632E132846915E78
SHA-256:	D1E64D397F8E1857FAADB0856158D1FD41E9D49DE33659EC6B6F8D59267B1EE9
SHA-512:	01250436663AE0326E605AA5BC48D3803269CF1588456113B5945839A420E86F83D0B32D62B9B68BE2C692F24A2975134B6A62615847BCA5ED7EFECF96B64288
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:42:09.691 1140 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/05/12-20:42:09.752 1140 Recovering log #3.2021/05/12-20:42:09.753 1140 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):	5.142358722915479
Encrypted:	false
SSDEEP:	6:mXbzFlq2P923iKKdK25+XuoIFUtp8zZZmwP8WkwO923iKKdK25+XuxWLJ:sGv45KkTXYFUtp8N/P8W5L5KkTXHJ
MD5:	E05FB34ABF08D8AA5D54E0ED74F3E884
SHA1:	EFBC2C6C9F661FAF0A8E5EB80E3539FF0B14DEED
SHA-256:	EA21FAB95FCF49871813086EDAA1F40F0AADEC4618D7E6C620363095F05A10C2
SHA-512:	4882841057E23151426DDC98A4EEFE93DB6036EC589313FA229E8BD5E11CA955DEA13A0E24A7A97E1C6538F9D98337B377AB73DF65A83969413B33F1F079A474
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:42:09.390 1140 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/12-20:42:09.392 1140 Recovering log #3.2021/05/12-20:42:09.393 1140 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):	5.147123661101969
Encrypted:	false
SSDEEP:	6:mXVWuIAq2P923iKKdKWT5g1IdqIFUtp8yZmwP8npkwO923iKKdKWT5g1I3ULJ:sVW1Av45Kkg5gSRFUtp8y/P8p5L5Kkgk
MD5:	E2739A99BC184B0C0A1114D6B9B91A51
SHA1:	8431CCBD3785F4E770854489873A0934A312FB13
SHA-256:	2204D140A6B72CDAB9C37F43722CF748A11137F99684C2EA2394E577AB62C286
SHA-512:	E0AED20507ECA9CFF43421984810BBCA859715813397FB3259ECB42D7CC6719AE992F424E63B950A04B321E8DEF3BBD0842DC873C9C8AAA7E042561733B076A
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:42:09.223 1140 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/12-20:42:09.313 1140 Recovering log #3.2021/05/12-20:42:09.314 1140 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Entropy (8bit):	0.1234196071016983
Encrypted:	false
SSDEEP:	6:l9bNFlWCj/lvYlpls5MfiyM8Xa3BVJk0zxtzBpHOo/lCxthibIGCxC+/erCBeYST:TLBj/KviMfi1pk0zxtbHNuQ8GI/U71pn
MD5:	CCD10BE88DD3821DDD2C7301D1BB28A3
SHA1:	659F017ABFC70A81D84BD2492024EB23EA323747
SHA-256:	F23213DD39887C80616E3F3728F1EAC993720823443C29FBCD1503CDE709D954
SHA-512:	127F147528CC88DAE4100B9CCFE9CF489C85E3D2BE371D88F7BB76932E6EE6F2C5B09A118DB278419B854F380E4AB5F4674A33631E52FE86F7AE8AAC55756E1E
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	786
Entropy (8bit):	5.310648200666436
Encrypted:	false
SSDEEP:	24:4NPJBKxoP1FDB5OBJiIY78BJgskfa9yBD8eirz7:uPKo1FDBmoOUm7
MD5:	029856C1CBDCDDF5D2B529F37D90A084
SHA1:	0DE2BF540515BF56AE47B68975A351F7E7F485DB
SHA-256:	2AA30961F4363985BFE85BB53376034A89413DF9124D8700A0F450EABAB385CF
SHA-512:	947E14F8C9FD2DB60AE97811A2F8C53D30AC7EF6735942EF0D3A1CDAA3763002AE49DCAD1340B67953F09D0A392DFC278F252887596E7A6B4B2600881DF669C
Malicious:	false
Reputation:	low
Preview:	....."i....american..borrower..borrower's..com..details..first..https..inquiry..policy..shtml..website..yolotats*.....american.....borrower.....borrower's.....com.....details.. ....first.....https.....inquiry.....policy.....shtml.....website.....yolotats..2.....'.....a.....b.....c.....d.....e.....f.....h.....i.....l.....m.....n.....o.... .....p.....q.....r.....s.....t.....u.....w.....y.....:n.....B..... .....*6https://yolotats.com /Borrower/Borrower's-details.shtml2%First American Policy Inquiry Website:.....J.....)1.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.08935179225443109
Encrypted:	false
SSDEEP:	12:4yLSQIOm2IB/qLipS/u3lA0s75fOfAG0S9Lc:4KPIOvIB/qLiUu3+r5f/GjNc
MD5:	C2544F6266207BE3927DC73FDBBD8D4F
SHA1:	CAFC7DD056FBF25F0C12D17E616074B1D6A175A3
SHA-256:	67EC9DF55BA267F77CD5B534D15E6BD2175DB53AB369F3A71D2DBF19ED47423D
SHA-512:	67EF5F6CC0DADA7B3972878E1718C99ABB0185630654332E13BC0873C7DCEE82C3DD42571501C09AC860696307181E4395E1151EB751F24D9A94FE40938B0749
Malicious:	false
Reputation:	low
Preview:	....

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):	5.1861086294987455
Encrypted:	false
SSDEEP:	6:mXGecow+q2P923iKKdK8a2jMGIFUtp8GecsXZmwP8Gec+Qr3VkwO923iKKdK8a23:sz1v45Kk8EFUtp8J/P8mrF5L5Kk8bJ
MD5:	194984C3B781CF47B21ADF0468C29224
SHA1:	790A6CE2A029FD899EDD3CD71EAD9A7EB9842E71
SHA-256:	452338B4B5B6C75B239580B41E4688FAE8B1CAED99BBF0737658C67A29CF24E1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SHA-512:	A550AFF39B6DC2227ECB018EE4C98D30BD89A6CB905C728C21D27A58351B3049B4C8EA06B132F4C42B33A024064E8891631034BFA487229AC5EBE1DC6A68B20 6
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:41:15.968 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/0 5/12-20:41:15.978 15d8 Recovering log #3.2021/05/12-20:41:15.980 15d8 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):	5.159059994786932
Encrypted:	false
SSDEEP:	6:mXGS9+q2P923iKKdKgXz4rRIFUtp8GRbN2WZmwP8GRbN9VkwO923iKKdKgXz4q8d:s79+v45KkgXiuFUtp8shJ/P8sh9V5L5j
MD5:	47F1C2F6F20D5CC28EB6EF24F85FD9E9
SHA1:	67243C93898BE9B4FF4534C200FD11679C9FA04A
SHA-256:	3B5B3E3E8C4AC0E5AC08774F3DB7F1FEA4FCEB5F0F8E3C6E2D90615B3D4D61B1
SHA-512:	9F10F991B9DCC016EC98431BC1B63D8C4BAF16E643859252CD0684AB9446E0C6B76D7684ECE7EAB0AC2969A271FCF47E411ECEEAE99C7B844768EF7BC980E0 99
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:41:16.236 140c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/ 05/12-20:41:16.239 140c Recovering log #3.2021/05/12-20:41:16.239 140c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Noti fications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.0113820338371613
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoG:wIElwQF8mpcSJ2Yc1
MD5:	98DD210E9B5342ACA6CF116E498C687A
SHA1:	73B158F60E9F26FCFBCBD36A8950CEA7D134BAE4
SHA-256:	4DFD2098335121810248047 2B7B892A7D94F1B1F975F3E6019E4D5E6514880C3
SHA-512:	E9B4A90AB3238903B219334693D52B61E0E74C9D38A3E7FFBCDBFC240CF6F77913D0D71EFDA45460DC2D246EAFCBA9038D2E811155EE7C7BFC02F0A69692A7 B
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):	0.8258895624766801
Encrypted:	false
SSDEEP:	48:BUqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUh6:BUhIElwQF8mpcSo
MD5:	877F20D6D9A33E95DCECDF50AF655E8E
SHA1:	3DC6CCF654004C440A80B081FF82D15856DE252F
SHA-256:	7AF3755C41B14CAEBC4C5C9AAD6152A6598B205BAF4E5124ED238AEC919DA684
SHA-512:	988FDEBAD4B90A4EE010A0BF7A6038596E4FC9DF016C93F0A561A909AD1B8117ED4AAFA89FFB343BAB76692EAE9272DDEEDBD7AF5F6CD6283EDABBD884019 364
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Preview:	.....[.:l..... ....

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):	95
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljl
MD5:	181ED05FAE6D31CDBFC2680CB632F859
SHA1:	B6391180B7167969686A3986E06D975F4CE67FAD
SHA-256:	62150C5EA1D8CFDE4916440F9662C32F3DCC1207BBC5441536D121EC683607E4
SHA-512:	40D79847C0420FA9395511DAA271B735ABD60CB55983F23DBF9552E56AAE1D915058D6D236D37D433FA7B16567957DB2C515BDB61B9032003914FF34EFA26BB5
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.1597729947086
Encrypted:	false
SSDEEP:	6:mXG0UN+q2P923iKKdKrQMxIFUtp8G0C7XZmwP8G0C73VkwO923iKKdKrQMFLJ:s3Nv45KkCFUtp83+/P83y5L5KktJ
MD5:	0D45B4CE7192830B52F15F6D3B22EC39
SHA1:	4A73FA61E76255F71842795D341C6DA68D4965D9
SHA-256:	1B0596CFFEEE60A3B1061D6E1FC9413729FEA167D1BAF6781C17F65EF89F9A65
SHA-512:	B12CF89D4902D64DC4095DBF0071DEF9A26B56E1091CECE7DCB521822BDEB0292BCE86A7AA70C227151FC9D9E366ABEF7FCD93D6C656BF3B3F0F65BE1AB0E 7A8
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:41:16.149 b48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/12-20 :41:16.150 b48 Recovering log #3.2021/05/12-20:41:16.150 b48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.130248648684975
Encrypted:	false
SSDEEP:	6:mXGeci9F39+q2P923iKKdK7Uh2ghZIFUtp8GecDeWNJZmwP8Gecc9VkwO923iKKF:sTN+v45KkIhHh2FUtp86/P8DV5L5KkIT
MD5:	72E54B57EA223C226AE3AC88CA7EC6FF
SHA1:	79FDB54EE4E6A0782C8878CB53B48B2E9CB6C8D3
SHA-256:	D008E0DF4E6FCC7525F7C430553575870961AA60B8814162FF9829A7920B7EE5
SHA-512:	E636B94A22A6E3DF8A6AAB1F33D1C9C63A62685D4A1AD1666DEB8699D82859071C3D5D660A2199B2DF7591A04AA29639AE1D6686C5DA7926966E13FD19D8D1E 5
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:41:15.945 142c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/05/12-20:41:15.953 142c Recovering log #3.2021/05/12-20:41:15.958 142c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\533d441f-2c82-4fb7-b488-51a1d33de4c4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\533d441f-2c82-4fb7-b488-51a1d33de4c4.tmp	
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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.242189859769372
Encrypted:	false
SSDEEP:	12:s3jvyv45KkFFUtp83fue/P83+R5L5KkOJ:EzY45KkfgW++DL5KkK
MD5:	23832FFB415573B44A65E76245D97393
SHA1:	FB4BFF69AE286F1D1951BCD57226843B4F29385E
SHA-256:	1FBED2549BFBC11600923722CD28E0F8AE7E205CE6551938E36ADCFB714D6943
SHA-512:	9152C54E485E99FA7788467825E774A5139AA131DC6390AF703AF7CF75B944A1FBC105BB98878459D6CD3DCCF117070C64C2E75DE868F70811A9592272B233AF
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:41:16.186 1418 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/05/12-20:41:16.188 1418 Recovering log #3.2021/05/12-20:41:16.189 1418 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):	5.2714935818059425
Encrypted:	false
SSDEEP:	6:mXGFNL+q2P923iKKdKusNpqz4rRIFUtp8Gfl11ZmwP8GQLVkwO923iKKdKusNpqS:s4Nyv45KkmiuFUtp8EX/P8VR5L5Kkm2J
MD5:	16EB941A25F8D5C4A95281FECBC64BFB
SHA1:	7E00BA0A083A261801F8A9EFD46991ACA260860E
SHA-256:	803456B0EF381CC4D5E9649A721373623D793124E662FFCC21EE1A8E6EA3A090
SHA-512:	825CB59C66CD81017B599229C0140448D4EDA4120176CFA1F63213F5F0E159B5CED77E1FA8111B2A9C4F7F8440ED26420D575EAC54688FDEFF093873F20473B0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Preview:	2021/05/12-20:41:16.235 1618 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/05/12-20:41:16.237 1618 Recovering log #3.2021/05/12-20:41:16.238 1618 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.203081770168938
Encrypted:	false
SSDEEP:	12:sEVsyv45KkMFUtp8EVD/P8EVfR5L5KkTJ:VVsY45KkUgvVZVfDL5Kkl
MD5:	CE922B829A25DDB92DE0629DE15D7E7A
SHA1:	8775C3F9CE4BD4DDB9A71E585536E49DCB008AA9
SHA-256:	8304657B1275F83AA235A2BEFC5817A6897D235586830CDB23C6E5C613FA4517
SHA-512:	8E3C2BDC731CEEA84580D12FF35929895FA8D9D9505196849506E2FA73F7238F29E500FE4DBFA4C2835E97F309BA792CAF185940597FA36743C1ABA59DD68A60
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:41:33.110 1418 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/05/12-20:41:33.111 1418 Recovering log #3.2021/05/12-20:41:33.111 1418 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.170132524927664
Encrypted:	false
SSDEEP:	12:sNjyv45KkkGHArBFUtp8f3/P8fDR5L5KkkGHAryJ:AM45KkkGgPgCc3L5KkkGga
MD5:	EAA81D11FA35954188830EFB8141D828
SHA1:	ED7E50E0F8FFD2EEE8F3C1A81163FE036CC18770
SHA-256:	6A234FEC33CB68E89DFD11A02634ED4D0987CDAE57F1EB1DAB0D7887EB290A46
SHA-512:	5E30BC3E5F6FEA9E48656DC16AFB2AAB6D8B6702321CA56E237133388529EC9C99E966DC5595BFED693B0D17DA277E36A32BBB021B2ACA2D2C196FE1DE6CBDF5
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:42:08.029 1618 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/05/12-20:42:08.030 1618 Recovering log #3.2021/05/12-20:42:08.030 1618 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):	434
Entropy (8bit):	5.156166449863495
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
SSDEEP:	12:szS+v45KkkGHArqiuFUtp8zXoSZ/P8zXoSNV5L5KkkGHArq2J:l45KkkGgCgyh2hlL5KkkGg7
MD5:	C1E652CEB7666B3671FF1F28DCA5A810
SHA1:	794BAF6E22DC53EADEED2BF53A4D61044024C271
SHA-256:	5B97F07DA6C5B41D2183C466D273D6A9DAE95CF04CA30ABD9D400C608C53CBE3
SHA-512:	CCEBDE95CBA8E061B1BCB8F18C7A8DD996E0BB1625CD1E910A0CA667F476314557E71CD37AF431AAD4C886DED05F3471F8DDBF8E957B827F6220D2162B3623A
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:42:08.051 1b0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/05/12-20:42:08.052 1b0c Recovering log #3.2021/05/12-20:42:08.052 1b0c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.209816736587708
Encrypted:	false
SSDEEP:	6:mXGecuRjL+q2P923iKKdKpIFUtp8GecKKWZmwP8GecsG+LVkwO923iKKdKa/WLJ:sXpL+v45KkmFUtp8uW/P8VG+LV5L5Kk7
MD5:	268F98523BB6BD17D6E74F0429691FCD
SHA1:	0D47092119512BF554C17E1424C50A594A4BE56B
SHA-256:	4C75F2056B3C93BD38DCFEE4583F08E74E8F9FD2B729BE4742D7EEC5500468A6
SHA-512:	6A0414DBF679F201F6B8ACDF92051A8D2EEC2CB38DAC39EC96BE24A19444DFBD363CC05857C4E30AF01F5E1FD17F75938B6E631AE7231F829E6F754A791A944
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:41:15.958 15cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/05/12-20:41:15.969 15cc Recovering log #3.2021/05/12-20:41:15.974 15cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.242664578883253
Encrypted:	false
SSDEEP:	12:shLv45KkkOrsFUtp8h6n/P8hx5L5KkkOrzJ:S45Kk+gYL5Kkn
MD5:	9463952C1BE85D87CDCE3B51E2065B39
SHA1:	E7A2C418ABFA6BAD7F127B761A766B022C7EB7F1
SHA-256:	9B43C869924EB496D62D94234BDBA6DA01AA0625D491DEAF55A7B017F79B5973
SHA-512:	3AB5AC6E971EF9A7261698D5597D52309BF30272039005267BDA57A045E071E008B8A0E8A5C03A1F24386E74CA635B5DEC277524415CF7567F88883C8F9FECFA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Preview:	2021/05/12-20:42:12.242 1b08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/05/12-20:42:12.244 1b08 Recovering log #3.2021/05/12-20:42:12.245 1b08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:IVJlXAn:oEn
MD5:	0F8A152E121F4D948C9717E6B5FD10A5
SHA1:	0D8FA18B49E25666790E036D28ABA7A8782F29BC
SHA-256:	37564FC016FAD10136BD0C105C2DE883E6598EBEABCF5AE9413C0B639529FB62
SHA-512:	0649391068C6163387E1965620F2EBFD4D2886F5320BD0DBCFEAA8846A1B7D35E0126F47A998434895903D72C2C83BD283F206232DF8A57DC1E45389B5D0565E
Malicious:	false
Reputation:	low
Preview:	....l0L..>.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a476d9a2-44e5-43be-8cc8-fa5399f0c909.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):	5.554045492309323
Encrypted:	false
SSDEEP:	12:YdDZ6Hk3O+UAnIvld06cY8rNgmh4r+UAnIEllWcNnYj+UAnIECmaVlR7N+UAnIAD:YT6H0UhHPkG1KUe9aUeClVb7wUkRUeIQ
MD5:	C2F21BF7ADE3C37256669E9EE6D6C48B
SHA1:	D7A3F1282B988734F82675C868EA512D47F5C05C
SHA-256:	2B30D974A5358A3DC1984E38AE7C11298DEF21B80AEBF9D9C70557594A003E81
SHA-512:	5B4FECEC2A685DCB56AE1787883B6A620937E82FB68B1CDABB0373C4E9EAB7A21BB8ACB873C1A95731CEB58A6DA659B6D4B93AF4D81DEB8A3733B238FA59C2BB
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":1652413279.040318,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620877279.040321},{"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\b1b3df6d-81ff-4ff7-a900-eaec7311a366.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):	16746
Entropy (8bit):	5.577802877520334
Encrypted:	false
SSDEEP:	384:NbHtULlzKXM1kXqKf/pUZNCgVLH2HfDwrUlig4YM:ELlsM1kXqKf/pUZNCgVLH2Hf0rUtgg
MD5:	FAE503A1A9CE425207AC241D98F61BF1
SHA1:	21DB299DD6C509DDE246A1E50848F6A0F855778F
SHA-256:	323DF2BB3ADEFD18005146E7F9CF9C5949A9EFF648BEF6B915E4CAFC9150355D
SHA-512:	F38CD652898A95DAC055D0C1FD985F65C42EAE66A235EAA27BFDA136E6787FBE0766AFAB8F0C10832A724C97E001D076B3E0CFEDE17F52069F72DF1E0824FB7
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":"13265350875949573","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\daf825cd-4502-4416-b4c9-19448949f82e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	5774
Entropy (8bit):	5.183185057958971
Encrypted:	false
SSDEEP:	96:nLrPU/2iZdO0SVJzIk0JCKL83Uk2SMHo/bOTQVuwn:nLru2ebS7C4KvkhV
MD5:	7D15018176047E8BDBF2B33107964A78
SHA1:	C02D5B7E5A66DD392AABAFA5C0617A238DE306F4
SHA-256:	16698FF779B9D67AB37EE9D399E9E700C4D6A9041E84774F1297B8A19150B89D
SHA-512:	70559218CEECF1866BF508D087CA4B97B356211E5915EC5D53CBADF79EC127F08AA282FAD68BC439607EB0FE429D6E202C9B230C54AD229E3DC7CFF4D53955C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265350876161971","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.413017847645856
Encrypted:	false
SSDEEP:	3:tUKCgRPVHV7WPj1Zmwv38gRPVHXMSVV8s8gRPVHXSUVSVWGv:mXr1ZmwP8cVv8ZUwtv
MD5:	32F9A3B168A69391C94A0C380F117929
SHA1:	67A2D56381AE191CED39FFBCA726E730892C8522
SHA-256:	429A6F28DC3410B0328C9974EAFC0981BA247A9C1B19A3F8905F86D0850E50F9
SHA-512:	DCD2B0049E854FECBE63B7CFBA324052B3EDAC37E1C6A4FBDF4047FFCF5B2CDAED111D98546F2DD0F467E38CEF195F5863EED298A870DD1AB444D397DE08FC0
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:42:06.038 137c Recovering log #3.2021/05/12-20:42:06.222 137c Delete type=0 #3.2021/05/12-20:42:06.223 137c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\db1e5215-cd33-424b-b20f-b42ecb9c317c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.195538725381159
Encrypted:	false
SSDEEP:	6:mXhyE9+q2P923iKKdKfrzAdIFUtp8hKCJZmwP8hKN9VkwO923iKKdKfrzILJ:sh+v45Kk9FUtp8hR/P8hq5L5Kk2J
MD5:	4CF6E18BE895C20F9EB3228D9305ACDC
SHA1:	8B3B7EE1594AF353D5C2150C7B63736883106727
SHA-256:	ECC1F21858845E390F7FA0F1AB8DAD159EA97A762E3E8B4F724B82339934FB52
SHA-512:	F4F8AABBCAE0E1B4B831B61C46AF9C6183D2B7B37D0CF427128F5892E0307E6E223B5739C6CF5270399C79B14CBE69284882169BD230AA6FAE56EB21AA4FBA8
Malicious:	false
Reputation:	low
Preview:	2021/05/12-20:42:11.787 1b08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/05/12-20:42:11.792 1b08 Recovering log #3.2021/05/12-20:42:11.793 1b08 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:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\a1428026-7b3e-4d06-82bd-195b327f723a.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):	359931
Entropy (8bit):	6.015385226635916
Encrypted:	false
SSDEEP:	6144:apubsIwHRY+8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB+:aAbNxzurRDn9nfNxF4ijZVtilB+
MD5:	E220C13A7C31912DC3E0CD41A86430FB
SHA1:	36B9EEA3A5FD9A891CEB5655F0660A4290A64C69
SHA-256:	E4426D1C539410EBA7E3E1E6485765B6416DF588A141C424E1CB26DDF2B5F748
SHA-512:	6BFE5D9A162405217D314CCB93DD46EC3FF0535FD988349FCE65E3FC1E4F77A7C58ADCFCA07CF72D8E7E1C88C5F454C3DED7A1C5BAD6FC0B4F24B3E59A5F85B
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877279015723e+12,"network":1.62084488e+12,"ticks":106991788.0,"uncertainty":4527246.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"132653508758610

C:\Users\user\AppData\Local\Google\Chrome\User Data\b2390955-b7fd-405f-9775-a38989966d51.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):	359931
Entropy (8bit):	6.01538632417016
Encrypted:	false
SSDEEP:	6144:mpubsIwHRY+8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB+:mAbNxzurRDn9nfNxF4ijZVtilB+
MD5:	4495E24B63508E80070B265C0476CB9E
SHA1:	0B617827928D4BBFD5338F7CFCCE5AE93618DF64
SHA-256:	838740A0356E0BE77D4B7778AD42C3D2D00DD79D21C4DE86D6FBEE974D452B64
SHA-512:	309AF9559356A9B9AD0506CFF7D39F78EC0F0EEECB8D73CE1C1D3EF0B2C3D8580905EC653942495A4A76C38DB607CEAD7C829D6A3AEE76BEC1249A18694AD02
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620877279015723e+12,"network":1.62084488e+12,"ticks":106991788.0,"uncertainty":4527246.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075544633"},"policy":{"last_statistics_update":"132653508758610

C:\Users\user\AppData\Local\Temp\23670a59-3f7d-44cd-bb47-b678a0f34a9a.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\23670a59-3f7d-44cd-bb47-b678a0f34a9a.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..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\26022141-f371-4902-a106-e68062ad445e.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\748e34b5-1e6e-41ca-9f4a-ccac19e43429.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\7be03483-19c8-43d8-b5f2-304d3604e036.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\7be03483-19c8-43d8-b5f2-304d3604e036.tmp	
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..I.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\ae5723d0-dac9-4404-a578-a4c9b0786e60.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.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\b3c9b359-482c-49cf-af85-2a78bc6e3721.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	10642
Entropy (8bit):	4.641836385055058
Encrypted:	false
SSDEEP:	192:IrtboGRhnwUzU/zYO0qM8nuBVuiw28m/K7h0hRvhV5hzhVe+BfKc:4tUGjwUl/zYO3uBVui//8eDd1Te+Bfh
MD5:	27B9B633CED45B19CEA20B9ED168397C
SHA1:	301B29534966FE7378177F1099CC4A2E3BD3B3C4
SHA-256:	DFF2D81A64805C759A2001CD4EDEA7A666A5707E00A2A12BF4CCBDFC387EDC09
SHA-512:	B357E2BE579786DEA927A2E6C4EC20AD1AE84E68CB0070EA25C009E1AFEC138DC50EA4946740B1012FA7165F2704FE6D2809E5B97025584C11A0A61E05185F8
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 00995f1c90f187f2017b54d6f609ed073045be032513e844d2634c0cc451e1b6 4bf2d82fab96eaae89a3c250b007ada4f60c60bf09848d01f5513afb962447b6.SERVER_HANDSHAKE_TRAFFIC_SECRET 00995f1c90f187f2017b54d6f609ed073045be032513e844d2634c0cc451e1b6 0647396726 19e0bacdedfcc0f127b4a5ccdf75c08eb4fcbf3b22c2b6a30c6f05.CLIENT_HANDSHAKE_TRAFFIC_SECRET f3446eeb50812247fd8189834bc30ff99523ab3cab53f94ab5da2a8c728d209c d40d302dfbfc3df1083f10a06297c1da6cfe942b1b9ce96a46d5374cfe3782a8.SERVER_HANDSHAKE_TRAFFIC_SECRET f3446eeb50812247fd8189834bc30ff99523ab3cab53f94ab5da2a8c728d209c 5547fc64a62b972b0feb22a3ac22af6a5eb3b264ce40b20baf9db9cf9f85e075.CLIENT_HANDSHAKE_TRAFFIC_SECRET 626165b91606cbe84863435596d112fbda74b0b7d8fb946ef30a3887385e4ff8 5d5414c5b970c490bd383ccb9b911fd62b2366f25c6d68de24caedb0f4606ceb.SERVER_HANDSHAKE_TRAFFIC_SECRET 626165b91606cbe84863435596d112fbda74b0b7d8fb946ef30a3887385e4ff8 1fca3df240ff38ad904714f53f9cc633c622cc6c1881f4155aa55f365fdd72e9.CLIENT_TRAFFIC_SECRET_0 f344

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\7be03483-19c8-43d8-b5f2-304d3604e036.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L]....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir1060_1621826258\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_dir1060_1621826258\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": "C onnecteu-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_dir1060_1621826258\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

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\CRX_INSTALL_locales\cs\messages.json	
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_dir1060_1621826258\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:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C53E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "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 completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\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+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "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 transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\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

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\CRX_INSTALL_locales\el\messages.json	
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_dir1060_1621826258\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
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_unava ilable": {.. "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_dir1060_1621826258\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_unava ilable": {.. "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_dir1060_1621826258\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_dir1060_1621826258\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
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 transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\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_unavailable": {.. "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_dir1060_1621826258\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:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEAD8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavailable": {.. "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_dir1060_1621826258\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

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\CRX_INSTALL_locales\fil\messages.json	
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_dir1060_1621826258\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_dir1060_1621826258\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": {.. "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_dir1060_1621826258\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

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\CRX_INSTALL_locales\hr\messages.json	
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_dir1060_1621826258\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
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_dir1060_1621826258\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:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA 2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\CRX_INSTALL_locales\ja\messages.json	
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
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_dir1060_1621826258\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_dir1060_1621826258\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:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D3444
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_dir1060_1621826258\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

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\CRX_INSTALL_locales\lv\messages.json	
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_dir1060_1621826258\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
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_dir1060_1621826258\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_dir1060_1621826258\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

C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\CRX_INSTALL_locales\pl\messages.json	
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.".. }..}..

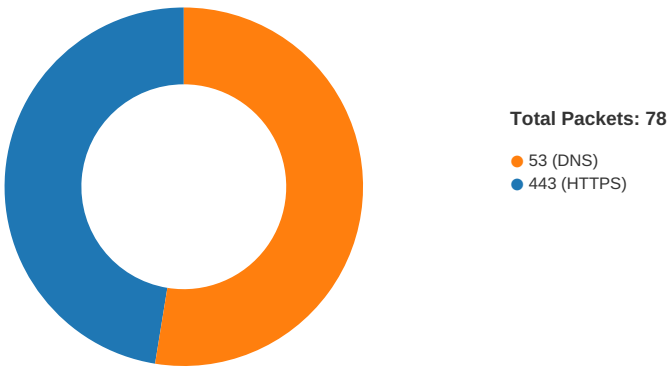
C:\Users\user\AppData\Local\Temp\scoped_dir1060_1621826258\CRX_INSTALL_locales\pt_BR\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE
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.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:41:09.020359039 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.022182941 CEST	49689	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:09.022243977 CEST	49689	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:09.037525892 CEST	443	49687	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.037575960 CEST	443	49687	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.037604094 CEST	443	49687	20.190.159.134	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:41:09.037628889 CEST	443	49687	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.037651062 CEST	443	49687	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.037676096 CEST	443	49687	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.037699938 CEST	443	49687	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.037724018 CEST	443	49687	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.037744999 CEST	443	49687	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.037760019 CEST	49687	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:09.037795067 CEST	49687	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:09.041650057 CEST	443	49680	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.041691065 CEST	443	49680	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.041716099 CEST	443	49680	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.041739941 CEST	443	49680	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.041764975 CEST	443	49680	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.041789055 CEST	443	49680	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.041811943 CEST	443	49680	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.041819096 CEST	49680	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:09.041838884 CEST	443	49680	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.041863918 CEST	443	49680	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.041873932 CEST	49680	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:09.041933060 CEST	49680	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:09.083635092 CEST	49687	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:09.112127066 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.112154007 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.134654045 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.259701967 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.259756088 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.259783983 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.259810925 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.259834051 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.259860039 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.259876966 CEST	49689	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:09.259882927 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.259906054 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.259926081 CEST	443	49689	20.190.159.134	192.168.2.5
May 12, 2021 20:41:09.259954929 CEST	49689	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:09.260000944 CEST	49689	443	192.168.2.5	20.190.159.134
May 12, 2021 20:41:18.731244087 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:18.849627018 CEST	49711	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:18.891186953 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:18.891314983 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:18.891653061 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.007924080 CEST	443	49711	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.008042097 CEST	49711	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.008752108 CEST	49711	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.050976992 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.051897049 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.051917076 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.051928997 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.051938057 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.052027941 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.052089930 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.052864075 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.052881002 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.052947998 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.167329073 CEST	443	49711	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.167917967 CEST	443	49711	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.167968988 CEST	443	49711	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.168009043 CEST	443	49711	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.168037891 CEST	443	49711	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.168061018 CEST	49711	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.168206930 CEST	49711	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.168816090 CEST	443	49711	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.168849945 CEST	443	49711	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.168920040 CEST	49711	443	192.168.2.5	69.49.235.204

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:41:19.783335924 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.784161091 CEST	49711	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.784368038 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.943576097 CEST	443	49711	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.943931103 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.944425106 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.945178986 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.945220947 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.945269108 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.945275068 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.945317984 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.945333004 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.945357084 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.945419073 CEST	443	49710	69.49.235.204	192.168.2.5
May 12, 2021 20:41:19.945441008 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.985177994 CEST	49711	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:19.985860109 CEST	49710	443	192.168.2.5	69.49.235.204
May 12, 2021 20:41:20.067857981 CEST	49720	443	192.168.2.5	104.129.24.42
May 12, 2021 20:41:20.214534998 CEST	443	49720	104.129.24.42	192.168.2.5
May 12, 2021 20:41:20.214703083 CEST	49720	443	192.168.2.5	104.129.24.42
May 12, 2021 20:41:20.215106010 CEST	49720	443	192.168.2.5	104.129.24.42
May 12, 2021 20:41:20.216398954 CEST	49722	443	192.168.2.5	69.87.16.180
May 12, 2021 20:41:20.250629902 CEST	49723	443	192.168.2.5	69.87.16.180
May 12, 2021 20:41:20.361426115 CEST	443	49720	104.129.24.42	192.168.2.5
May 12, 2021 20:41:20.362596035 CEST	443	49720	104.129.24.42	192.168.2.5
May 12, 2021 20:41:20.362643957 CEST	443	49720	104.129.24.42	192.168.2.5
May 12, 2021 20:41:20.362682104 CEST	443	49720	104.129.24.42	192.168.2.5
May 12, 2021 20:41:20.362719059 CEST	443	49720	104.129.24.42	192.168.2.5
May 12, 2021 20:41:20.363034010 CEST	49720	443	192.168.2.5	104.129.24.42
May 12, 2021 20:41:20.365354061 CEST	443	49720	104.129.24.42	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:41:09.110913038 CEST	65307	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:09.169250011 CEST	53	65307	8.8.8.8	192.168.2.5
May 12, 2021 20:41:09.185292006 CEST	64344	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:09.245556116 CEST	53	64344	8.8.8.8	192.168.2.5
May 12, 2021 20:41:09.313940048 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:09.363986015 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 20:41:10.774488926 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:10.823335886 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 20:41:11.556763887 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:11.605510950 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 20:41:12.176424980 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:12.235054016 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 20:41:12.775161982 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:12.826311111 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 20:41:13.696701050 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:13.745485067 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 20:41:15.042217970 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:15.091073990 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 20:41:16.794440031 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:16.845367908 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 20:41:18.596354961 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:18.597929001 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:18.605540991 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:18.605859995 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:18.658164024 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 20:41:18.662166119 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 20:41:18.662707090 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 20:41:18.671425104 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 20:41:19.137512922 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:19.193772078 CEST	49992	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:41:19.207129955 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 20:41:19.217008114 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:19.245708942 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 20:41:19.280554056 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 20:41:19.307291031 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:19.364741087 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 20:41:20.008892059 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:20.009576082 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:20.066828966 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 20:41:20.215234995 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 20:41:20.380053997 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:20.462882042 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 20:41:20.806689024 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:20.858378887 CEST	53	50394	8.8.8.8	192.168.2.5
May 12, 2021 20:41:21.668288946 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:21.716993093 CEST	53	58530	8.8.8.8	192.168.2.5
May 12, 2021 20:41:22.877716064 CEST	53813	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:22.931437016 CEST	53	53813	8.8.8.8	192.168.2.5
May 12, 2021 20:41:36.749191999 CEST	60516	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:36.811120987 CEST	53	60516	8.8.8.8	192.168.2.5
May 12, 2021 20:41:41.311206102 CEST	51649	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:41.372908115 CEST	53	51649	8.8.8.8	192.168.2.5
May 12, 2021 20:41:41.630443096 CEST	65086	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:41.695949078 CEST	53	65086	8.8.8.8	192.168.2.5
May 12, 2021 20:41:41.933669090 CEST	56432	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:42.002209902 CEST	53	56432	8.8.8.8	192.168.2.5
May 12, 2021 20:41:50.154002905 CEST	52929	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:50.211776018 CEST	53	52929	8.8.8.8	192.168.2.5
May 12, 2021 20:41:56.135010958 CEST	64317	53	192.168.2.5	8.8.8.8
May 12, 2021 20:41:56.196906090 CEST	53	64317	8.8.8.8	192.168.2.5
May 12, 2021 20:42:03.344813108 CEST	56895	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:03.402492046 CEST	53	56895	8.8.8.8	192.168.2.5
May 12, 2021 20:42:03.699680090 CEST	61515	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:03.699734926 CEST	56675	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:03.699754953 CEST	62372	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:03.756892920 CEST	53	62372	8.8.8.8	192.168.2.5
May 12, 2021 20:42:03.761840105 CEST	53	56675	8.8.8.8	192.168.2.5
May 12, 2021 20:42:03.910274029 CEST	53	61515	8.8.8.8	192.168.2.5
May 12, 2021 20:42:06.418472052 CEST	57172	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:06.504164934 CEST	53	57172	8.8.8.8	192.168.2.5
May 12, 2021 20:42:10.382435083 CEST	55267	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:10.439966917 CEST	53	55267	8.8.8.8	192.168.2.5
May 12, 2021 20:42:11.848669052 CEST	50969	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:11.907284021 CEST	53	50969	8.8.8.8	192.168.2.5
May 12, 2021 20:42:16.291270971 CEST	64362	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:16.342856884 CEST	53	64362	8.8.8.8	192.168.2.5
May 12, 2021 20:42:17.303589106 CEST	61446	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:17.361671925 CEST	53	61446	8.8.8.8	192.168.2.5
May 12, 2021 20:42:17.397346973 CEST	57515	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:17.457307100 CEST	53	57515	8.8.8.8	192.168.2.5
May 12, 2021 20:42:17.602185011 CEST	58199	53	192.168.2.5	8.8.8.8
May 12, 2021 20:42:17.659660101 CEST	53	58199	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 20:41:18.605859995 CEST	192.168.2.5	8.8.8.8	0x834e	Standard query (0)	yolotats.com	A (IP address)	IN (0x0001)
May 12, 2021 20:41:20.008892059 CEST	192.168.2.5	8.8.8.8	0x18f5	Standard query (0)	insagent.firstam.com	A (IP address)	IN (0x0001)
May 12, 2021 20:41:20.009576082 CEST	192.168.2.5	8.8.8.8	0x6805	Standard query (0)	gofirstam.com	A (IP address)	IN (0x0001)
May 12, 2021 20:41:41.311206102 CEST	192.168.2.5	8.8.8.8	0x2cf8	Standard query (0)	www.maskeny.com	A (IP address)	IN (0x0001)
May 12, 2021 20:42:03.699680090 CEST	192.168.2.5	8.8.8.8	0xc101	Standard query (0)	insagent.firstam.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 20:42:03.699734926 CEST	192.168.2.5	8.8.8.8	0xdf50	Standard query (0)	www.maskeny.com	A (IP address)	IN (0x0001)
May 12, 2021 20:42:03.699754953 CEST	192.168.2.5	8.8.8.8	0x9e2d	Standard query (0)	gofirstam.com	A (IP address)	IN (0x0001)
May 12, 2021 20:42:06.418472052 CEST	192.168.2.5	8.8.8.8	0xadec	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:41:18.671425104 CEST	8.8.8.8	192.168.2.5	0x834e	No error (0)	yolotats.com		69.49.235.204	A (IP address)	IN (0x0001)
May 12, 2021 20:41:20.066828966 CEST	8.8.8.8	192.168.2.5	0x6805	No error (0)	gofirstam.com		104.129.24.42	A (IP address)	IN (0x0001)
May 12, 2021 20:41:20.215234995 CEST	8.8.8.8	192.168.2.5	0x18f5	No error (0)	insagent.firstam.com		69.87.16.180	A (IP address)	IN (0x0001)
May 12, 2021 20:41:41.372908115 CEST	8.8.8.8	192.168.2.5	0x2cf8	No error (0)	www.maskeny.com	maskeny.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:41:41.372908115 CEST	8.8.8.8	192.168.2.5	0x2cf8	No error (0)	maskeny.com		184.175.83.99	A (IP address)	IN (0x0001)
May 12, 2021 20:42:03.756892920 CEST	8.8.8.8	192.168.2.5	0x9e2d	No error (0)	gofirstam.com		104.129.24.42	A (IP address)	IN (0x0001)
May 12, 2021 20:42:03.761840105 CEST	8.8.8.8	192.168.2.5	0xdf50	No error (0)	www.maskeny.com	maskeny.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:42:03.761840105 CEST	8.8.8.8	192.168.2.5	0xdf50	No error (0)	maskeny.com		184.175.83.99	A (IP address)	IN (0x0001)
May 12, 2021 20:42:03.910274029 CEST	8.8.8.8	192.168.2.5	0xc101	No error (0)	insagent.firstam.com		69.87.16.180	A (IP address)	IN (0x0001)
May 12, 2021 20:42:06.504164934 CEST	8.8.8.8	192.168.2.5	0xadec	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:42:06.504164934 CEST	8.8.8.8	192.168.2.5	0xadec	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 20:41:19.052864075 CEST	69.49.235.204	443	192.168.2.5	49710	CN=yolotats.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun May 09 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 08 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 12, 2021 20:41:19.168816090 CEST	69.49.235.204	443	192.168.2.5	49711	CN=yolotats.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun May 09 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 08 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 12, 2021 20:42:02.941834927 CEST	69.49.235.204	443	192.168.2.5	49748	CN=yolotats.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun May 09 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 08 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 20:42:04.056035995 CEST	104.129.24.42	443	192.168.2.5	49756	CN=gofirstam.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 16 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Jun 15 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 12, 2021 20:42:04.087459087 CEST	184.175.83.99	443	192.168.2.5	49757	CN=www.maskeny.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Apr 02 11:58:47 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Thu Jul 01 11:58:47 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

● chrome.exe
● chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 1060 Parent PID: 3444

General

Start time:	20:41:14
Start date:	12/05/2021
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://yolotats.com/Borrower/Borrower's-details.shtml'
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 5708 Parent PID: 1060

General

Start time:	20:41:16
Start date:	12/05/2021
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=1704,16863434715654432222,3804912756075544807,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1752 /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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly