ID: 635363
Cookbook: browseurl.jbs
Time: 20:18:27
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

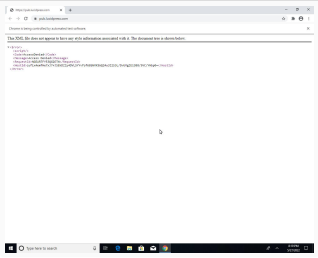
Windows Analysis Report

http://pub.lucidpress.com

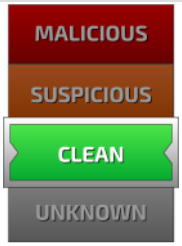
Overview

General Information

Sample URL:	http://pub.lucidpress.com
Analysis ID:	635363
Infos:	



Detection

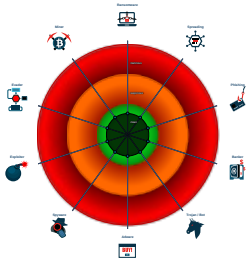


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 4324 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "http://pub.lucidpress.com MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6180 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1616,15869322143913586381,16477777855430292938,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

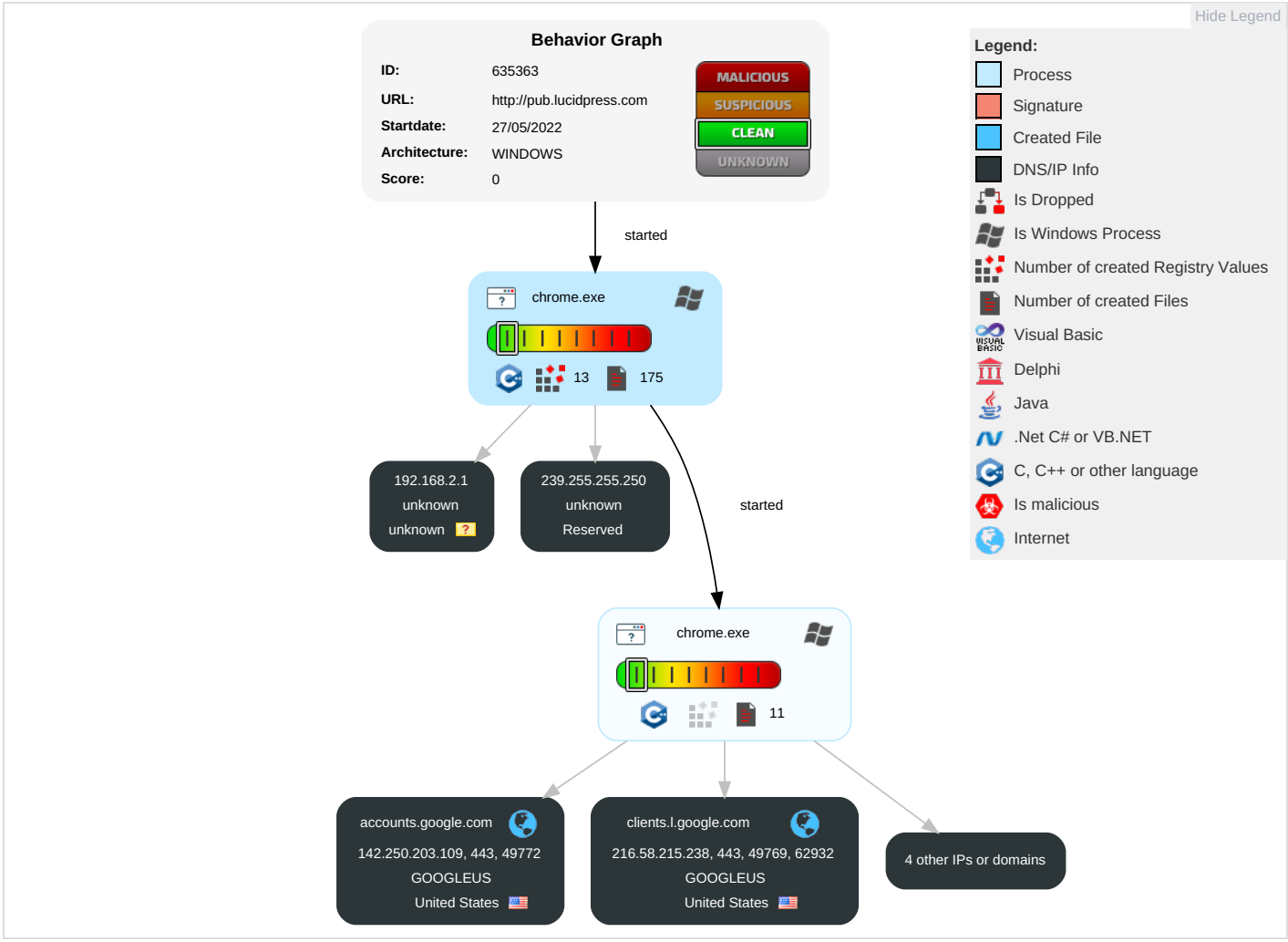
Joe Sandbox Signatures

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	5 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

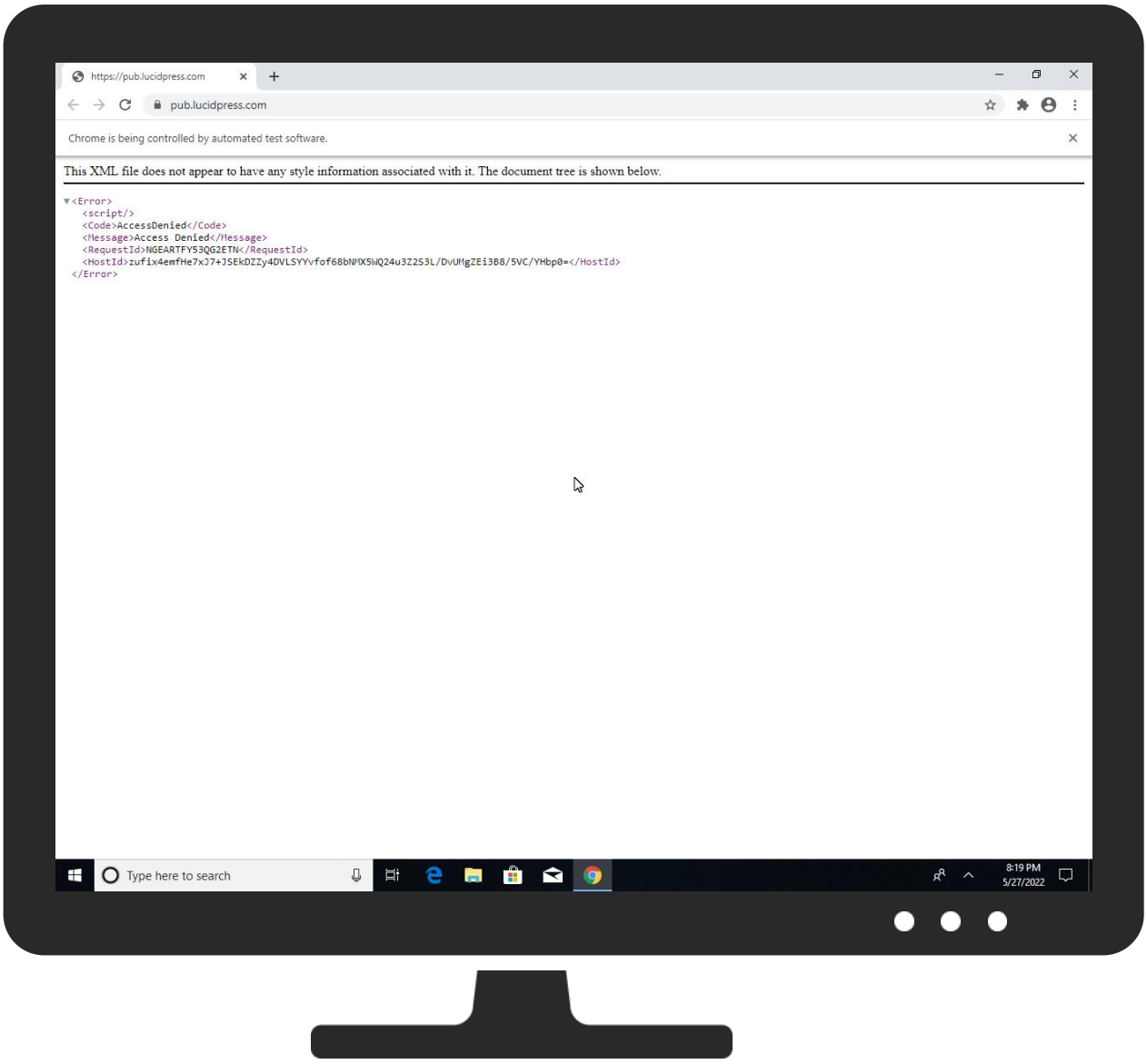
Behavior Graph



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://pub.lucidpress.com	1%	Virustotal		Browse
http://pub.lucidpress.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
d3v04nmt9jknbk.cloudfront.net	13.226.244.72	true	false		high
clients.l.google.com	216.58.215.238	true	false		high
pub.lucidpress.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

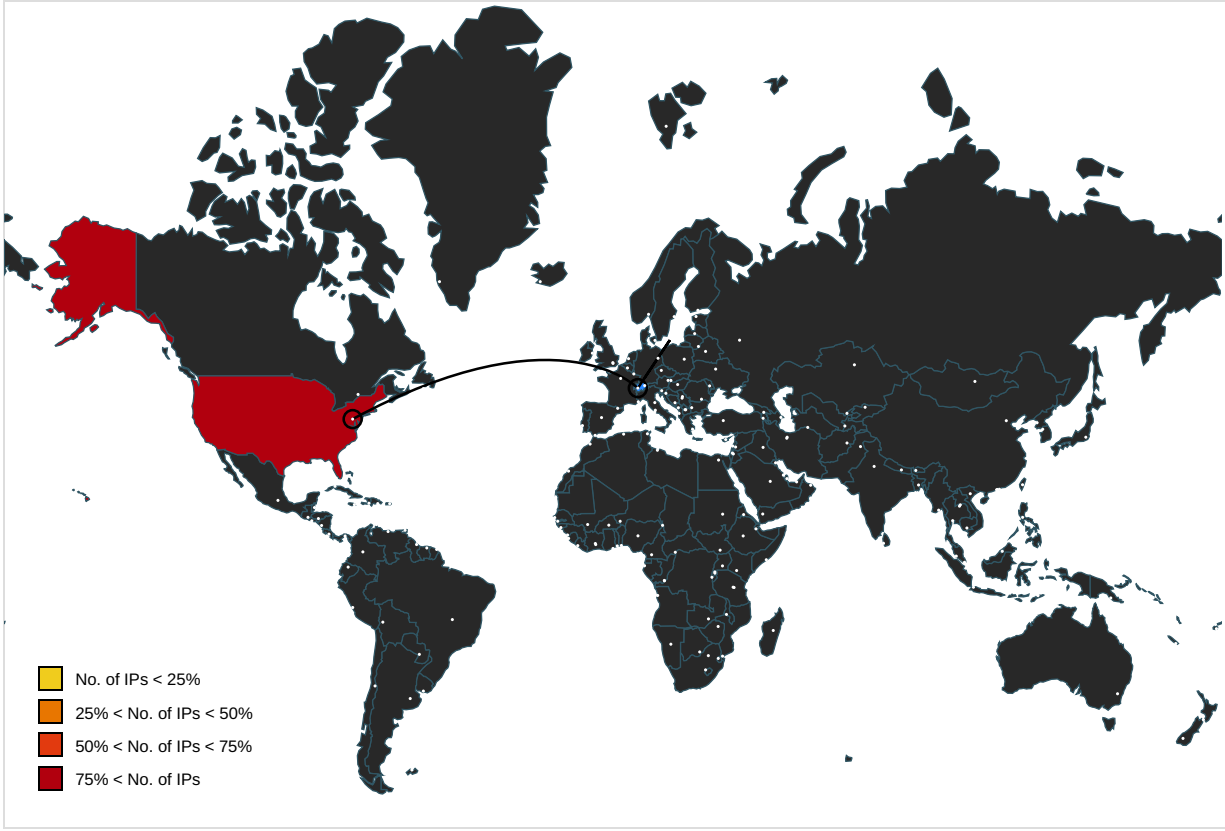
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://pub.lucidpress.com/	false		high
http://https://pub.lucidpress.com/favicon.ico	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://pub.lucidpress.com/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com	47544592-1de0-4eb7-8ede-c717ec11fa67.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://dns.google	47544592-1de0-4eb7-8ede-c717ec11fa67.tmp.1.dr, e7739206-7d4f-488d-9117-0c4ffc4ffae5.tmp.1.dr	false	• URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.0.dr	false		high
http://https://ogs.google.com	47544592-1de0-4eb7-8ede-c717ec11fa67.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://accounts.google.com	47544592-1de0-4eb7-8ede-c717ec11fa67.tmp.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://clients2.googleusercontent.com	47544592-1de0-4eb7-8ede-c717ec11fa67.tmp.1.dr	false		high
http://https://apis.google.com	47544592-1de0-4eb7-8ede-c717ec11fa67.tmp.1.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.0.dr	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.0.dr	false		high
http://https://www.google.com/	manifest.json.0.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.0.dr	false		high
http://https://clients2.google.com	47544592-1de0-4eb7-8ede-c717ec11fa67.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.226.244.72	d3v04nmt9jknbk.cloudfront.net	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.215.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635363
Start date and time: 27/05/202220:18:27	2022-05-27 20:18:27 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://pub.lucidpress.com
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:	11
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@23/84@3/6
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.203.110, 142.250.203.99, 74.125.163.198, 34.104.35.123, 80.67.82.211, 80.67.82.235, 40.125.122.176, 20.54.89.106, 52.242.101.226
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, a1449.dscg2.akamai.net, arc.msn.com, r1.sn-4g5lznle.gvt1.com, r1---sn-4g5lznle.gvt1.com, redirector.gvt1.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
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\Local\Google\Chrome\User Data\066e1eff-d36c-4e9c-8948-66526803648a.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7439677927248827
Encrypted:	false
SSDEEP:	384:FzAvXNSMZmNxVeETONrrgvHd3wPF8H10GsLrmxrvxgZBlwraHmCFy9jjDMOhprNg:NG61VypEsMezfB54nHelK/NDZc
MD5:	2588B644D1018B48E245E450CA96687F
SHA1:	06DC3E7DD09482962E30F43ADF0BCDB10AF99C5A
SHA-256:	3048CF6A2F22C941E03A2CCBE638EB93EDBCE075AB930A15B775E7B8EDCB8F10
SHA-512:	6A7D25EFBC86660F722398BFB570DBB7E95BAE9C251741633AE14B4B05F5ACEE436A9BFEA005056227763F06796433F6F4CDEA4DAC253C7B434A625CFD5C933B
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...s]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\550058c2-f2cc-480f-843e-2f73e06aab99.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7438211773058985
Encrypted:	false
SSDEEP:	384:LzAvXNSM1NSTONrrgvHd3wPF8H10GsLrmxrvxgZBlwraHmCFy9jjDMOhprNW17qI:w61VypEsMezfB54nHelK/NDZG
MD5:	53FEEA275EC46A2FBDB3EAD96C405A0F
SHA1:	9084056B63979ED11D44909A3656A590878FF380
SHA-256:	4624F44C1A492ED154E36090D52E7ECDCF7604598AC0201C9CE9F0D618592FE5
SHA-512:	2964FDA8F7D705A7C606E34B50A667D43B87BFCEFC846C628B094459AFDE490DA182B2828C0A7505A8109DC2415985735E1BA13DD58EE5828214E90F32446452
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...s]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\7405ca4f-682d-4031-86df-08e48d0a443d.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):	397820
Entropy (8bit):	6.014394464122053
Encrypted:	false
SSDEEP:	12288:alG9c+VLIJ515exzurRDn9nfNxF4ijZVtilBO:Ty+SE0RzxxPjjt8O
MD5:	6D11028B987FCA3FB11D937C94011F5A
SHA1:	FE0763A03283B37CB6F018D7B5C896D20343B369
SHA-256:	E382988B2AF7EC15AF356E3B796B059D59A2E584C0E6F52D5AAB7790E4C8EB72
SHA-512:	2F9046818CC52723B12F9B1DE656EEAEA4ADD6B01E43C3E67CDECDB36EEB16E9550B7F867148C14C0F7C7FA1778A546766879E53157541BBB567A25F080E876B
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":1.653707975453782e+12,"network":1.653675576e+12,"ticks":195389857.0,"uncertainty":3834149.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13298181572728

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):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9n:+Y66cR9
MD5:	7A9D405E9218ED86C7ED3BB729DAA896
SHA1:	E5BB69E833231B755B20E5A0C9B2392D8B923C66
SHA-256:	D83D002DFE4F96C43A6FBF24FC7AA739945731ABDEC2AFB53EDDCE2D2D87D6AF
SHA-512:	F34290BF6A4B1AA63F47436C0788FC1DAC7B970A1861EF1D1891826FD3DFD0FD484A900E23A3024C19CA93DE842BF8B5BC7A5E159362A4C3A36AE8D47C8551A7
Malicious:	false
Reputation:	low
Preview:	sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\47544592-1de0-4eb7-8ede-c717ec11fa67.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\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985D
Malicious:	false
Reputation:	low
Preview:	.f.5.....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):	5.235555621601426
Encrypted:	false
SSDEEP:	6:AX3IDVN4q2P923iKKdK25+Xqx8chI+IFUtqVfX3IFJZmwYVfX3IqDkwO923iKKdP:AXoVN4v45KkTXfchI3FUtiXYJ/IXTD5Y
MD5:	93F0B3C5CA43D28BCA38BC1DC341911D
SHA1:	7615B20C82F42F7EB3B074615FD2AEA633DE4AC0
SHA-256:	450720884265286DADD556835B5028DAE160B73BA480FECF5125526CA5F52F5D
SHA-512:	C52BFA8462BFA88972EAA5B66B18356EEEED64BDD65790484B8D7A83B4DB9DF7E4EAFEA32C8EAD25D505DCEFEAD4ADC7C1791FC4F78DA843DC94503EA8E24399
Malicious:	false
Reputation:	low
Preview:	2022/05/27-20:19:39.592 1bf0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/27-20:19:39.594 1bf0 Recovering log #3.2022/05/27-20:19:39.595 1bf0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.235555621601426
Encrypted:	false
SSDEEP:	6:AX3IDVN4q2P923iKKdK25+Xqx8chI+IFUtqVfX3IFJZmwYVfX3IqDkwO923iKKdP:AXoVN4v45KkTXfchI3FUtiXYJ/IXTD5Y
MD5:	93F0B3C5CA43D28BCA38BC1DC341911D
SHA1:	7615B20C82F42F7EB3B074615FD2AEA633DE4AC0
SHA-256:	450720884265286DADD556835B5028DAE160B73BA480FECF5125526CA5F52F5D
SHA-512:	C52BFA8462BFA88972EAA5B66B18356EEEED64BDD65790484B8D7A83B4DB9DF7E4EAFEA32C8EAD25D505DCEFEAD4ADC7C1791FC4F78DA843DC94503EA8E24399
Malicious:	false
Reputation:	low
Preview:	2022/05/27-20:19:39.592 1bf0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/27-20:19:39.594 1bf0 Recovering log #3.2022/05/27-20:19:39.595 1bf0 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\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871599185186076

Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DE CAA
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\Preferences (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5088
Entropy (8bit):	4.971507240270524
Encrypted:	false
SSDEEP:	96:norafK1pSKI9Ik0JCKL8XRykG/111CbOTQVuwn:nor31pSTC4K3kSq
MD5:	56296CB8256A5EF614F5AF4485B2A839
SHA1:	5A68CA43F89E216C5FF2519D3023EF2570949DD4
SHA-256:	5088A4050F06D58B214E4989CCA896B1579ACE84374AA92C69F60D672E1E580B
SHA-512:	F0B177C6CED4CC0F99108BE86790F49B4CD4797D9A63B3557B1B6CF4B5FDC7E3B125EEE7329EE63512CBD5E367459B050832481102DBEC72EBE4D4BE2DD66A 97
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298181574063701","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\Secure Preferences (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17703
Entropy (8bit):	5.57729977290577
Encrypted:	false
SSDEEP:	384:OivtuLlCqXB1kXqKf/pUZNCgVLH2HfDHrUg1dZ84N:0LlvB1kXqKf/pUZNCgVLH2HfbrUg/Z8+
MD5:	5DBEC31DDC61ACFA5FAC4A562FA8510A
SHA1:	32EE4C9EC3A6E17805855FD21DB241318D1EA438
SHA-256:	EEFCFE44604C11FE8152E0F7AE382C45FC6BBC7F9B61620CFEEC64479CF61D4E
SHA-512:	EB0884B1BF127E8D63D677A4B6AF9EC2ADA1EA2870AE3F763A7A269D71F92D0450ED1D39AB7E4BD2EC126455784F913BE77BF91A94468B901E3AEA4BCA16AEE7
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13298181573039080","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_i

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):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	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\e7739206-7d4f-488d-9117-0c4ffc4ffae5.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b63836ec-6635-49da-8a18-696b26a40eed.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):	17703
Entropy (8bit):	5.57729977290577
Encrypted:	false

SSDEEP:	384:OivtuLlCqXB1kXqKf/pUZNCgVLH2HfDHrUg1dZ84N:0LlvB1kXqKf/pUZNCgVLH2HfbrUg/Z8+
MD5:	5DBEC31DDC61ACFA5FAC4A562FA8510A
SHA1:	32EE4C9EC3A6E17805855FD21DB241318D1EA438
SHA-256:	EEFCFE44604C11FE8152E0F7AE382C45FC6BBC7F9B61620CFEEC64479CF61D4E
SHA-512:	EB0884B1BF127E8D63D677A4B6AF9EC2ADA1EA2870AE3F763A7A269D71F92D0450ED1D39AB7E4BD2EC126455784F913BE77BF91A94468B901E3AEA4BCA16AEE7
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13298181573039080","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ceb94f7d-df78-42a9-a54c-38066295f817.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):	5088
Entropy (8bit):	4.971507240270524
Encrypted:	false
SSDEEP:	96:norafK1pSKI9Ik0JCKL8XRykG/111CbOTQVuwn:nor31pSTC4K3kSq
MD5:	56296CB8256A5EF614F5AF4485B2A839
SHA1:	5A68CA43F89E216C5FF2519D3023EF2570949DD4
SHA-256:	5088A4050F06D58B214E4989CCA896B1579ACE84374AA92C69F60D672E1E580B
SHA-512:	F0B177C6CED4CC0F99108BE86790F49B4CD4797D9A63B3557B1B6CF4B5FDC7E3B125EEE7329EE63512CBD5E367459B050832481102DBEC72EBE4D4BE2DD66 97
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298181574063701","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","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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ

MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f3245c96-a635-48bf-9568-db938ae11702.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):	17702
Entropy (8bit):	5.5773350894792415
Encrypted:	false
SSDEEP:	384:OivtrLlCqXB1kXqKf/pUZNCgVLH2HfDHrUKS1dZ84t:BLlvB1kXqKf/pUZNCgVLH2HfbrUd/Z8m
MD5:	04D330E6C248472920F1B7CAB251ECC8
SHA1:	498A5601488CB68A0534146291E336B33F0E4A15
SHA-256:	BF8A5A8E74ED63D22D063879B8410FF92A549EC28F83811CFC1087FAB1A71D3D
SHA-512:	03E77CF338787D50FCC8000F45F6C51AE122D40454109ABD0306AB570443DC7C27851DBB6FD8A23CE4414F292BAAE5FA9F5CF5E5194D3883BC90457E2B57D66 C
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"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":"13298181573039080","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_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ffb05f2f-bad0-42b9-89f7-107a5451aef8.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 5F21
Malicious:	false
Reputation:	low
Preview:	.

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:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724

Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	397820
Entropy (8bit):	6.014394464122053
Encrypted:	false
SSDEEP:	12288:alG9c+VLIJ515exzurRDn9nfNxF4ijZVtilBO:Ty+SE0RzxxPjjt8O
MD5:	6D11028B987FCA3FB11D937C94011F5A
SHA1:	FE0763A03283B37CB6F018D7B5C896D20343B369
SHA-256:	E382988B2AF7EC15AF356E3B796B059D59A2E584C0E6F52D5AAB7790E4C8EB72
SHA-512:	2F9046818CC52723B12F9B1DE656EEAEA4ADD6B01E43C3E67CDECDB36EEB16E9550B7F867148C14C0F7C7FA1778A546766879E53157541BBB567A25F080E876B
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":1.653707975453782e+12,"network":1.653675576e+12,"ticks":195389857.0,"uncertainty":3834149.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13298181572728

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7438211773058985
Encrypted:	false
SSDEEP:	384:LzAvXNSM1NSTONrrgvHd3wPF8H10GsLrmxrvxgZBlwraHmCFy9jjDMOhprNW17qI:w61VypEsMezfB54nHelK/NDZG
MD5:	53FEEA275EC46A2FBDB3EAD96C405A0F
SHA1:	9084056B63979ED11D44909A3656A590878FF380
SHA-256:	4624F44C1A492ED154E36090D52E7ECDCF7604598AC0201C9CE9F0D618592FE5
SHA-512:	2964FDA8F7D705A7C606E34B50A667D43B87BFCEFC846C628B094459AFDE490DA182B2828C0A7505A8109DC2415985735E1BA13DD58EE5828214E90F3244645
Malicious:	false
Reputation:	low

Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...s]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\bcf295b0-4532-48d0-9438-5f63a56443f3.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):	397820
Entropy (8bit):	6.0143944278568044
Encrypted:	false
SSDEEP:	12288:mlG9c+VLIJ515exzurRDn9nfNxF4ijZVtilBO:/y+SE0RzxxPjjt8O
MD5:	07E1BCA4DD0DC7F27BAF005B8BEF9675
SHA1:	EEF82EC5DC530A132737A6130A0CA2C2B67055C8
SHA-256:	01D141E114E13447A2D16C39004D3C92E7988588044457E5D4C289062150FCD7
SHA-512:	DE62FD67451E917DC6D3135B400F8DEEA1894309C546E7EF4C58516822C5D62CCA3180B6A5F3C180EA2F8C86F714B846FBD753C8CBBBCB58C82BD0031763475
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":1.653707975453782e+12,"network":1.653675576e+12,"ticks":195389857.0,"uncertainty":3834149.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230469170993"},"policy":{"last_statistics_update":"13298181572728

C:\Users\user\AppData\Local\Google\Chrome\User Data\fd88ec9e-890a-4b2f-adf6-7e6a213e2e1d.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):	397820
Entropy (8bit):	6.014394464122053
Encrypted:	false
SSDEEP:	12288:alG9c+VLIJ515exzurRDn9nfNxF4ijZVtilBO:Ty+SE0RzxxPjjt8O
MD5:	6D11028B987FCA3FB11D937C94011F5A
SHA1:	FE0763A03283B37CB6F018D7B5C896D20343B369
SHA-256:	E382988B2AF7EC15AF356E3B796B059D59A2E584C0E6F52D5AAB7790E4C8EB72
SHA-512:	2F9046818CC52723B12F9B1DE656EEAEA4ADD6B01E43C3E67CDECDB36EEB16E9550B7F867148C14C0F7C7FA1778A546766879E53157541BBB567A25F080E876B
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":1.653707975453782e+12,"network":1.653675576e+12,"ticks":195389857.0,"uncertainty":3834149.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13298181572728

C:\Users\user\AppData\Local\Temp\4badc51e-eda6-451a-b2c3-ea89dacf7a31.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false
Reputation:	low
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\82621c0c-b3a9-40bf-afaa-d2947204b216.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\scoped_dir4324_2011126058\4badc51e-eda6-451a-b2c3-ea89dacf7a31.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false
Reputation:	low
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\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:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C
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_dir4324_2011126058\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:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CI B4
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_dir4324_2011126058\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488 CB
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_dir4324_2011126058\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_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_dir4324_2011126058\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_dir4324_2011126058\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:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "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_dir4324_2011126058\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_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\en_GB\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\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:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
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_dir4324_2011126058\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:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
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_dir4324_2011126058\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_dir4324_2011126058\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_dir4324_2011126058\CRX_INSTALL_locales\fil\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\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 7
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_dir4324_2011126058\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:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA755
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "messa ge": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	503
Entropy (8bit):	4.819520019697578
Encrypted:	false
SSDEEP:	12:YGGYpTOEu5TfIJPFJEPJEsxmfEWJEsxmfRpmJEzrMrQp5TfnHV5/WIWO/NrnLAOK:YHYpq7EJPkJExfJExRpmJE/LXzHV5/ji
MD5:	9CF848209FF50DBF68F5292B3421831C
SHA1:	D29880B7B15102469123D8747BF645706CE8595B
SHA-256:	EA1744C3CFBAA684A31A00067E8493ED114EFF3E878C797C9C55A7B122D855CD
SHA-512:	B784AEE4926F850F30072ABDA85E2E2E3966285F14BDF647BD2A41C5C06CAB04BC962584830E4E913896010396EAD02D90528235B9D9EDA1BDEFBFBB5333ED F5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikacija trenuta\u010dno nije dostupna."},"craw_connect_to_network":{"message":"Pove\u017eite se s mre\u017eom."},"app_nam e":{"message":"Pla\u0107anja u web-trgovini Chrome"},"app_description":{"message":"Pla\u0107anja u web-trgovini Chrome"},"iap_unavailable":{"message":"Pla\u0107 anje u aplikaciji trenuta\u010dno nije dostupno."},"please_sign_in":{"message":"Prijavite se na Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be c ompleted."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\hu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	612
Entropy (8bit):	4.865151680865773
Encrypted:	false
SSDEEP:	12:YGGYpiKQhMDCJNYygdGs61gdGs3piKQChMDZAYRO/NrnLAOK:YHYpzQhsiPgdG1gdGcpzQChsZAYOFvAD
MD5:	4AD92AFDE3408FBBE43B0C3C71677650
SHA1:	3488901077F336A3196F9AE116E36DF1674E1ACA
SHA-256:	61258FE04C23AE14FDC99EE846CEA71CC703990CC0F80C3934299646E86C475E
SHA-512:	EB945FA455DEB9D70033DC0A8AA55D1F47AA00214B70AD34D5419A54F9C05B267F96F9785139F452BEE6972376DDF13EE51C681845A2B0818172FB75BA1FD093
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Az alkalmaz\u00e1s jelenleg nem \u00e9rhet\u0151 el."},"craw_connect_to_network":{"message":"K\u00e9rj\u00fck, csatlakozzon egy h\u00e1l\u00f3zathoz."},"app_name":{"message":"Chrome Internetes \u00e1ruh\u00e1z Fizet\u00e9si rendszere"},"app_description":{"message":"Chrome Internetes \u00e1ruh\u00e1z Fizet\u00e9si rendszere"},"iap_unavailable":{"message":"Az alkalmaz\u00e1son bel\u00fcli fizet\u00e9s jelenleg nem \u00e9rhet\u0151 el."},"plea se_sign_in":{"message":"Jelentkezzen be a Chrome-ba."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\id\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	461
Entropy (8bit):	4.642271834875684
Encrypted:	false
SSDEEP:	12:YGGYpDBHAeSnLPo2sWo25pmo22C/SzFAAh+M9WO/NrnLAOK:YHYplHcFTpmzOptWOFvAOK
MD5:	9008516AA1D8F8C2B8ECE70B7E4963AD
SHA1:	EA7AD4BE77A80A4B9FB1E59A340010830E494747
SHA-256:	89CAB0AF2B53C6ABEB93C8C628DDCBDD286A7A2672FE03440411BB654E3A0675
SHA-512:	46534829417CAD54310BA90AD4545918A2E934508E0CC3467E367944E52315B1BC6500119214EABD40D641DD167C077935436135AF1C0DB1D1007AE98E6175FC
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikasi tidak tersedia saat ini."},"craw_connect_to_network":{"message":"Sambungkan ke jaringan."},"app_name":{"message":"P embayaran Chrome Webstore"},"app_description":{"message":"Pembayaran Chrome Webstore"},"iap_unavailable":{"message":"Pembayaran Dalam Aplikasi saat ini tidak tersedia."},"please_sign_in":{"message":"Harap masuk ke Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\it\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	464
Entropy (8bit):	4.701550173628233
Encrypted:	false
SSDEEP:	12:YGGYpmXXHEva6Plqd6Wlqd3p6PqTX2zaWO/NrnLAOK:YHYpmnkvNtdRtd3pX6+WOFvAOK
MD5:	BB9C32BA62DDA02F9471C64B5F9CF916
SHA1:	9825037D5D9185C58456CDD887C77B10A41D8C84
SHA-256:	43A0B113D3773BA78F82BB9E42DDC46F6892D0FBBB351F94A7C105E4A146E9C1
SHA-512:	4D3DB91A6251F2DD9CBF97D29805A7AC23F49988966E9B686D486B4A8CEBEA33F5502E3891D5231674061127C282C745FB87FDA7467A6172851BF6925506C8CA
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App al momento non disponibile."},"craw_connect_to_network":{"message":"Collegati a una rete."},"app_name":{"message":"Pagam enti Chrome Web Store"},"app_description":{"message":"Pagamenti Chrome Web Store"},"iap_unavailable":{"message":"La funzione Pagamenti In-App non \u00e8 al momento disponibile."},"please_sign_in":{"message":"Accedi a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	806
Entropy (8bit):	4.671841695172103
Encrypted:	false
SSDEEP:	12:YGGYpqbrR5IYstMNcXh82q8b0kOoZ46ToZ43pqbtVD2CR5IYstR0O8b0KhO/Nrnk:YHYpcFiLRMACqNpctVPieOAhOFvAOK

MD5:	96C8CBD161D3CE9CB1A46CB2CD0C6583
SHA1:	78BBFCF035B5B620E353C8E520653ADD3F4E7DB8
SHA-256:	81D8F1D9F72B3139BC5D9845BCF82990308FB6175D07514D8238B1E6D5D02E8A
SHA-512:	692468B7B44D961D8248BBC30CC11DE9F3F7E89D01A609E6CB71CAF653D8212C15DFA834C5FB6E8261FD21A25E9616861C0A3FC01DB27CBBE79C3FDE2C654 DD
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u30a2\u30d7\u30ea\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u305b\u3093\u3002"},"craw_con nect_to_network":{"message":"\u30cd\u30c3\u30c8\u30ef\u30fc\u30af\u306b\u63a5\u7d9a\u3057\u3066\u304f\u3060\u3055\u3044\u3002"},"app_name":{"message": "Chrome \u30a6\u30a7\u30d6\u30b9\u30c8\u30a2\u6c7a\u6e08"},"app_description":{"message":"Chrome \u30a6\u30a7\u30d6\u30b9\u30c8\u30a2\u6c7a\u6e08"},"ia p_unavailable":{"message":"\u30a2\u30d7\u30ea\u5185\u30da\u30a4\u30e1\u30f3\u30c8\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u3 05b\u3093\u3002"},"please_sign_in":{"message":"Chrome \u306b\u30ed\u30b0\u30a4\u30f3\u3057\u3066\u304f\u3060\u3055\u3044\u3002"},"jwt_retrieve_failed": {"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\ko\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	656
Entropy (8bit):	4.88216622785951
Encrypted:	false
SSDEEP:	12:YGGYpqHZMskkrcaw6cT/pb8pqHkrskeQV7wUO/NrnLAOK:YHYpsrkYcawwps5kdwUOFvAOK
MD5:	3CAF23A8EA2332D78B725B6C99EC3202
SHA1:	95C3504F55A929449EF2E3AB92014562AACD39AD
SHA-256:	BFE72BBC492B9018A599CB6575366696E431E6A38400E4B2ED06EAE3340D3AE5
SHA-512:	C000FCCB567D3590D4C401005E78C539961455BB13686296EC4FF7018BB0A4DAB2DA96FBDAA33D999C1409B5796932370219B3FF8490B671586DEBD6145519D
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\ud604\uc7ac \uc571\uc744 \uc0ac\uc6a9\ud560 \uc218 \uc5c6\uc2b5\ub2c8\ub2e4."},"craw_connect_to_network":{"messag e":"\ub124\ud2b8\uc6cc\ud06c\uc5d0 \uc5f0\uacb0\ud558\uc138\uc694."},"app_name":{"message":"Chrome \uc6f9 \uc2a4\ud1a0\uc5b4 \uacb0\uc81c"},"app_description": {"message":"Chrome \uc6f9 \uc2a4\ud1a0\uc5b4 \uacb0\uc81c"},"iap_unavailable":{"message":"\ud604\uc7ac \uc778\uc571 \uacb0\uc81c\ub97c \uc0ac\uc6a9\ud560 \uc218 \uc5c6\uc2b5\ub2c8\ub2e4."},"please_sign_in":{"message":"Chrome\uc5d0 \ub85c\uadf8\uc778\ud558\uc138\uc694."},"jwt_retrieve_failed":{"message":"The tra nsaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	576
Entropy (8bit):	4.846810495221701
Encrypted:	false
SSDEEP:	12:YGGYpmEOnxwkD9AMoAYQa9AMoAYNpALveYAyO/NrnLAOK:YHYpmznayAMHcAMHQpAzeYAyOFvAOK
MD5:	41F2D63952202E528DBBB683B480F99C
SHA1:	9DD998542DBE6609299D4A5A25364A32FA7D7865
SHA-256:	FF7C083CD1E6134DD8263C634336EB852274BAD1BFAD18762814C42BC65309D8
SHA-512:	7BD2E2D4264C6BD62DF2584F3C1D3A910C5C5A28F4532F1E8F0C2235E93714EDD6074EA24960D4DEB4F9125DA81CA813F06330EFF66FA8DF1552D1DAC68644 E
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Programa \u0161iuo metu negalima."},"craw_connect_to_network":{"message":"Prisijunkite prie tinklo."},"app_name":{"message": "\u201eChrome\u201c internetin\u0117s parduotuv\u0117s mok\u0117jimo sistema"},"app_description":{"message":"\u201eChrome\u201c internetin\u0117s pard uotuv\u0117s mok\u0117jimo sistema"},"iap_unavailable":{"message":"Mok\u0117jimai programoje \u0161iuo metu negalimi."},"please_sign_in":{"message":"Prisijunkite prie \u201eChrome\u201c."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	584
Entropy (8bit):	4.856464171821628
Encrypted:	false
SSDEEP:	12:YGGYp6nQ11155y9k5hInf6whInf3pRKbqk0R5VR8WO/NrnLAOK:YHYpp11dy9iIdIvpc2ZgWOFvAOK
MD5:	1D21ED2D46338636E24401F6E56E326F

SHA1:	24497EDB25724BC4A57823C5CD06F50DB9647DD4
SHA-256:	434A375C32B8A21C435511C551F740FD4D170EC528A8F4EFC3D798EA4A07B606
SHA-512:	10A870718CC6281EE09DE01900D303B06589D9281C5849D6105C6FCF58BFFA3855F29C6ECA3689FFE6EF304BABCF41C5700EE2D8AFE711D57CB711194366FA6A
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Lietotne pagaid\u0101m nav pieejama."},"craw_connect_to_network":{"message":"L\u016bdzu, izveidojiet savienojumu ar t\u012bklu."},"app_name":{"message":"Chrome interneta veikala maks\u0101jumu sist\u0113ma"},"app_description":{"message":"Chrome interneta veikala maks\u0101jumu sist\u0113ma"},"iap_unavailable":{"message":"Maks\u0101jumi lietotn\u0113s pa\u0161laik nav pieejami."},"please_sign_in":{"message":"L\u016bdzu, pierakstieties p\u0101rl\u016bk\u0101 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\nb\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	501
Entropy (8bit):	4.804937629013952
Encrypted:	false
SSDEEP:	12:YGGYpB928UZjdyE9iDCiop8682fURHWO/NrnLAOK:YHYpXK/iOiop8NFHWOFvAOK
MD5:	8F0168B9A546D5A99FD8A262C975C80E
SHA1:	B0718071BD0B7251D4459E9C87DF50C14622FBD6
SHA-256:	F03FA7384DF79EBA6E0274D570996030F595A3BF6B781929DD9DB6593262E41F
SHA-512:	A1191CDC496DDD7470BDCFAF186BB9488767159E0CA6A6242D195FA3351704DC8F8BBD03DBEE57D37BBD897C9E8D14B7325FB37D58AC80DEC0F972FF89375B8
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen er utilgjengelig for \u00f8yeblikket."},"craw_connect_to_network":{"message":"Du m\u00e5 koble til et nettverk."},"app_name":{"message":"Chrome Nettmarked-betalinger"},"app_description":{"message":"Chrome Nettmarked-betalinger"},"iap_unavailable":{"message":"Betaling i app er ikke tilgjengelig for \u00f8yeblikket."},"please_sign_in":{"message":"Du m\u00e5 logge p\u00e5 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	472
Entropy (8bit):	4.651254944398292
Encrypted:	false
SSDEEP:	12:YGGYpqK5XUoE32GFM2GapUEn7v0WO/NrnLAOK:YHYp/XaLeLapUEgWOFvAOK
MD5:	E7F74DCE7B6411E4E0D95E9252CF74FA
SHA1:	33CC6C73C5F8D0144C0260C2E5A9BD0DB3EF6477
SHA-256:	3564AEF46C01602B19CC29FD8A79676C543427EDE98206D0C91B33AF0CCF3977
SHA-512:	B0987002F8BC4F0B0AC41A87E90BA729464BF2F34D1CC413DD3837019F5F37FD46EB9E9FDABB97F5BDCB50768ABF808AF6E7C531CD7BCA477C71990D2F13335B
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App momenteel niet beschikbaar."},"craw_connect_to_network":{"message":"Maak verbinding met een netwerk."},"app_name":{"message":"Betalingen via Chrome Web Store"},"app_description":{"message":"Betalingen via Chrome Web Store"},"iap_unavailable":{"message":"In-app-betalingen is momenteel niet beschikbaar."},"please_sign_in":{"message":"Log in bij Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	549
Entropy (8bit):	4.978056737225237
Encrypted:	false
SSDEEP:	12:YGGYpTHlBqHdqcUP5Qp0mAW5Qp0mdpm5Qp0p9JqD2WO/NrnLAOK:YHYpRMdO5bmj5bmdpm5bLJBWOFvAOK
MD5:	E16649D87E4CA6462192CF78EBE543EC
SHA1:	53097D592B13F3C1370366B25024EA72208B136A
SHA-256:	EB435F7460A63576CA1ECB51948E7A3AD5168D2F175AE2B5836D469672923D84
SHA-512:	6EC702CEC6E312CAC6F33109A57F7D83A3F073F2F9A9BD42DB0F91A36F87D800EEB978C69023B6A0E00B86ECE3E1024C269F89D038F0926619F40D075F6689D

Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikacja jest obecnie niedost\u0119pna."},"craw_connect_to_network":{"message":"Po\u0142\u0105cz si\u0119 z sieci\u0105."},"app_name":{"message":"P\u0142atno\u015bci w sklepie Chrome Web Store"},"app_description":{"message":"P\u0142atno\u015bci w sklepie Chrome Web Store"},"iap_unavailable":{"message":"P\u0142atno\u015bci w ramach aplikacji s\u0105 teraz niedost\u0119pne."},"please_sign_in":{"message":"Zaloguj si\u0119 w Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\pt_BR\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	513
Entropy (8bit):	4.734605177119403
Encrypted:	false
SSDEEP:	12:YGGYpGAV9hv3/1PIc6WIc3paIBMMAV+KcIWO/NrnLAOK:YHYpGwLvt5R53pacHw1pWOFvAOK
MD5:	1F4BC8A5EFD59D61127ABEECD4B6CAE3
SHA1:	8647B4D2D643AE4F784ABDDC50D87A39AD02971A
SHA-256:	E1950CBBF056F068EA56160DDB318F3E6232BFBBE096D221C7CA6FCAACE2A8B9
SHA-512:	B58A95BBBC0A16B06826684198B481D2E15A7C760956721C3B538C62C902873A7856F328506457EE66311E45D7A16A4AAAC85B12853AA7EF09780189D28EB3DE
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplicativo indispon\u00edvel no momento."},"craw_connect_to_network":{"message":"Conecte-se a uma rede."},"app_name":{"message":"Pagamentos da Chrome Web Store"},"app_description":{"message":"Pagamentos da Chrome Web Store"},"iap_unavailable":{"message":"No momento, os Pagamentos no aplicativo n\u00e3o est\u00e3o dispon\u00edveis."},"please_sign_in":{"message":"Fa\u00e7a login no Google Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\pt_PT\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	503
Entropy (8bit):	4.742240430473613
Encrypted:	false
SSDEEP:	12:YGGYpmvMAV9BKx1PIZUFWIZUapITEpBqMAVCWWO/NrnLAOK:YHYpmvMwOxtEUIEUapITqMwCWWOFvAD
MD5:	D80ECE7E4B3741CD9CD29B89D006B864
SHA1:	8F0D587B78E36861ED00524ABF886FA20E14CAE4
SHA-256:	C8FF9ACAEA1D3B6F8483339CB40F66BC563CCA8DD87F2337F813C492B20F451B
SHA-512:	8A53D9618BBD1A62CD48501E5620932631C1B045612082D99429628D2BF4409AEE3FA695107E82037B5CB332111C456CF3A74235C66B61380CF1E382914F1088
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplica\u00e7\u00e3o atualmente indispon\u00edvel."},"craw_connect_to_network":{"message":"Ligue-se a uma rede."},"app_name":{"message":"Pagamentos via Chrome Web Store"},"app_description":{"message":"Pagamentos via Chrome Web Store"},"iap_unavailable":{"message":"Os Pagamentos na app est\u00e3o atualmente indispon\u00edveis."},"please_sign_in":{"message":"Inicie sess\u00e3o no Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\ro\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	554
Entropy (8bit):	4.8596885592394505
Encrypted:	false
SSDEEP:	12:YGGYpqOHHEG7PMeH8EPJWb2r9EWJWb2r9RpmJW9FjkUhI3C7PMdWO/NrnLAOK:YHYpbnEG7PjIJBfJBRpmJmBh57PEWOFY
MD5:	D63E66B94A4EA2085D80E76209582FB1
SHA1:	4ECAC3EB64DD6253310A0776E6D42257FC290D77
SHA-256:	91A5AAD210C3E0241106E8821B3897EDEFEC9D85033C94DB2324FF3A5FDE5AC7
SHA-512:	09AC34CF286FD0730EED4F6DB3E2FD00A026D0F42DCC75AE49B045DDAD38DFA38B0FB7823ECAC8B0A9BC2A89F4EAF4BCE081779F2ECDF6CC39286045577DC5C9
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"\u00cen prezent, aplica\u021bia nu este disponibil\u0103."},"craw_connect_to_network":{"message":"Conecteaz\u0103-te la o re \u021bea."},"app_name":{"message":"Pl\u0103\u021bi prin Magazinul web Chrome"},"app_description":{"message":"Pl\u0103\u021bi prin Magazinul web Chrome "},"iap_unavailable":{"message":"Pl\u0103\u021bile \u00een aplica\u021bie nu sunt disponibile momentan."},"please_sign_in":{"message":"Conecteaz\u0103-te la Chr ome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\ru\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1165
Entropy (8bit):	4.224419823550506
Encrypted:	false
SSDEEP:	24:YHYpNQVFc0BHlbZ0JRiKUG0L6RqQV9zJd0L6RqQV9zJRp00EQVqaQVFc0BRTlPzU:YHYpNQLHFQYKA6wQTz+6wQTz3paQAaQ8
MD5:	22F9E62ABAD82C2190A839851245A495
SHA1:	E7F79BD875918F0D0799DB5F45FAC6297FB66AF7
SHA-256:	9FC1167626C97BCBFDAFF23C6033A44252F89A501AF1DF41C43CB3A994FEB09F
SHA-512:	F577F2F0C344C4E4050AF025A9FB9AC78CADF7FE177F63AB9863826A9808B7FBF5D3363E3B61D7A6DB083EF5EBAC5474D710347B701640AB9C229A3E5D1F0A4 8
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u0440\u0438\u043b\u043e\u0436\u0435\u043d\u0438\u0435 \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043 d\u043e."},"craw_connect_to_network":{"message":"\u041f\u043e\u0434\u043a\u043b\u044e\u0447\u0438\u0442\u0435\u0441\u044c \u043a \u0441\u0435\u0442\u0438 \u0438\u043d\u0442\u0435\u0440 438."},"app_name":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u0430 \u0418\u043d\u0442\u0435\u0440\u043d\u0435\u0442-\u043c\u0430\u0433\u0430\u0437\u0438\u043d Chrome"},"app_description":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u0430\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u0430 \u0418\u043d\u0442\u0435\u0440\u043d\u0435\u0442-\u043c\u0430\u0433\u0430\u0437\u0438\u043 37\u0438\u043d\u0430 Chrome"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u0435\u043d\u0438 \u0447\u0435\u0440\u0435\u0437 \u043f\u0440\u0438\u043b\u043e\u0436\u0435\u043d\u0438\u0435 \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043 38\u043b\u043e\u0436\u0435\u043d\u0438\u044f \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0430."},''

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\sk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	548
Entropy (8bit):	4.850036636276313
Encrypted:	false
SSDEEP:	12:YGGYprMpsgCmIkPJE7ZEWJE7ZRpmJEtMxfAVADJ4ZAvIWO/NrnLAOK:YHYprMFCmvJE7ZfJE7ZRpmJEtMSVGKZo
MD5:	4BBAA10FD00AADBBA3EF6E805E8E1A62
SHA1:	1991901BD6A20C4A7977F09DF30C0CFF0524C504
SHA-256:	906C4F7FDDE15DE4C841E7910BBF14D9175E894BCB244B56E8447A5ADFA5B7AB
SHA-512:	3490F8826E3DB0C8B4FE7B1866DA27F6585ADF52E74392A592A60A916E8A784FF7B92B3DE8985084546D663588369D9BB03FCB25196B7F9C6DF607BEB7DEF01(
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplik\u00e1cia moment\u00e1lne nie je dostupn\u00e1."},"craw_connect_to_network":{"message":"Pripojte sa k sieti."},"app_name": {"message":"Platby Internetov\u00e9ho obchodu Chrome"},"app_description":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"iap_unavailable":{"message": "Platby v aplik\u00e1cii moment\u00e1lne nie s\u00fa k dispoz\u00edcii."},"please_sign_in":{"message":"Prihl\u00e1ste sa do prehliada\u010da Chrome."},"jwt_retr ieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\sl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	494
Entropy (8bit):	4.7695148367588285
Encrypted:	false
SSDEEP:	12:YGGYpTOEtyPFTEPJEsvmfEWJEsvmfRpmJEiArERfH5/4WO/NrnLAOK:YHYpqoyPRAJEs4fJEs4RpmJEi6AfH5/x
MD5:	F45DE58765A37FD095319D7DEB0F2FB6
SHA1:	B585A485C9BC1982EDF7AE0B9AC73A8E91D41CB5
SHA-256:	8366774AA582035BC7D949F4E28FAEC371C305D01404DF56FFF5A78B4F6ECDB7
SHA-512:	F86334E6E6F90961AD9C8E7DD1A4E923476249469180AC69D9DE59746FE26FAECB585898FC50310380F20CEB0971CA1EB7B55046DA75276840AEA6BAFF574E6(
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"Aplikacija trenutno ni na voljo."},"craw_connect_to_network":{"message":"Pove\u017eite se z omre\u017ejem."},"app_name":{"message":"Pla\u010dila v spletni trgovini Chrome"},"app_description":{"message":"Pla\u010dila v spletni trgovini Chrome"},"iap_unavailable":{"message":"Pla\u010dila v aplikacijah trenutno niso na voljo."},"please_sign_in":{"message":"Prijavite se v Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\sr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1152
Entropy (8bit):	4.2078334514915685
Encrypted:	false
SSDEEP:	24:YHYpY0f7BxQVnRl5LRO1QV1J0V8aQVEeORbo0V8aQVEeORbIp00V4i0f7BXR2QVj:YHYpV9xQVP5LyQHQQc/QcGpcH9XR2QVj
MD5:	92C1FAC62EB7F92EC3794D4A141BEF32
SHA1:	2AFA41BF51BF9A1089B0B92A9D2DC74299B79813
SHA-256:	9DF154C93B02695AF1CC39F085D9D178EC6AF131A62C2AFC65F125F8F9A5B7AC
SHA-512:	D0709E4F586EAC03548A47D72156CF48D9B4EB9AF9ED8335DF75F541AE1B4172541647EC8BA081965647A9EAE10DB342F87558977BE6075B2D3CC5C3995ED6EE
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0410\u043f\u043b\u0438\u043a\u0430\u0446\u0438\u0458\u0430 \u0458\u0435 \u0442\u0440\u0435\u043d\u0443\u0442\u043d\u043e \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0430."},"craw_connect_to_network":{"message":"\u041f\u043e\u0432\u0435\u0436\u0438\u0442\u0435 \u0441\u0435 \u0441\u0430 \u0438\u043d\u0442\u0435\u0440\u043d\u0435\u0442\u043e\u043c."},"app_name":{"message":"\u041f\u043b\u0430\u045b\u0430\u045a\u0430 \u0443 Chrome \u0432\u0435\u0431-\u043f\u0440\u0435\u0434\u0430\u0432\u043d\u0438\u0446\u0438"},"app_description":{"message":"\u041f\u043b\u0430\u045b\u0430\u045a\u0430 \u0443 Chrome \u0432\u0435\u0431-\u043f\u0440\u0435\u0434\u0430\u0432\u043d\u0438\u0446\u0438"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u045b\u0430\u045a\u0430 \u0443 \u0430\u043f\u043b\u0438\u043a\u0430\u0446\u0438\u0458\u0438 \u0441\u0443 \u0442\u0440\u0435\u043d\u0443\u0442\u043d\u043e \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0435."},"please_sign_in":{"message":"\u041f\u04

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\sv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	523
Entropy (8bit):	4.788896709100935
Encrypted:	false
SSDEEP:	12:YGGYpg6hVGZE3aFMaap8Sp5b6hwUwrdIWO/NrnLAOK:YHYpg6hPaeaap8Sr6hwXIWOFvAOK
MD5:	6E1BE9CEE29818E54E3D1C7D483DD6F7
SHA1:	B9DD926B60E225C5BE8A1DBB7EF3ACE422A204A9
SHA-256:	E348583D8C53F4A5DEC4551DA93785C17108466E427E06F84708AA383EA0E326
SHA-512:	3ADB32C0F098E064B774E7E7F615F54C44ADFB3BFC554B06A17048C6077C5885D42BD89F6733D64D65EA1785033B36B386EF0B6661FD539855484EA5A2900BB7
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen \u00e4r inte tillg\u00e4nglig f\u00f6r tillf\u00e4llet."},"craw_connect_to_network":{"message":"Anslut till ett n\u00e4tverk."},"app_name":{"message":"Betalning via Chrome Web Store"},"app_description":{"message":"Betalning via Chrome Web Store"},"iap_unavailable":{"message":"Betalning i appen \u00e4r inte tillg\u00e4ngligt f\u00f6r n\u00e4rvarande."},"please_sign_in":{"message":"Logga in i Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\th\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	4.09652661599029
Encrypted:	false
SSDEEP:	24:YHYpqQV8k6Nvgnd0BQV3d0BQV5pWdPiWdBy7MIoWOFvAOK:YHYpqQ+k6NUaBQlaBQXpW3dBUMIehQ
MD5:	283D5177FB2FC7082967988E2683EC7C
SHA1:	DEDE43967F3CEF9D9325F140872A63BFCE2AA8C5
SHA-256:	E8D5820BDE31B66A7641068FDEDD1A5F20C1A783460B98887A670F38422099CF
SHA-512:	74413C00C58B7136038D4C41D5C7C79EC02A9830779ABB719D72536B74C5E338B1548A20290559FB3F4E2A938B728CF99041050DD1970848EE9A6590EB0AB3E4
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"\u0e44\u0e21\u0e48\u0e2a\u0e32\u0e21\u0e32\u0e23\u0e16\u0e43\u0e0a\u0e49\u0e07\u0e32\u0e19\u0e41\u0e2d\u0e1b\u0e44\u0e14\u0e49\u0e43\u0e19\u0e02\u0e13\u0e30\u0e19\u0e35\u0e49"},"craw_connect_to_network":{"message":"\u0e42\u0e1b\u0e23\u0e14\u0e40\u0e0a\u0e37\u0e48\u0e2d\u0e21\u0e15\u0e48\u0e2d\u0e01\u0e31\u0e1a\u0e40\u0e04\u0e23\u0e37\u0e2d\u0e02\u0e48\u0e32\u0e22"},"app_name":{"message":"\u0e23\u0e30\u0e1a\u0e1a\u0e0a\u0e33\u0e23\u0e30\u0e40\u0e07\u0e34\u0e19\u0e02\u0e2d\u0e07 Chrome \u0e40\u0e27\u0e47\u0e1a\u0e2a\u0e42\u0e15\u0e23\u0e4c"},"app_description":{"message":"\u0e23\u0e30\u0e1a\u0e1a\u0e0a\u0e33\u0e23\u0e30\u0e40\u0e07\u0e34\u0e19\u0e02\u0e2d\u0e07 Chrome \u0e40\u0e27\u0e47\u0e1a\u0e2a\u0e42\u0e15\u0e23\u0e4c"},"iap_unavailable":{"message":"\u0e23\u0e30\u0e1a\u0e1a\u0e0a\u0e33\u0e23\u0e30\u0e40\u0e07\u0e34\u0e19\u0e43\u0e19\u0e41\u0e2d\u0e1b\u0e1e\u0e25\u0e34\u0e40\u0e04\u0e0a\u0e31\u0e19\u0e44\u0e21\u0e48\u0e1e\u0e23\u0e49\u0e2d\u0e21\u0e4

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\tr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	572
Entropy (8bit):	4.93347615778905
Encrypted:	false
SSDEEP:	12:YGGYpFh852XmYG45SfVVh5SX8pFBkw452kK/O/NrnLAOK:YHYpFhJ2Y95AJ5l8pFhlkwOFvAOK
MD5:	1BF2AA4BB904B406C9C2B7DF769BB540
SHA1:	8D29C4B7A79AB0657747CA194D1934292A46D2A8
SHA-256:	0F2E8285BA3E2BDBA6B16435FB941B07159AACFAC80196AD5941B79AB52B712A
SHA-512:	0DF48AE0A518A940489E91D8A0D6E7E47A3153747358E06CD792BFA3D826F47FA1502268F602E7D7EDFC1C111AEB3FAF0E67F845986DDA77E2FC4B3336BCF46C
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Uygulama \u015fu anda kullan\u0131lam\u0131yor."},"craw_connect_to_network":{"message":"L\u00fctfen bir a\u011fa ba\u011flan\u0131n."},"app_name":{"message":"Chrome Web Ma\u011fazas\u0131 \u00d6demeleri"},"app_description":{"message":"Chrome Web Ma\u011fazas\u0131 \u00d6demeleri"},"iap_unavailable":{"message":"Uygulama \u0130\u00e7i \u00d6demeler \u015fu anda kullan\u0131lamaz."},"please_sign_in":{"message":"L\u00fctfen Chrome'da oturum a\u00e7\u0131n."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\uk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1088
Entropy (8bit):	4.268588181103308
Encrypted:	false
SSDEEP:	24:YHYpNQVVQVrll5eN7jAQVF0Zz0id0Zz0iRp00AQVqaQVVQVSMQVvjlkYHA1RnWOi:YHYpNQPQZ75exkQAz0/z00p2QAaQPQQN
MD5:	FD1C9890679036E1AD914218753B1E8E
SHA1:	58160F7A0FC94110A2876223E406A517C8E2660B
SHA-256:	39D19CC3387FFCE13A8F11DAD72E2FCBB7CD1A4367EC699AD7C40D6F52ECE717
SHA-512:	03E81C398EE6A5DC65A40CA07E1A4CBEC2662D2C151A76C9ECB813587D672AC71311C39C5C5DA8A1AE78A3A6CE3938609D1365F7819424FC34289C7743DF002
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u0440\u043e\u0433\u0440\u0430\u043c\u0430 \u0442\u0438\u043c\u0447\u0430\u0441\u043e\u0432\u043e \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0430."},"craw_connect_to_network":{"message":"\u041f\u0456\u0434\u2019\u0454\u0434\u043d\u0430\u0439\u0442\u0435\u0441\u044f \u0434\u043e \u0456\u043d\u0442\u0435\u0440\u043d\u0435\u0442\u0443."},"app_name":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u0456 \u0412\u0435\u0431-\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0443 Chrome"},"app_description":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u0456 \u0412\u0435\u0431-\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0443 Chrome"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u0456 \u0447\u0435\u0440\u0435\u0437 \u043f\u0440\u043e\u0433\u0440\u0430\u043c\u0443 \u0437\u0430\u0440\u0430\u0437 \u043d\u0435 \u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0456."},"please_sign_in":{"message":"\u0423\u0432\u0456\u0439\u0434\u0456\u0442\u044c \u0443

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\vi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.846531831162704
Encrypted:	false
SSDEEP:	12:YGGYpqp80NORWLNiNI2k8yypSNiNI2k8yy+piNiNI2miI80NO5WO/NrnLAOK:YHYpmvNcCgWgUpudiIvN6WOFvAOK
MD5:	7D52E9357AB847B4CC8DBC8CC4DA93F5
SHA1:	AF877F3992D8056C8F08462BD575595BF79FE5B0
SHA-256:	313F71F3FFDCEFC76FC746FF2029FBF8FBE38BD83DCF952FC3DDCD8AA96D5CFB
SHA-512:	E66E7FACDF35A0F72AC61DEAAEC43A2DAC976CADEA146EBE3E90E739178F173E32ADCF909F05F2657F2AD66E2ECB6015F6733CEA4B9E42337246469F89D3A12F

Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u1ee8ng d\u1ee5ng hi\u1ec7n kh\u00f4ng kh\u1ea3 d\u1ee5ng."},"craw_connect_to_network":{"message":"Vui l\u00f2ng k\u1ebft n\u1ed1i v\u1edbi m\u1ea1ng."},"app_name":{"message":"Thanh to\u00e1n tr\u00ean c\u1eeda h\u00e0ng Chrome tr\u1ef1c tuy\u1ebfn"},"app_description":{"message":"Thanh to\u00e1n tr\u00ean c\u1eeda h\u00e0ng Chrome tr\u1ef1c tuy\u1ebfn"},"iap_unavailable":{"message":"Thanh to\u00e1n trong \u1ee9ng d\u1ee5ng hi\u1ec7n kh\u00f4ng kh\u1ea3 d\u1ee5ng."},"please_sign_in":{"message":"Vui l\u00f2ng \u0111\u0103ng nh\u1eadp v\u00e0o Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\zh_CN\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	602
Entropy (8bit):	4.917339139635893
Encrypted:	false
SSDEEP:	12:YGGYpqrL0MdI1i1kovbdKD/vbdKopqIQfvJ19KhO/NrnLAOK:YHYpMLfjvsTvsop3QPAOFvAOK
MD5:	393680A09DEE0CB9046A62BDC0750B74
SHA1:	54E7F8215061A4AB241B87AE4E81C8F860EB2C2B
SHA-256:	D5FB52C2897FD5C294784DB63C933AC77C609D10AC91431CCB295D87452CBEE6
SHA-512:	14C214CAEFC69B085E918F492C75E2A48BC6A9C2D347D29403B26E69A474825E302A3E106710E5C04E047BD57EE684A67846A5DE956705FFBF41BB0614B8CEB2
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u5e94\u7528\u76ee\u524d\u65e0\u6cd5\u4f7f\u7528\u3002"},"craw_connect_to_network":{"message":"\u8bf7\u8fde\u63a5\u5230\u7f51\u7edc\u3002"},"app_name":{"message":"Chrome \u7f51\u4e0a\u5e94\u7528\u5e97\u4ed8\u6b3e\u7cfb\u7edf"},"app_description":{"message":"Chrome \u7f51\u4e0a\u5e94\u7528\u5e97\u4ed8\u6b3e\u7cfb\u7edf"},"iap_unavailable":{"message":"\u76ee\u524d\u65e0\u6cd5\u4f7f\u7528\u5e94\u7528\u5185\u4ed8\u6b3e\u3002"},"please_sign_in":{"message":"\u8bf7\u767b\u5f55 Chrome\u3002"},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_locales\zh_TW\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	680
Entropy (8bit):	4.916281462386558
Encrypted:	false
SSDEEP:	12:YGGYpqI8ROuDWMg0kP2uD/vbd8Em2uD/vbd8RpqI8RauDRsXwvC/KhO/NrnLAOK:YHYp38suDUSuD/v2OuD/v2Rp38cuDGbq
MD5:	CD30D132A7213FC1B7E03C6D0A49CCF7
SHA1:	1141DED39023B821FE9BB4682E0D1EB5469DAF76
SHA-256:	5717F13D10E63255947F750C79CBB6BD04A6D97A08261E8D5764AF5EB0561A28
SHA-512:	0DCD3CEB93AB58655551B00D7AD4FE4A6F1F6B24EDD31244FF9B57AE529BF1A9E0220A6258C64790F9CC9F026AB9DA3AEE1575809CC94DC4F8754194C958FD19
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u76ee\u524d\u7121\u6cd5\u4f7f\u7528\u9019\u500b\u61c9\u7528\u7a0b\u5f0f\u3002"},"craw_connect_to_network":{"message":"\u8acb\u9023\u4e0a\u7db2\u8def\u3002"},"app_name":{"message":"Chrome \u7dda\u4e0a\u61c9\u7528\u7a0b\u5f0f\u5546\u5e97\u4ed8\u6b3e\u7cfb\u7d71"},"app_description":{"message":"Chrome \u7dda\u4e0a\u61c9\u7528\u7a0b\u5f0f\u5546\u5e97\u4ed8\u6b3e\u7cfb\u7d71"},"iap_unavailable":{"message":"\u76ee\u524d\u7121\u6cd5\u4f7f\u7528\u61c9\u7528\u7a0b\u5f0f\u5167\u4ed8\u6b3e\u529f\u80fd\u3002"},"please_sign_in":{"message":"\u8acb\u767b\u5165 Chrome\u3002"},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL_metadata\verified_contents.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):	7780
Entropy (8bit):	5.791315351651491
Encrypted:	false
SSDEEP:	192:RktDNJ2UzsL5KcASyoH+CouKP/iNGRo/oRHMIT:AZQflcsU
MD5:	0834821960CB5C6E9D477AEF649CB2E4
SHA1:	7D25F027D7CEE9E94E9CBDEE1F9220C8D20A1588
SHA-256:	52A24FA2FB3BCB18D9D8571AE385C4A830FF98CE4C18384D40A84EA7F6BA7F69
SHA-512:	9AEAFC3ECE295678242D81D71804E370900A6D4C6A618C5A81CACD869B84346FEAC92189E01718A7BB5C8226E9BE88B063D2ECE7CB0C84F17BB1AF3C5B1A3C4
Malicious:	false

Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfbG9jYWxlcy9iZy9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiZHUtdGRPdUNWcmxDY254Q0poRkg2NXpLU05vb1RiUE56bDNHbzdRMGJ3SSJ9LHsicGF0aCI6Il9sb2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJ6ZGtWaF9XdkxJWlhkck5xWHBvSHNRMGh1ZGtSM2d1QlMzb2VsTEZLNklVIn0seyJwYXRoIjoiX2xvY2FsZXMvZWwvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6ImgyaEZ0YUJoLXJQUEtoUm00QkFWM0VEZmhFbnh5MElGOVhYT3Z0aHhlNjAifSx7InBhdGgiOiJfbG9jYWxlcy9lbi9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoid0pSZDFmM3NxMERFVTJHLXd
C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\craw_background.js	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	544643
Entropy (8bit):	5.385396177420207
Encrypted:	false
SSDEEP:	6144:abyfBNC2FRdjiRXqbe5Dq31IVlMqX+wd5/CcMMJcRULt0NjyTOEzZQ+h72W3GB0n:Ft/g
MD5:	6EEBED29E6A6301E92A9B8B347807F5F
SHA1:	65DFB69B650560551110B33DCBA50B25E5B876DE
SHA-256:	04CD9494B0ED83924DAD12202630B20D053D9E2819C8E826A386C814CC0A1697
SHA-512:	FEDE6DB31F2AD242E7BC7B52A8859BA7F466A0B920A8DADCB32DCFB5B2A2742E98B767FF22E0C5BC5C11FEC021240AA9E458486C9039EB4EBE5CF6AF7BE97BF2
Malicious:	false
Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var d,e=e||{};e.scope={};e.arrayIteratorImpl=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}};};e.arrayIterator=function(a){return{next:e.arrayIteratorImpl(a)}};e.ASSUME_ES5=!1;e.ASSUME_NO_NATIVE_MAP=!1;e.ASSUME_NO_NATIVE_SET=!1;e.SIMPLE_FROUND_POLYFILL=!1;e.ISOLATE_POLYFILLS=!1;e.FORCE_POLYFILL_PROMISE=!1;e.FORCE_POLYFILL_PROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;.e.defineProperty=e.ASSUME_ES5||"function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};e.getGlobal=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");};e.global=e.getGlobal(this);.e.IS_SYMBOL_NATIVE="func
C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\craw_window.js	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	261316
Entropy (8bit):	5.444466092380538
Encrypted:	false
SSDEEP:	3072:I5vU7I6s2M9duIWFCbmYJ4tnFWdqpMad2vywhIp81QFv9F9nNsZgiDdOFlV/mZmc:I5vqFCb2p8Gx9FNNsZ9Dd/ceR
MD5:	1709B6F00A136241185161AA3DF46A06
SHA1:	33DA7D262FFED1A5C2D85B7390E9DBC830CBE494
SHA-256:	5721A4B3F8E09C869A629EFFD350B51C9D46F0AC136717D4DB6265C0EE6F9AC8
SHA-512:	26835B4C050F53AD2DDB84469DF9A84BBB2786A655AB52DFC20B54BEDCB81D1ECD789198D5B7D8B940242E5CEAC818A177444D402397AE82C203438C4B1D19CB
Malicious:	false
Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var b,k=k||{};k.scope={};k.createTemplateTagFirstArg=function(a){return a.raw=a};k.createTemplateTagFirstArgWithRaw=function(a,c){a.raw=c;return a};k.arrayIteratorImpl=function(a){var c=0;return function(){return c<a.length?{done:!1,value:a[c++]}:{done:!0}};};k.arrayIterator=function(a){return{next:k.arrayIteratorImpl(a)}};k.makeIterator=function(a){var c="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return c?c.call(a):k.arrayIterator(a)};.k.arrayFromIterator=function(a){for(var c,d=[];!(c=a.next()).done;)d.push(c.value);return d};k.arrayFromIterable=function(a){return a instanceof Array?a:k.arrayFromIterator(k.makeIterator(a))};k.ASSUME_ES5=!1;k.ASSUME_NO_NATIVE_MAP=!1;k.ASSUME_NO_NATIVE_SET=!1;k.SIMPLE_FROUND_POLYFILL=!1;k.ISOLATE_POLYFILLS=!1;k.FORCE_POLYFILL_PROMISE=!1;k.FORCE_POLYFILL_PROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;.k.objectCreate=k.ASSUME_ES5||"function"==typeof Object.cre
C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\css\craw_window.css	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1741
Entropy (8bit):	4.912380256743454
Encrypted:	false
SSDEEP:	24:LalZ74H+rMwJHwIodHRmxt3jiu1iu1RDpfeWlMl548wJHwDwCapt/VMYXj8Eq27K:Z+rMm71le88S1tWYXmrVZFH
MD5:	67BF9AABE17541852F9DDFF8245096CD

SHA1:	A4AC74DD258E8E0689034FAA1B15A5C7C56DC3BB
SHA-256:	10DFBD2D98950B79EE12F6B8E3885AABE31543048DE56AD4FC0A5E34D0D9D4EC
SHA-512:	298FA132C6F122798FDB9BC6DE8024915147ADC20355B56A92F0ED9ACCE4549BE6E7F42212E07DCA166E31624D4E66E299565845D4BA1C51CA935050641B61F
Malicious:	false
Reputation:	low
Preview:	html, body {. margin: 0;. overflow: hidden;.}..webview {. width: 100%;. height: 100%;. min-height: 100%;. position: absolute;.}...craw_overlay {. position: absolute;.. left : 0;. top: 0;. right: 0;. bottom: 0;.. background-color: white;.. -webkit-transition: opacity 250ms linear;.. display: -webkit-flex;. -webkit-flex-direction: column;. -webkit-flex: 1 0%;. -webkit-align-items: center;. -webkit-justify-content: center;.. -webkit-app-region: drag;.}...craw_overlay img {. margin: 16px;.}..#loading_overlay {. opacity: 1;.}..#offline_overlay {. opacity: 0;. display: none;.}..#offline_overlay > img {. -webkit-filter: saturate(0%);.}..#offline_overlay > span {. font-family: 'Open Sans', 'Deja Vu Sans', Arial, sans-serif;. font-size: 15px;. line-height: 21px;. color: #8d8d8d;. display: block;.}..#loading_splash {. width: 128px;. height: 128px;.}..#drag_overlay {. position: absolute;. left: 0;. top: 0;. right: 0;. bottom: 0;. pointer-events: none;. -webkit

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\html\craw_window.html

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	810
Entropy (8bit):	4.723481385335562
Encrypted:	false
SSDEEP:	12:hYenuEJIig5fRpvV4AEdN2sAAuzg/7RwQuLYpUH9KfRnQBGgZKy3QGgjPSWZDQL:hYeLJKTVNEuLAuzg/twQucpS9bj3
MD5:	34A839BC40DEBC746BBD181D9EF9310C
SHA1:	8B4EAA74D31EED5B0BABA3CA5460201F6B10DA46
SHA-256:	BB8742615E4CD996AE5D0200E443AE6A6F0B473255F03AFFDB8FB4660DE4554D
SHA-512:	EE81E5509CBC2CB2B6C834224688C1E1B1AA9AA3866C52F8EAED040D5C390653C52D8D681E2E2CF62906643962ABAC823D5B622385B983B21E0DCCAFDF281E FF
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <link href="/css/craw_window.css" rel="stylesheet">. <script src="/craw_window.js"></script>. </head>. <body>. <webview> </webview>. . . . . <div cl ass="craw_overlay" id="offline_overlay">. . . <br /span>. . . . . </body>.</html>.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\images\flapper.gif

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 30 x 30
Category:	dropped
Size (bytes):	70364
Entropy (8bit):	7.119902236613185
Encrypted:	false
SSDEEP:	768:g5TXOSBAqNIPmA8NcjCWdM0VFMJEwavTeElfWupav5TXg7wV+irIPny9MTVQHydi:g5KSmiIPmAhZWiMsDfWug7DmqM6HybkF
MD5:	398ABB308EEBC355DA70BCE907B22E29
SHA1:	CFFB77B8A1724B8F81D98C6D6AD0071D10162252
SHA-256:	2B73533F47A99FFEA9CC405FFAFA9C4C53623F62487AEBFBA415945120B22040
SHA-512:	FC7A56FC8A61A582161874B54ADBAD30A84840190008EDB0B6FBF84F91393CA58E988E3FE446F11A0C3C691C18249B93AEC2904B3D0C4F0857D79034F662385A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....!..NETSCAPE2.0.....,.....9.:.h0.bT(6.!l.&..("g*k..JL1.[....o. .(:...B(.6."...Z.CUyh0.....j.C.z8..S....2.T'...Q..4 g[]$ueW.Ny Q.IoL!AoF#9h>7.0t..%..,.@.m4..7..!.....,.....9.:.h0.bT(6.!l.&..("g*k..JL1.[....o. .(:...B(.6."...Z.CUyh0.....j.C.z8..S....2.T'...Q..4 g[]$ueW.NyQ.IoL!AoF#9h>7.0t..%..,.@.m 4..7..!.....,.....'..w=.....\.)._6.k..OF...n.#\~"....2b3..I.)..eu.Q.`.e.....gr.?>.s.I0.....@.~.Tr.[8.+.,.;..EE....S.*f.....,.....B8/D..;.9.q.....ukC...r.I....j.....BGY...o2J....+O4....X4.....cH%7....I....0H!.!....!,..... .....p8.a$....hh@.4....X,A.0L..(....JX.j...,.....z.X.Q....jB.d....B..

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\images\icon_128.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4364
Entropy (8bit):	7.915848007375225
Encrypted:	false
SSDEEP:	96:YjlLDJjTvXUtNvX8dgb9HT6y8nviyHG5iCRYtIP:YtNTfUzvX8KM+MGRsIP
MD5:	4DBC9F9E6F5A08D299BAC9E54DF07694
SHA1:	BB38F5DE34B1E0BE1109220BA55271087A4D9EA5

SHA-256:	91C2718DD23B4356D71F88F6146868369033291086DF327534546DFA459BEB0E
SHA-512:	A5F2B1F47502836130D8083F757B7773C1E1CB36B76AD298CC29AB2B428C8002D2F15BD839838FC326DAC3681C2F48AB25A3E7631D33726C4B25E8EC1417091
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a.....IDATx..yp.....gF#.:.[H.l.l..8...`/.k....,!a7Km...E...Te..T.....J...p....%.(....+...3....eY.e...L.o...5....h4...\....{?....~.u.`0.....`0.....`0.....`.Y.....[(.....).4....a i..w38.+....Bf././..]...{.....8...3.....3W~OJ.. /...u6V.C..U.0.+._=.c..9.X.?....L....S@.L...m.0..>.C...L|TF.p5..f4M.,.V....8..a.<...RP..@)E,..E"...h.....!...-....,I..T.....m..._[[{w{{.... {*.^.....M.x..h4.h.....\.R.E....j).7.....h4.A.E....,. ...iii.Vj?2...=/.B.FK9P..@)=Rj..D".Y...2.B..x.}0...&J...2.....f.O..e.H.....!.J)'I..R....B.....QJ;K..L...L.l".L~mhh.R.@).FFF ~.L&...~.B.....u.....}.....~.....f..yUU.....^M...6.....].,w.e..~.!$.C.R.....E(%e9.,....k..@...W8.....@.....O..@%.~..@.S..P.....`Tp...."...?ME..c.....s...`..S1...7.b.. aNE..k...3.yP.}.Ch.}.....B.....IPE..C.<....T....k.....Z..o_.....g.....P..A=y.J.)h..@.q.-.*].AU.4...F.M.....y%B]+ .\.~..9.....:..=...r.....E].o...F..P.....i...|....

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\images\icon_16.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	558
Entropy (8bit):	7.505638146035601
Encrypted:	false
SSDEEP:	12:6v/7vyVgSKYsfFzXxXsrPfA+b0YX+5IOUWCQKznuow7:6yVnKYsfFzhXsrIq0YXmgQGn6
MD5:	FB9C46EA81AD3E456D90D58697C12C06
SHA1:	5FC450F7D73CCFAC8F0D818CB3392BA4D91B69DE
SHA-256:	016CA659BA080E194FBFC0929602B16506ED60AA6019FAA51410C4FD93B583E8
SHA-512:	ADD810EE9EB7CAEC505B5FD90A1F184CE39D8F8C689DCC240F188FE353B9575489492E07D572A3B1C11A1555CE66AFCA5134903E4C1AA3D54BC7C5ED3E65B 50C
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDAT8...Mk.Q...;... .....F..QW.....F....J.?.w..7~.....'.Q..B]... .QS...M&_w..b&.|`.....p...f.?.D$.y^.....y*...\..Z..t6..oRj.@&.u..G.qN).t.-V*.>(.N .Ep]wFk.60o.]0.`Y..cT..Y.Tb.`DF.d..s.Z..E..9.4._C..._...%..*.^....4.I...Y..X..R..../...Wj+w0[.]..._B.k.${.\.>.%.....lz .w.ALxo.2;..a..".p..S..&..uXS...<..6..[..zD.._.N+w.WbM7y e6X<...'(,=.r}.....$f..5..P....k..."..8.s.<zgSm@.....).Y.....:e..\|.....F...I..A$.....T?.....m....8.....N...z.....V..vd.h'....C.?.....H.;]..C.M.....9.b.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\images\topbar_floating_button.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.475799237015411
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZtnAkx/RPJDmV7bScsP4a9zln94FptVp:6v/lhPKM4nDspnAkZJNmgPdln2TTp
MD5:	8803665A6328D23CC1014A7B0E9BE295
SHA1:	9DA6EE729D5A6E9F30658B8EC954710F107A641F
SHA-256:	D5F9234DC36E7FFA85F35B2359A4F82276F8395EFA76E4553507EA990B27FC6C
SHA-512:	ECD9E71B8BA1ED8BD4CA5A0936CB66A83611C4ABCBDA76C250F4CDF4AD80320212E8F5EEB79A38910718F8346ECC1AD580A3FA835EC2B22BE497F36899FB5 930
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...Q..0.....2...(p...~Z.}'.>I%O...V!s...../...`.<..`.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\images\topbar_floating_button_close.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	252
Entropy (8bit):	6.512071394066515
Encrypted:	false
SSDEEP:	6:6v/lhPKM4nDsp7q1hKVlomsj9rxKNgtmN0VZ+GFYep:6v/7iMXVq1ylxemNgtmKVnYM
MD5:	0599DFD9107C7647F27E69331B0A7D75
SHA1:	3198C0A5F34DB67F91A0035DBC297354CBC95525
SHA-256:	131817CD9311C03DF22D769DD2AD7FA2E6E9558863A89F7E5E1657424031A937
SHA-512:	0076ACB9D6A886BD987876E49495038F9388B292A9EFE5C9093CCA64CA3692E3A5D24E35172C7697F6AAE34B86CA217EE59C003423E46D9499BD27EC7D77A64
Malicious:	false
Reputation:	low

Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<....IDATx..... ..Pp.X....H...b@...|.^LC_.E.BP+.....X.P.....q..~..p/. ..s.....%D^...$.....@.!...<...).? .4{.k.G3...4..[cH..0..l.8.!r..m.R..{.....`.f...#.x.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\images\topbar_floating_button_hover.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.423186859407619
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZtnAkx/9lVtEHxrPLyN+ltNPhv/l2up:6v/lhPKM4nDspnAkZHVtERrPLygltNPn
MD5:	7CB6B9DC1A30F63B8BD976924B75AD96
SHA1:	0C40B0C496D2F2B5F2021C117EC8610AC03AB469
SHA-256:	721B7AAA9A42A54A349881615A12E3A26983ACA48E173FD2F66E66AA0D725735
SHA-512:	4764937364E355956B242B84010AC56102536D2AACBE4227F0E88E4DE7AB468571957EA6C33012539156E5349AE4F777115615AE3361F60ADDF9CD227424F76A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...A..0...+B.z.s...*.....$.<u..[.....h.....C.CA).....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\images\topbar_floating_button_maximize.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	166
Entropy (8bit):	5.8155898293424775
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZttd//HmnFz1P/ZjXlUTqyCIc30ltK1p:6v/lhPKM4nDsptF/HOP/ZjXlUeyCo/p
MD5:	232CE72808B60CBE0F4FA788A76523DF
SHA1:	721A9C98C835D2CD734153BBE07833C6637ECD68
SHA-256:	AFA4EA944CBDEC8543242E627EF46D5BFD3766DCAC664E7E50CDEEF2B352740C
SHA-512:	4048EEA5A78DD569521C488C4CE4F7B77AC0454C92EE9107A81A1B3AF91A4EE036039AC1A0A6B8DD26B12E7F1595DB80B7FAA7B6A25D9032BF385528A81A86 54
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...HIDATx.....0.CQS.....~..."..........m.v+Sq....<!...M8m...'...@$..0....E.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\images\topbar_floating_button_pressed.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.46068685940762
Encrypted:	false
SSDEEP:	3:yionv//thPl3xWrA4RthwkBDsTBZtnAkx/9lVtEXIyN+ltN1/lsg1p:6v/lhPKM4nDspnAkZHVtEZgltN1eup
MD5:	E0862317407F2D54C85E12945799413B
SHA1:	FA557F8F761A04C41C9A4BA81994E43C6C275DBB
SHA-256:	5C10CE0589EB115600F77381130B70AE0B7B3752614D86D4C89E857658AA222B
SHA-512:	07CB69327961FD0019BEF8EF7590B5524905AC373A815F73F6D9E0B26840929F919A96CAA977D4B5656704DACD0F352D568FB3997F80EE6BB94C95B58839DBFE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...A..0...+B..@wu...*.....$.<u..[.....h.....M..x(....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir4324_2011126058\CRX_INSTALL\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1322
Entropy (8bit):	5.449026004350873

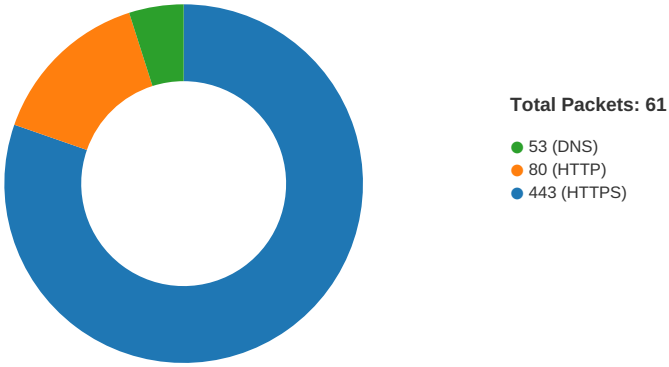
Encrypted:	false
SSDEEP:	24:1HEis7ViC/yox/fiqeUoLFlmF1s80FKrGfd0d3NZNZx1Fq7eY7nfj1B:WL7V2opiV1mvs8rxTZRczhB
MD5:	01334FB9D092AF2AA46C4185E405C627
SHA1:	47AD3C0E82362FFE5B881DF8D71D6F79AB7F5796
SHA-256:	F52714812D68C577A445169D11E84DF6751C2D6886BC429643072BB5D61C6C27
SHA-512:	888D96ADB7A847ABE472145258C8C46950EB2FA3BA7D596C2E90A17C8FB06FD0155C56CC8ABA5D076D89368417464BCB2D236F9E40E53241950A01F9F8ED548F
Malicious:	false
Reputation:	low
Preview:	{.. "app": {.. "background": {.. "scripts": ["craw_background.js"].. }.. },.. "default_locale": "en",.. "description": "__MSG_APP_DESCRIPTION__",.. "display_in_launcher": false,.. "display_in_new_tab_page": false,.. "icons": {.. "128": "images/icon_128.png",.. "16": "images/icon_16.png".. },.. "key": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrKfMnLqViEyokd1wk57FxJtW2XXpGXzIHBzv9vQI/01UsuP0lV5/lj0wx7zJ/xcibUgDeIxobvv9XD+zO1MdjMWuqJFcKuSS4Suqkje6u+pMrTSGOSHq1bmBVh0kpToN8YoJs/P/yrRd7FEtAXTaFTGxQL4C385MeXSjaQfiRiQIDAQAB",.. "manifest_version": 2,.. "minimum_chrome_version": "29",.. "name": "__MSG_APP_NAME__",.. "oauth2": {.. "auto_approve": true,.. "client_id": "203784468217.apps.googleusercontent.com",.. "scopes": ["https://www.googleapis.com/auth/sierra", "https://www.googleapis.com/auth/sierrasandbox", "https://www.googleapis.com/auth/chromewebstore", "https://www.googleapis.com/auth/chromewebstore.readonly"].. },.

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:19:36.449724913 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.449784994 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.449886084 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.450160027 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.450189114 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.452224970 CEST	49770	80	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.453067064 CEST	49771	80	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.455889940 CEST	49772	443	192.168.2.5	142.250.203.109
May 27, 2022 20:19:36.455919981 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.456002951 CEST	49772	443	192.168.2.5	142.250.203.109
May 27, 2022 20:19:36.456254959 CEST	49772	443	192.168.2.5	142.250.203.109
May 27, 2022 20:19:36.456269979 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.483784914 CEST	80	49770	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.483926058 CEST	49770	80	192.168.2.5	13.226.244.72

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:19:36.484525919 CEST	49770	80	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.484673977 CEST	80	49771	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.484766960 CEST	49771	80	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.501869917 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.502294064 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.502345085 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.503223896 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.503313065 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.505410910 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.505559921 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.516261101 CEST	80	49770	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.516431093 CEST	80	49770	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.516741037 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.517355919 CEST	49772	443	192.168.2.5	142.250.203.109
May 27, 2022 20:19:36.517411947 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.518949986 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.519057989 CEST	49772	443	192.168.2.5	142.250.203.109
May 27, 2022 20:19:36.552536964 CEST	49774	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.552570105 CEST	443	49774	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.552675009 CEST	49774	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.552921057 CEST	49774	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.552930117 CEST	443	49774	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.625890970 CEST	49770	80	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.638621092 CEST	443	49774	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.638962030 CEST	49774	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.638979912 CEST	443	49774	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.640707016 CEST	443	49774	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.640815973 CEST	49774	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.715837955 CEST	49772	443	192.168.2.5	142.250.203.109
May 27, 2022 20:19:36.716125965 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.716628075 CEST	49774	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.717158079 CEST	443	49774	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.717475891 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.717675924 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.717955112 CEST	49772	443	192.168.2.5	142.250.203.109
May 27, 2022 20:19:36.717973948 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.718535900 CEST	49774	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:36.718559980 CEST	443	49774	13.226.244.72	192.168.2.5
May 27, 2022 20:19:36.724324942 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.724356890 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.761523008 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.761678934 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.761715889 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.761744976 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.761837006 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.764027119 CEST	49769	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:36.764056921 CEST	443	49769	216.58.215.238	192.168.2.5
May 27, 2022 20:19:36.771194935 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.771312952 CEST	49772	443	192.168.2.5	142.250.203.109
May 27, 2022 20:19:36.771351099 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.771461964 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.771529913 CEST	49772	443	192.168.2.5	142.250.203.109
May 27, 2022 20:19:36.795150995 CEST	49772	443	192.168.2.5	142.250.203.109
May 27, 2022 20:19:36.795195103 CEST	443	49772	142.250.203.109	192.168.2.5
May 27, 2022 20:19:36.856868982 CEST	49774	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:37.121956110 CEST	443	49774	13.226.244.72	192.168.2.5
May 27, 2022 20:19:37.122188091 CEST	443	49774	13.226.244.72	192.168.2.5
May 27, 2022 20:19:37.122271061 CEST	49774	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:37.395539999 CEST	49774	443	192.168.2.5	13.226.244.72

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:19:37.395581007 CEST	443	49774	13.226.244.72	192.168.2.5
May 27, 2022 20:19:37.807461977 CEST	49781	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:37.807519913 CEST	443	49781	13.226.244.72	192.168.2.5
May 27, 2022 20:19:37.807602882 CEST	49781	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:37.807898998 CEST	49781	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:37.807930946 CEST	443	49781	13.226.244.72	192.168.2.5
May 27, 2022 20:19:37.881561995 CEST	443	49781	13.226.244.72	192.168.2.5
May 27, 2022 20:19:37.883202076 CEST	49781	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:37.883240938 CEST	443	49781	13.226.244.72	192.168.2.5
May 27, 2022 20:19:37.883949041 CEST	443	49781	13.226.244.72	192.168.2.5
May 27, 2022 20:19:37.894531965 CEST	49781	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:37.894700050 CEST	49781	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:37.894777060 CEST	443	49781	13.226.244.72	192.168.2.5
May 27, 2022 20:19:38.036273956 CEST	49781	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:38.290297985 CEST	443	49781	13.226.244.72	192.168.2.5
May 27, 2022 20:19:38.290558100 CEST	443	49781	13.226.244.72	192.168.2.5
May 27, 2022 20:19:38.290656090 CEST	49781	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:38.295180082 CEST	49781	443	192.168.2.5	13.226.244.72
May 27, 2022 20:19:38.295212984 CEST	443	49781	13.226.244.72	192.168.2.5
May 27, 2022 20:19:48.464818954 CEST	49771	80	192.168.2.5	13.226.244.72
May 27, 2022 20:19:48.496675968 CEST	80	49771	13.226.244.72	192.168.2.5
May 27, 2022 20:19:48.496798038 CEST	49771	80	192.168.2.5	13.226.244.72
May 27, 2022 20:20:21.588551044 CEST	49770	80	192.168.2.5	13.226.244.72
May 27, 2022 20:20:21.620275974 CEST	80	49770	13.226.244.72	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:19:36.415095091 CEST	63712	53	192.168.2.5	8.8.8.8
May 27, 2022 20:19:36.420950890 CEST	63187	53	192.168.2.5	8.8.8.8
May 27, 2022 20:19:36.427289009 CEST	60658	53	192.168.2.5	8.8.8.8
May 27, 2022 20:19:36.448594093 CEST	53	63187	8.8.8.8	192.168.2.5
May 27, 2022 20:19:36.450830936 CEST	53	63712	8.8.8.8	192.168.2.5
May 27, 2022 20:19:36.454628944 CEST	53	60658	8.8.8.8	192.168.2.5
May 27, 2022 20:19:38.778467894 CEST	62932	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:38.808322906 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.808856010 CEST	62932	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:38.837363005 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.837402105 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.837423086 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.837445021 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.838824034 CEST	62932	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:38.842402935 CEST	62932	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:38.866833925 CEST	62932	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:38.867230892 CEST	62932	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:38.907016993 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.907754898 CEST	62932	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:38.909702063 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.924674988 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.924740076 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.924757957 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.925546885 CEST	62932	443	192.168.2.5	216.58.215.238
May 27, 2022 20:19:38.974545956 CEST	443	62932	216.58.215.238	192.168.2.5
May 27, 2022 20:19:38.985285997 CEST	62932	443	192.168.2.5	216.58.215.238

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 20:19:36.415095091 CEST	192.168.2.5	8.8.8.8	0x4a78	Standard query (0)	pub.lucidpress.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 20:19:36.420950890 CEST	192.168.2.5	8.8.8.8	0x4d36	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
May 27, 2022 20:19:36.427289009 CEST	192.168.2.5	8.8.8.8	0x8d7a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 20:19:36.448594093 CEST	8.8.8.8	192.168.2.5	0x4d36	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 20:19:36.448594093 CEST	8.8.8.8	192.168.2.5	0x4d36	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
May 27, 2022 20:19:36.450830936 CEST	8.8.8.8	192.168.2.5	0x4a78	No error (0)	pub.lucidpress.com	d3v04nmt9jknbk.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 20:19:36.450830936 CEST	8.8.8.8	192.168.2.5	0x4a78	No error (0)	d3v04nmt9jknbk.cloudfront.net		13.226.244.72	A (IP address)	IN (0x0001)
May 27, 2022 20:19:36.450830936 CEST	8.8.8.8	192.168.2.5	0x4a78	No error (0)	d3v04nmt9jknbk.cloudfront.net		13.226.244.9	A (IP address)	IN (0x0001)
May 27, 2022 20:19:36.450830936 CEST	8.8.8.8	192.168.2.5	0x4a78	No error (0)	d3v04nmt9jknbk.cloudfront.net		13.226.244.121	A (IP address)	IN (0x0001)
May 27, 2022 20:19:36.450830936 CEST	8.8.8.8	192.168.2.5	0x4a78	No error (0)	d3v04nmt9jknbk.cloudfront.net		13.226.244.33	A (IP address)	IN (0x0001)
May 27, 2022 20:19:36.454628944 CEST	8.8.8.8	192.168.2.5	0x8d7a	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- accounts.google.com
- pub.lucidpress.com
- clients2.google.com
- https:

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49772	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49774	13.226.244.72	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49769	216.58.215.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49781	13.226.244.72	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49770	13.226.244.72	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 20:19:36.484525919 CEST	1140	OUT	GET / HTTP/1.1 Host: pub.lucidpress.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
May 27, 2022 20:19:36.516431093 CEST	1155	IN	HTTP/1.1 301 Moved Permanently Server: CloudFront Date: Fri, 27 May 2022 18:19:36 GMT Content-Type: text/html Content-Length: 183 Connection: keep-alive Location: https://pub.lucidpress.com/ X-Cache: Redirect from cloudfront Via: 1.1 29f497d809ce69f1f314c1e13d9cdec2.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FCO50-C1 X-Amz-Cf-Id: HDWxtRtgi4-eLk3l1Ph3HkRvMnk-lXk6rcXZoGEBL-aSrzmjbx_wAw== Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 43 6c 6f 75 64 46 72 6f 6e 74 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> CloudFront </body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49772	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:19:36 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 18:19:36 UTC	0	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:19:36 UTC	3	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 18:19:36 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-H9sHVDnvbrthnM8-uQujrw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-H9sHVDnvbrthnM8-uQujrw' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 18:19:36 UTC	5	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-05-27 18:19:36 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49774	13.226.244.72	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:19:36 UTC	0	OUT	GET / HTTP/1.1 Host: pub.lucidpress.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 18:19:37 UTC	5	IN	HTTP/1.1 403 Forbidden Content-Type: application/xml Transfer-Encoding: chunked Connection: close Date: Fri, 27 May 2022 18:19:36 GMT Server: AmazonS3 access-control-allow-headers: Content-Type,Authorization,Cache-Control,X-Lucid-Retry,X-B3-Baggage-Pageview,X-B3-Baggage-Session,X-Lucid-Flow-Id access-control-allow-methods: OPTIONS,HEAD,GET,PUT,DELETE,POST,PATCH content-security-policy: frame-ancestors https: http: ; strict-transport-security: max-age=31536000 x-content-type-options: nosniff x-permitted-cross-domain-policies: none referrer-policy: no-referrer-when-downgrade Vary: Origin X-Cache: Error from cloudfront Via: 1.1 13dcb5d1ef6aaeefea92da59d4323d88.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FCO50-C1 X-Amz-Cf-Id: PWUJZAVLwcJ5RpgsEgVa5ZyAzDxzkgJ-sGVGkQUnvaR1zjWY8XbDKA==

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:19:37 UTC	6	IN	Data Raw: 66 33 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 3c 45 72 72 6f 72 3e 3c 43 6f 64 65 3e 41 63 63 65 73 73 44 65 6e 69 65 64 3c 2f 43 6f 64 65 3e 3c 4d 65 73 73 61 67 65 3e 41 63 63 65 73 73 20 44 65 6e 69 65 64 3c 2f 4d 65 73 73 61 67 65 3e 3c 52 65 71 75 65 73 74 49 64 3e 4e 47 45 41 52 54 46 59 35 33 51 47 32 45 54 4e 3c 2f 52 65 71 75 65 73 74 49 64 3e 3c 48 6f 73 74 49 64 3e 7a 75 66 69 78 34 65 6d 66 48 65 37 78 4a 37 2b 4a 53 45 6b 44 5a 5a 79 34 44 56 4c 53 59 59 76 66 6f 66 36 38 62 4e 4d 58 35 57 51 32 34 75 33 5a 32 53 33 4c 2f 44 76 55 4d 67 5a 45 69 33 42 38 2f 35 56 43 2f 59 48 62 70 30 3d 3c 2f 48 6f 73 74 49 64 3e 3c 2f 45 72 72 6f 72 3e 0d 0a Data Ascii: f3<?xml version="1.0" encoding="UTF-8"?><Error><Code>AccessDenied</Code><Message>Access Denied</Message><RequestId>NGEARTFY53QG2ETN</RequestId><HostId>zufix4emfHe7xJ7+JSEkDZZy4DV LSYYvfof68bNMX5WQ24u3Z2S3L/DvUMgZEi3B8/5VC/YHbp0=</HostId></Error>
2022-05-27 18:19:37 UTC	6	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49769	216.58.215.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

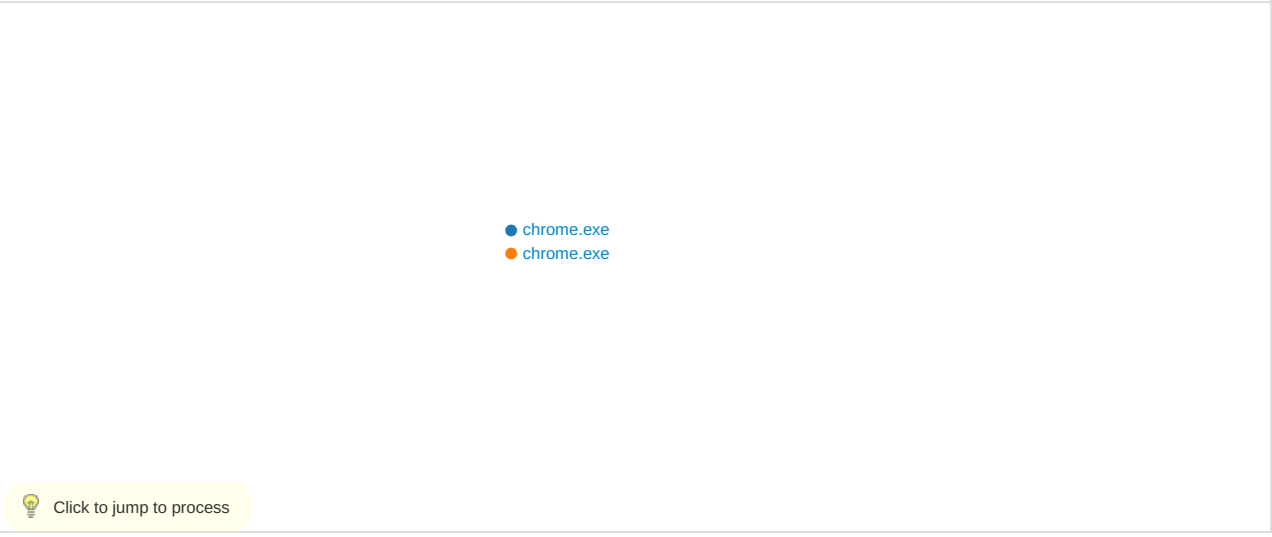
Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:19:36 UTC	1	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel= &prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelp bcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 18:19:36 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-Eg8j-CRuKUZzV-ZFhjAIug' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 18:19:36 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5625 X-Daystart: 40776 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 18:19:36 UTC	2	IN	Data Raw: 33 36 64 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 32 35 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 34 30 37 37 36 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 36d<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5625" elapsed_seconds="40776"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-05-27 18:19:36 UTC	3	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c54 50122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" p rotected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-05-27 18:19:36 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49781	13.226.244.72	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:19:37 UTC	6	OUT	GET /favicon.ico HTTP/1.1 Host: pub.lucidpress.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://pub.lucidpress.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 18:19:38 UTC	6	IN	HTTP/1.1 403 Forbidden Content-Type: application/xml Transfer-Encoding: chunked Connection: close Date: Fri, 27 May 2022 18:19:37 GMT Server: AmazonS3 access-control-allow-headers: Content-Type,Authorization,Cache-Control,X-Lucid-Retry,X-B3-Baggage-Pageview,X-B3-Baggage-Session,X-Lucid-Flow-Id access-control-allow-methods: OPTIONS,HEAD,GET,PUT,DELETE,POST,PATCH content-security-policy: frame-ancestors https: http: ; strict-transport-security: max-age=31536000 x-content-type-options: nosniff x-permitted-cross-domain-policies: none referrer-policy: no-referrer-when-downgrade Vary: Origin X-Cache: Error from cloudfront Via: 1.1 37f9b15f0f28557295e030db52aad868.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FCO50-C1 X-Amz-Cf-Id: 1y-E9rXhOWlo9c_39wLMqyRqEXQD_p21zNPt4XJQrTBoia6hG3GBnw==
2022-05-27 18:19:38 UTC	7	IN	Data Raw: 66 33 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 3c 45 72 72 6f 72 3e 3c 43 6f 64 65 3e 41 63 63 65 73 73 44 65 6e 69 65 64 3c 2f 43 6f 64 65 3e 3c 4d 65 73 73 61 67 65 3e 41 63 63 65 73 73 20 44 65 6e 69 65 64 3c 2f 4d 65 73 73 61 67 65 3e 3c 52 65 71 75 65 73 74 49 64 3e 50 52 36 39 46 47 39 36 57 54 51 41 52 37 32 59 3c 2f 52 65 71 75 65 73 74 49 64 3e 3c 48 6f 73 74 49 64 3e 50 6b 74 68 6b 77 62 38 47 65 31 6a 66 56 6a 39 34 75 4c 69 2b 46 4c 53 2b 65 33 57 45 32 42 57 34 34 49 6c 74 62 67 4a 77 56 62 30 4e 37 38 74 6b 33 34 55 72 38 44 33 62 31 71 45 63 2f 6d 62 61 72 68 49 39 30 54 4a 77 41 6f 3d 3c 2f 48 6f 73 74 49 64 3e 3c 2f 45 72 72 6f 72 3e 0d 0a Data Ascii: f3<?xml version="1.0" encoding="UTF-8"?><Error><Code>AccessDenied</Code><Message>Access Denied</Message><RequestId>PR69FG96WTQAR72Y</RequestId><HostId>Pkthkwb8Ge1jfVj94uLi+FLS+e3WE2BW44lltbgJwVb0N78tk34Ur8D3b1qEc/mbarhI90TJwAo=</HostId></Error>
2022-05-27 18:19:38 UTC	7	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4324, Parent PID: 5696

General

Target ID:	0
Start time:	20:19:31
Start date:	27/05/2022
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 "http://pub.lucidpress.com
Imagebase:	0x7ff6a7220000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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: 6180, Parent PID: 4324

General

Target ID:	1
Start time:	20:19:32
Start date:	27/05/2022
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=1616,15869322143913586381,16477777855430292938,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /prefetch:8
Imagebase:	0x7ff6a7220000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly