ID: 635099
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 13:18:24
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

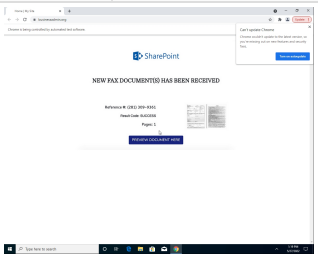
Windows Analysis Report

https://businessadmin.org/

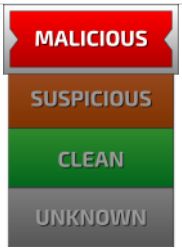
Overview

General Information

Sample URL:	https://businessadmin.org/
Analysis ID:	635099



Detection



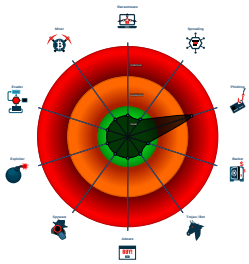
HTMLPhisher

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish20
- HTML body contains low number of ...
- Suspicious form URL found
- No HTML title found

Classification



Process Tree

- **System is start**
- chrome.exe (PID: 1836 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation --single-argument https://businessadmin.org/ MD5: 74859601FB4BEEA84B40D874CCB56CAB)
  - chrome.exe (PID: 4712 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1704,4736951046417788977,18058605637325600590,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2072 /prefetch:8 MD5: 74859601FB4BEEA84B40D874CCB56CAB)
- **cleanup**

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
87441.1.pages.csv	JoeSecurity_HtmlPhish_20	Yara detected HtmlPhish_20	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish20

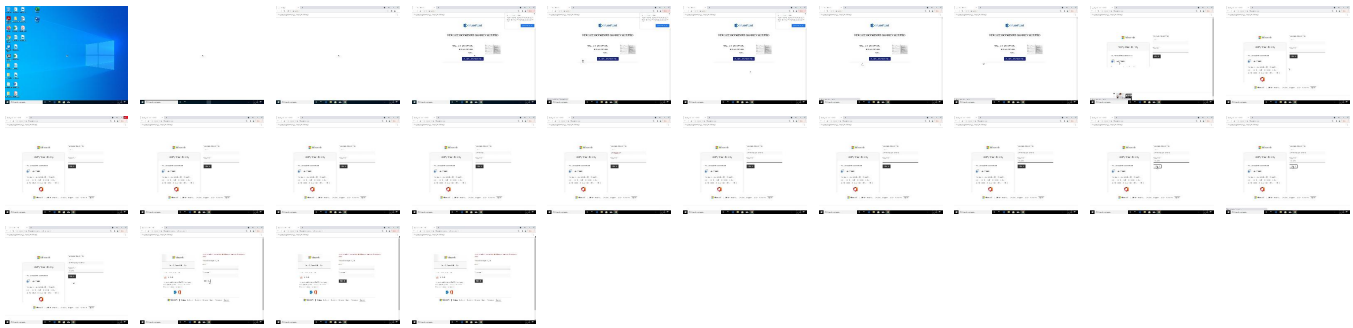
Mitre Att&ck Matrix

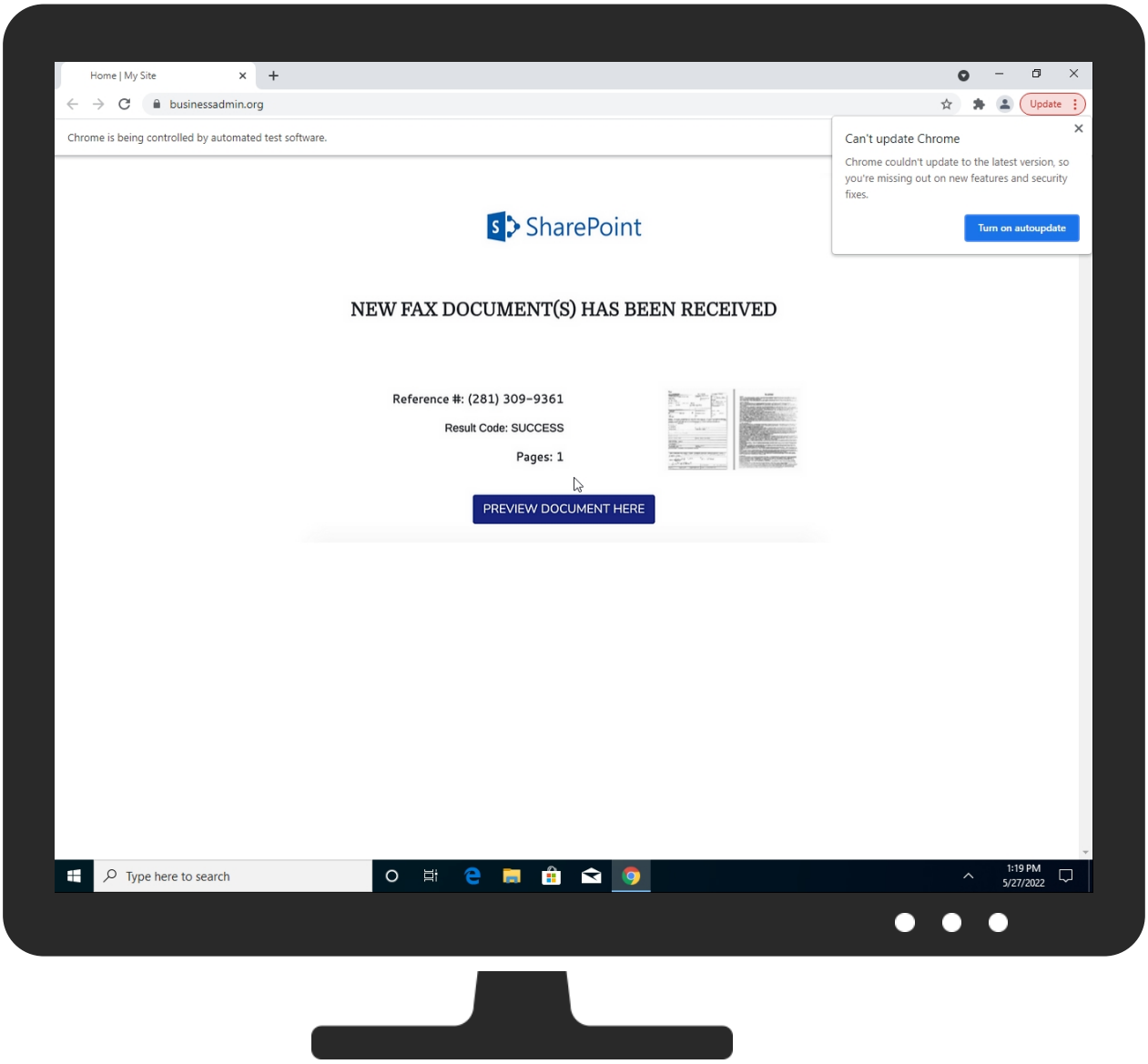
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 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	1 Extra Window Memory Injection	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 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)	1 Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 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)	1 Extra Window Memory Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

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
https://businessadmin.org/	0%	Virustotal		Browse
https://businessadmin.org/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
td-ccm-168-233.wixdns.net	0%	Virustotal		Browse
businessadmin.org	0%	Virustotal		Browse
frog.editorx.com	0%	Virustotal		Browse
www.businessadmin.org	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.184.227	true	false		high
td-ccm-168-233.wixdns.net	34.117.168.233	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	142.250.186.141	true	false		high
sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com	52.41.81.16	true	false		high
gcp.media-router.wixstatic.com	34.102.176.152	true	false		high
weebly.map.fastly.net	151.101.1.46	true	false		unknown
pages-wildcard.weebly.com	199.34.228.54	true	false		high
td-static-34-96-106-200.parastorage.com	34.96.106.200	true	false		high
businessadmin.org	185.230.63.107	true	false	• 0%, Virustotal, Browse	unknown
ssl-google-analytics.l.google.com	142.250.185.136	true	false		high
www.google.com	142.250.184.196	true	false		high
clients.l.google.com	142.250.184.206	true	false		high
bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com	52.201.127.108	true	false		high
productoffice365fax.weebly.com	unknown	unknown	false		high
siteassets.parastorage.com	unknown	unknown	false		high
static.wixstatic.com	unknown	unknown	false		high
cdn2.editmysite.com	unknown	unknown	false		high
frog.editorx.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
ec.editmysite.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
frog.wix.com	unknown	unknown	false		high
www.businessadmin.org	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
static.parastorage.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://productoffice365fax.weebly.com/	false		high
https://productoffice365fax.weebly.com/ajax/apps/formSubmitAjax.php	false		high
https://www.businessadmin.org/	true		unknown
http://productoffice365fax.weebly.com/incorrect-password.html	false		high
https://productoffice365fax.weebly.com/incorrect-password.html	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.125.108.199	unknown	United States		15169	GOOGLEUS	false
216.58.212.142	unknown	United States		15169	GOOGLEUS	false
34.96.106.200	td-static-34-96-106-200.parastorage.com	United States		15169	GOOGLEUS	false
52.41.81.16	sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
199.34.228.54	pages-wildcard.weebly.com	United States		27647	WEEBLYUS	false
185.230.63.107	businessadmin.org	Israel		58182	WIX_COMIL	false
34.203.102.82	unknown	United States		14618	AMAZON-AESUS	false
52.201.127.108	bi-flogger-alb-ext-343643057.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
142.250.184.227	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
142.250.184.206	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.138	unknown	United States		15169	GOOGLEUS	false
142.250.185.67	unknown	United States		15169	GOOGLEUS	false
142.250.184.196	www.google.com	United States		15169	GOOGLEUS	false
142.250.186.141	accounts.google.com	United States		15169	GOOGLEUS	false
151.101.1.46	weebly.map.fastly.net	United States		54113	FASTLYUS	false
34.117.168.233	td-ccm-168-233.wixdns.net	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false
142.250.185.136	ssl-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
142.251.37.99	unknown	United States		15169	GOOGLEUS	false
142.250.181.227	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
34.102.176.152	gcp.media-router.wixstatic.com	United States		15169	GOOGLEUS	false
142.250.186.42	unknown	United States		15169	GOOGLEUS	false
142.250.185.74	unknown	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:	635099
Start date and time: 27/05/202213:18:24	2022-05-27 13:18:24 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://businessadmin.org/
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.win@27/90@16/156
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): CompPkgSrv.exe, SIHClient.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.185.67, 216.58.212.142, 74.125.108.199
- Excluded domains from analysis (whitelisted): login.live.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenFile calls found.
- VT rate limit hit for: https://www.businessadmin.org/

Created / dropped Files

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\3f837ef4-6bb6-4c49-a519-d6ce8a8680f8.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):	105157
Entropy (8bit):	6.034790363314817
Encrypted:	false
SSDEEP:	
MD5:	EAA0D29FAAA5E226CA2324FE25DC28E1
SHA1:	63351FDCD792058013D348678DD06F4608A99A71
SHA-256:	2B508E98C3E32024C6CB73C593B453B580881063FEBD1199E9B29252E93D8106
SHA-512:	AB1055F211D128EEBB6749DFC2D9C5159EF7C87F7EAAB4BF94D6FAB18A87A520F0AB64C6E453356CE25C143FA955083FED066A727BEF98A6C5DA28E61198F56E
Malicious:	false
Reputation:	low

Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"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":1.653682742466372e+12,"network":1.653650343e+12,"ticks":168386431.0,"uncertainty":2827031.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"policy":{"last_statistics_update":"13298156339654847"},"profile":{"info_cache":{"Default":{"active_time":1653682741.229904,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\9f38feb6-e82b-4425-a3ef-6bd8fd95420e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95480
Entropy (8bit):	3.756568821221119
Encrypted:	false
SSDEEP:	
MD5:	FBB5ED735B8137CFA55078CC19A4FF48
SHA1:	86A0E131C89F9A92EA25618106235F29E222E63F
SHA-256:	7020574F85C5F3B970E22FC58F12CF89613FDC108945A287294975FF0F26C7A9
SHA-512:	C1610DCD971C740D64C84A654B8EB9A61B7D6A340C43400CCF371B0E335A663ED56F1959A53F1D51DC39BFE8F519AC52A64869E63FBC8C5AD4BA94AFBA5972B
Malicious:	false
Reputation:	low
Preview:	.t.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....puA...c.:.\.p.r.o.g.r.a.m. .f.i.l.e.s. .(.x.8.6.).\.m.i.c.r.o.s.o.f.t. .o.n.e.d.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.....f.i.l.e.s.y.n.c.s.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e."...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....2.1...0.8.3...0.4.2.5...0.0.0.3.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...l]8. ...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.7.-.Z.i.p.\.7.-.z.i.p...d.l.l.....n\....%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.7.-.z.i.p.\.....7.-.z.i.p...d.l.l.....7.-.Z.i.p.....7.-.Z.i.p. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....1.9...0.0.....l]8.....

C:\Users\alfredo\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):	3.254162526001658
Encrypted:	false
SSDEEP:	
MD5:	FA7200D6F80CD1757911C45559E59C0E
SHA1:	89C6E99BAEC4EBB3E9A97B928FB473D1498EBA88
SHA-256:	D9779EA4D6DD544A23C2A1C53146B6A4E596927F47DFA0680B0A7EE751D43BB2
SHA-512:	71D9B2DA8EAF404063D918812BA61C3EFB6A23A283B0332180A38C8137FBB21D7977C008D5A57A74469776945CD4ED42C0BCC09F923EDEC52D8F7FE90FA2D14
Malicious:	false
Reputation:	low
Preview:	sdPC.....A.>'..M..,.-.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\01e6f39d-7cc0-47be-ad51-6610b8bd74bb.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):	3343
Entropy (8bit):	4.945222848960228
Encrypted:	false
SSDEEP:	
MD5:	CAB8BEABE7E66A4015C98A3C77B3698B
SHA1:	C960AAAEA7014E105290C7D0F09BFCA837C8E8CC
SHA-256:	75431010BFE77818B8BEF4B0C4B328C00668DC6B13C09AAB769EBF58BDA4EDF7
SHA-512:	0D1E94E84294AEA4BF400FF9D0654748BFFEB92D3A1643A6A13B541ADB1BC13EA2F649560A27C8CC3D8AEF9DA5D6B668C7E3BE696091CE882A475B91A9A4CAC8
Malicious:	false
Reputation:	low

Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230891381309","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230891381310","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39697},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230887958662","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230887958664","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":52163},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230886326794","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230886326795","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\1310830b-321e-4d8a-b5f8-6497f65556f4.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):	4339
Entropy (8bit):	5.026045858342657
Encrypted:	false
SSDEEP:	
MD5:	CA4D2FEF727DFCE29AEA28A3E4B19F55
SHA1:	F3DB1E1A7A787FC81C8D0B191218F62953EF282D
SHA-256:	83E01E3E1D4386D6DCB5AA9960E9AAC3C9798116DBBA9FA090D23F2F782F36CB
SHA-512:	BCE8B762577BA360F94EBD6ADFAB1B03AC38B08BC60B11019B43C2B51AAD3F9AF2D773D5473818FC06EBCBB3198DCAB05C305FDAE200839002D8855FA83A10E2
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298156341543530","alternate_error_pages":{"backup":true},"autocomplete":{"retention_policy_last_version":92},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2734,"this_week_services_downstream_foreground_kb":{"112189210":1,"115188287":51,"21145003":243,"35565745":2,"5151071":2}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298156341534964"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1653682743.314395,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm":{"product_category_for_s

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\1ee046b7-032d-48ff-a71a-0c87bbc557a4.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:	modified
Size (bytes):	18396
Entropy (8bit):	5.555287307888642
Encrypted:	false
SSDEEP:	
MD5:	5BD953283D419A5D200395548ECA3C5A
SHA1:	9B8AB932D3241BB764D94DA7949CC1FB574D2ECA
SHA-256:	190CD36A6452267A9EBAD183F43CFA57AE87B582675115752EB439162E519D3B
SHA-512:	CE882B729B9B6AD3FD239DBD1AA856B2F8212FC9226C8A18275F9D919B429AE1A4ACC1A8C24AA7B5E5DD2850A2FEB1F58E76D0BC446F38F9AAB4DEC299C97C7E
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":"13298156340257038","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\alfredo\AppData\Local\Google\Chrome\User Data\Default\36f094cc-4ce6-46e6-b6c3-f540df4c72f9.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):	15765
Entropy (8bit):	5.573949594314066
Encrypted:	false
SSDEEP:	
MD5:	788BA81AB8C92F1EBCF22D858285D3C2
SHA1:	2541CF79477423B9B901586E659C170A2AD85E07
SHA-256:	600FD57F26A2DEF3E72F840FFC858B1ACB3F70345F495D2468AB7D465515039C

SHA-512:	08AD252283727AFA16C930E8D9ABE52DD03C673EE67A150DFB8484367035E03E8553413547B3B611DA94D7211355A3032CE04D0CDBC20A943BC7EACCEED2155
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":"13298156340257038","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\alfredo\AppData\Local\Google\Chrome\User Data\Default\3c353e07-df8e-4f8a-8ac7-8e18137f1466.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:	
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\3c359289-0de6-400b-955b-23b983b9f614.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):	3488
Entropy (8bit):	4.937657065599642
Encrypted:	false
SSDEEP:	
MD5:	D3E7BCDA3CFEB0E9A7E80D046D91A7E3
SHA1:	3BE90F5595F77955D2D63E03F8F39942C9634328
SHA-256:	40797C83392FE871C874A3A695D7DFE692DE4DC5D8E26CB856ED84948F7BEAA9
SHA-512:	46C9613FE0BEE7883B1442DFB7C93C8C9DB62DFB7F931C6FE155D98732002C40B7B14A1F4AFB0E2CE3E8875F185858A64CF72FDDD9BEC655F12C0E75FD29BEF5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298156341543530","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2734},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298156341534964"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"product_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"51102b54-14a5-4079-bd8b-e6b63d8b2b64"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"9D17C7184A596066D76E13B1D59D5E14","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	589
Entropy (8bit):	5.3469499692759
Encrypted:	false
SSDEEP:	
MD5:	8B836F1852C9DD66EE418A575379A7C3
SHA1:	B8BB08BC8704253B1087FF503C5F4343CD57CBE4
SHA-256:	3CC5CE2DC2693B8FE3EEC31B5BF0DBA1A45BB84BC5BFAB71866EA4BECAC1C6D0

SHA-512:	9A3F76FF868DD20687E6F0A457168EA1E829AC95FF3760BBE5F66ABE13163DBB2C09575DFF0147CD4FDB0370228E4D013906E9E1288A81401C5BC8E115E6961(
Malicious:	false
Reputation:	low
Preview:	....."2....businessadmin..home..https..my..org..site..www*N.....businessadmin.....home.....https.....my.....org.....site.....www..2.....a.....b.....d.....e.....g.....h.....i.....m.....n.....o.....p.....r.....s.....t.....u.....w.....y...:G.....B.....L..... .....*.https://businessadmin.org/2.Home | My Site:.....U..... .....*.https://www.businessadmin.org/2.Home | My Site:.....J.....

C:\Users\alfredo\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):	3343
Entropy (8bit):	4.945222848960228
Encrypted:	false
SSDEEP:	
MD5:	CAB8BEABE7E66A4015C98A3C77B3698B
SHA1:	C960AAAEA7014E105290C7D0F09BFCA837C8E8CC
SHA-256:	75431010BFE77818B8BEF4B0C4B328C00668DC6B13C09AAB769EBF58BDA4EDF7
SHA-512:	0D1E94E84294AEA4BF400FF9D0654748BFFEB92D3A1643A6A13B541ADB1BC13EA2F649560A27C8CC3D8AEF9DA5D6B668C7E3BE696091CE882A475B91A9A4CAC8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230891381309","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230891381310","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39697},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230887958662","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230887958664","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":52163},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230886326794","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230886326795","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy

C:\Users\alfredo\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):	4339
Entropy (8bit):	5.026045858342657
Encrypted:	false
SSDEEP:	
MD5:	CA4D2FEF727DFCE29AEA28A3E4B19F55
SHA1:	F3DB1E1A7A787FC81C8D0B191218F62953EF282D
SHA-256:	83E01E3E1D4386D6DCB5AA9960E9AAC3C9798116DBBA9FA090D23F2F782F36CB
SHA-512:	BCE8B762577BA360F94EBD6ADFAB1B03AC38B08BC60B11019B43C2B51AAD3F9AF2D773D5473818FC06EBCBB3198DCAB05C305FDAE200839002D8855FA83A10E2
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298156341543530","alternate_error_pages":{"backup":true},"autocomplete":{"retention_policy_last_version":92},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2734,"this_week_services_downstream_foreground_kb":{"112189210":1,"115188287":51,"21145003":243,"35565745":2,"5151071":2}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298156341534964"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1653682743.314395,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm":{"product_category_for_s

C:\Users\alfredo\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):	16306
Entropy (8bit):	5.567749237713529
Encrypted:	false
SSDEEP:	
MD5:	ABBD1DBFAD5A09A1EB3E93D9FF911654
SHA1:	36B6F16265D69155E5FCBCB6E79889DCFE3C2463
SHA-256:	9C8808C368A0D0A0673F5FA8D5EE384605FE92BF24B9ED7BBD5C2426F0CB8442

SHA-512:	CCA191FF6C56C1D25E412FB513C613723CAC1A9CC1A50327BBAC5BA85B358F7BD3879C108BE61C13733EBFBE4B25AF1708323B1768C48BA8C95FFFB24B0136 23
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:mh t: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":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"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,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13298156340257038","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\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\21bba6cd-6715-4435-b492-c1c47b007104.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	139
Entropy (8bit):	4.762700853527964
Encrypted:	false
SSDEEP:	
MD5:	038931FF72A0C6AA0695A404960B1B22
SHA1:	90802F36B75C3CA70FC8CD1CF8BDFBAE0E8723A4
SHA-256:	BEF93811AE263E2E9145A44205340015843B1D4485D084BB642EAEB500FE564C
SHA-512:	97903821D21BB748255C29BE83BCA5BE61E0E36719050D4BB780EBC35424202A23F3ED4EE0056833E7748F1D55D82A5F38476298C5012202776BEA411DA7001E
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\alfredo\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:	
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 D58
Malicious:	false
Reputation:	low
Preview:	.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000001.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:	
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443

SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\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:	
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\MANIFEST-000001

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C2375B
Malicious:	false
Reputation:	low
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\a7209e08-6427-4eac-953e-fb4b5eaf5207.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):	16306
Entropy (8bit):	5.567749237713529
Encrypted:	false
SSDEEP:	
MD5:	ABBD1DBFAD5A09A1EB3E93D9FF911654
SHA1:	36B6F16265D69155E5FCBCB6E79889DCFE3C2463
SHA-256:	9C8808C368A0D0A0673F5FA8D5EE384605FE92BF24B9ED7BBD5C2426F0CB8442
SHA-512:	CCA191FF6C56C1D25E412FB513C613723CAC1A9CC1A50327BBAC5BA85B358F7BD3879C108BE61C13733EBFBE4B25AF1708323B1768C48BA8C95FFFB24B01362323
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":"13298156340257038","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\alfredo\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000006.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:	
MD5:	AEFD77F47FB84FAE5EA194496B44C67A
SHA1:	DCFBB6A5B8D05662C4858664F81693BB7F803B82
SHA-256:	4166BF17B2DA789B0D0CC5C74203041D98005F5D4EF88C27E8281E00148CD611
SHA-512:	B733D502138821948267A8B27401D7C0751E590E1298FDA1428E663CCD02F55D0D2446FF4BC265BDCDC61F952D13C01524A5341BC86AFC3C2CDE1D8589B2E1
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000006.

C:\Users\alfredo\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:	
MD5:	AEFD77F47FB84FAE5EA194496B44C67A
SHA1:	DCFBB6A5B8D05662C4858664F81693BB7F803B82
SHA-256:	4166BF17B2DA789B0D0CC5C74203041D98005F5D4EF88C27E8281E00148CD611
SHA-512:	B733D502138821948267A8B27401D7C0751E590E1298FDA1428E663CCD02F55D0D2446FF4BC265BDCDC61F952D13C01524A5341BC86AFC3C2CDE1D8589B2E1
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000006.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\f066315c-3d7d-4dae-9156-124a8978280e.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):	3488
Entropy (8bit):	4.93792117772315
Encrypted:	false
SSDEEP:	
MD5:	D85F9400DB57BBB7B6D53ADC4D39D191
SHA1:	3FB69E63E637245DB1C08B76DE4E9F374B8B2727
SHA-256:	430FC31FAE9EC39FF492157EB1EDC0D23BB5075D74136D69297E2FFB79943BF0
SHA-512:	37B80A00A10C16F961DE7415B1B864007757C754BD6174DAA4E51E3DDA1115A81257C876251B2EEE68B47F70935FB598E1AB1A49E0B7EC6DF80F92B02DDB292F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298156341543530","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_removed":true},"browser":{"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":{"this_week_number":2734},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298156341534964"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"product_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"51102b54-14a5-4079-bd8b-e6b63d8b2b64"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"9D17C7184A596066D76E13B1D59D5E14","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\f899b80f-8c64-433b-9da2-58d312288467.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):	876
Entropy (8bit):	5.586671718383061
Encrypted:	false
SSDEEP:	
MD5:	B8ED22BD70E1015C604A79706AFE3D14
SHA1:	1B071D6712D323D67E05451ACF16FCA8EDEF8BBD
SHA-256:	1C781386CB9D5E4A5FB36730719BFB580D477412FFC226061EAF6E4A6645F613
SHA-512:	B27387B06FD96624EB1C0032263DD25A2F5D513B4E130F071B05DB330558CD700E379C0605038C64DD29A1E51445DB744A852A2FFFEF8C95FB6B24BEEE4AA5F A
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1653686344.197085,"host":"QHMLOI4IZ5GDQrPC3KikxV8CDoZ8ptywnZykQU7Obws=","mode":"force-https","sts_include_subdomains" :false,"sts_observed":1653682744.197089},{"expiry":1654701301.094781,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_i nclude_subdomains":false,"sts_observed":1623165301.094784},{"expiry":1654701298.912333,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=" ,"mode":"force-https","sts_include_subdomains":false,"sts_observed":1623165298.912336},{"expiry":1654701286.340989,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2 C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623165286.340993},{"expiry":1654701300.827908,"host":"+ccWXqaoH J9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623165300.827911}],"version":2}

C:\Users\alfredo\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:	
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\alfredo\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):	2.873140679513133
Encrypted:	false
SSDEEP:	
MD5:	3A0E5D4F452CF99191634D0FFAB744A0
SHA1:	F115BBB898EEFF640D8D19AD44A86C3FCDFFC0AD
SHA-256:	B9D528D3AE283039F4700C7E4E790744C58A26353A91B536DD91CBA4F648A35F
SHA-512:	87BF9DB30598EC454A02A4A32E5458E83870524D4AA497CB167C8A92B7521204B7B75E2BE18D61F9FBE51CA7DE8E35782AA65E6F6F11E4A4926A9B6C85D6528 A
Malicious:	false
Reputation:	low
Preview:	92.0.4515.107

C:\Users\alfredo\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):	109671
Entropy (8bit):	6.065198803233404
Encrypted:	false
SSDEEP:	
MD5:	F862C51E63E2F1AE88879A6F57C73D4E
SHA1:	ECEDF94C16D667806041AB658B56735C5AE50EDD
SHA-256:	62E1FB3267BE3C7AA433ED6C4769FF3AF52D9EF70CB3CE17D7C3BEC5BFC9EA98
SHA-512:	5ACEDE139DFCF460824DE273A97D3A43BB6A382A69967D832EDEBC512B82B64DE12D2A02A62737A8BED5785835E816921CB82FAB02AAEC43AC2A3997A742CF26
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"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":1.653682742466372e+12,"network":1.653650343e+12,"ticks":168386431.0,"uncertainty":2827031.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187259629"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\alfredo\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):	95480
Entropy (8bit):	3.756568821221119
Encrypted:	false
SSDEEP:	
MD5:	FBB5ED735B8137CFA55078CC19A4FF48
SHA1:	86A0E131C89F9A92EA25618106235F29E222E63F
SHA-256:	7020574F85C5F3B970E22FC58F12CF89613FDC108945A287294975FF0F26C7A9
SHA-512:	C1610DCD971C740D64C84A654B8EB9A61B7D6A340C43400CCF371B0E335A663ED56F1959A53F1D51DC39BFE8F519AC52A64869E63FBC8C5AD4BA94AFBA5972B
Malicious:	false
Reputation:	low
Preview:	.t.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....puA...c.:.\.p.r.o.g.r.a.m. .f.i.l.e.s. .(.x.8.6.).\.m.i.c.r.o.s.o.f.t. .o.n.e.d.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.....f.i.l.e.s.y.n.c.s.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e."...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....2.1...0.8.3...0.4.2.5...0.0.0.3....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...l]8. ...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.7.-.Z.i.p.\.7.-.z.i.p...d.l.l.....n\....%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.7.-.z.i.p.\.....7.-.z.i.p...d.l.l.....7.-.Z.i.p.....7.-.Z.i.p. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....1.9...0.0.....l]8.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\d7ec130d-d787-480e-82fe-bbfd2e27b454.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):	109671
Entropy (8bit):	6.065198803233404
Encrypted:	false
SSDEEP:	
MD5:	F862C51E63E2F1AE88879A6F57C73D4E
SHA1:	ECEDF94C16D667806041AB658B56735C5AE50EDD
SHA-256:	62E1FB3267BE3C7AA433ED6C4769FF3AF52D9EF70CB3CE17D7C3BEC5BFC9EA98
SHA-512:	5ACEDE139DFCF460824DE273A97D3A43BB6A382A69967D832EDEBC512B82B64DE12D2A02A62737A8BED5785835E816921CB82FAB02AAEC43AC2A3997A742CF26
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"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":1.653682742466372e+12,"network":1.653650343e+12,"ticks":168386431.0,"uncertainty":2827031.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187259629"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\df762e06-ea47-4b4d-89f4-cd299bad136a.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):	105176
Entropy (8bit):	6.035098292167179
Encrypted:	false
SSDEEP:	
MD5:	F69F22ACEFBEDC5AE2A88FC19BE36C77
SHA1:	F552736FA55004DB6DB58C61EFD146AA5B6E078A
SHA-256:	B78AB26472986C4227D16857334233B0B1B22C120B20810CEB89744BE826935E
SHA-512:	4912D79A3341006152F6C77787332D36688A564835BA30DCCF28976EFAEE90E6E751E4A103577B4D83F5E2982A018DFBE62B7E7DC346554E388B7DA1A598AB2A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"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":1.653682742466372e+12,"network":1.653650343e+12,"ticks":168386431.0,"uncertainty":2827031.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"policy":{"last_statistics_update":"13298156339654847"},"profile":{"info_cache":{"Default":{"active_time":1653682741.229904,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Temp\1265fdd7-b325-4713-8bab-ac90b940fd66.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:	
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."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\alfredo\AppData\Local\Temp\3401be7f-e326-4c4f-89f4-aa17a0e1a6ba.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	28748
Entropy (8bit):	**7.9918576871001425**
Encrypted:	**true**
SSDEEP:	
MD5:	2A37AD0EC191D53104BB46953AC6C43C
SHA1:	FD23FFC5B7E4A6B45FBD88A486D15FAA51DC07AE
SHA-256:	51F075EB69486CB23B32A0776782B4A1B2AF204429AB94510469E02B115E56CC
SHA-512:	AEB91CB7902A800D7B0C43627EC2B52121BC41BA29A1B6ABEDBFCFA4802254A0594ED239EA7A3F8D40241E43D436428D1E4AC117BD97269D78460F82F9BDCF68
Malicious:	false
Reputation:	low
Preview:	...........Zms.6..._..p..[.(.b[...M....N{..t ...S.....v...H.q.g:....]...p..6I8_d...C.\p.X$.2.p.g.8I}8.".D)$<..O...}.J9.3..a.i.'...x.....5O...x.....I.M.!.'\.l.2.0.cN.fq....\.....7..,.....>.p...w&. KS.....(O.V>.....O.r..V~J.`....U(..Y..MIy..w..g0e.....D.,L..y..N.+..._....O.h.]...V....r.....O.|.:....Li..>COy.....N.h.....R....Q%.,Xr.y...G8=.A....!8(..L....c....sA....t.Vl:...v...G ;...^.l...#.t.>...k..d..kr...B.....Pb.0*..!..;9.....~....j;....j.*O..!B.....?....^.]....;...[.g.B...%..'.7;.9.>..gP. p8....5l.Y.....Jp..R,.?..b..8O.....h.X(..G.).Cz.C..%....x.ET.....AEi.../..0.. ....k.*t.. .wl..e...H.i.F.....?.....z...?.....(../.O..R.?.4..7...j ..Q.....l..ob!..A..j...@..!).....K...MW.U.N.....W..Bh'8.'.y....Y.[o...PI..W.*...i...r.e..=.k^.WC..Uy.j..687^.z.#u5.4O.....-j.j3..L. 1..F...8.....@l.9.c.aGC.R.&..j.Q-av?...[4.E..T8....u..+9.<.n.Qw.D..N..S..3.D..... .%C.j.7.Y.s(.0wq.ZI.#"#..[K.GJ ....4.....?

C:\Users\alfredo\AppData\Local\Temp\6ddee3e6-6cfb-4c59-a955-a3de15642fce.tmp

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

File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	3110
Entropy (8bit):	7.933903341619943
Encrypted:	false
SSDEEP:	
MD5:	A83A2746B84F1CF573B02965B72ED592
SHA1:	85CC572D6F90029EB99AAFA56297D1BCA494313A
SHA-256:	DF4B53C1C7C48E80753D4945E6EC7847084F51BF57F0ED9D341326C74651D6EC
SHA-512:	C287F479EF572A06FF191C4E9A8A718507C97A2A45CB265D7DC65DD7922B80D36CE7660EC5D7EA9F3D1F1EF71C51C3E4F3D7973754F97A89B4F14D1B1FDE70E
Malicious:	false
Reputation:	low
Preview:	.....ko.7.....J...../..v..... ....zE.\+.T..f..%wW.$.....p8/.....z..\|a...}.#y.`.l..7Kr..T:'.UE,.&.i..Y.....h...B.....gJ....%.\.?.f]1R..@3.jHA..eHi&.Q..`....g.__?'3^...@~X..a8..... .....UN..%...&.F..K19".Y:.).L.L..WL..xxD>.P@ ...&'..j..)%.Q\..<!.3n.<#....;.gd2.LZ....x.m&.e.`&;.KX..."...<G....8.R.jsd....g.)..?.$=UVT...#.+g.!.....R..1..#D.k...3.Bj3iT.....*.M. .L....}..S.K.....zi..n.A{.....n..o.0j..q...w...3.7.N..].>...zK..sr1#.d..Tk..ckB...<....j.a.M1oe.9.jIQ.y+...6.....]....v.X.....q.....a>...2`.WV.v.'..~.3*.4.'8...hkT.H..9SOIF.%...;n.6.U.... i!...2v.9/.;.....R..8.(..L.b....aY2ps% ."...x.V..Y[.h.....^.........U.....p.'.&m.....6..%pWE....:..o.k...<.....5....j.I...*9...f..3.....-..0..D;.....*S.td/...........^_.v.)y ..Uf..q>.v2...0....o....Y %5;.5fn..{.....p_.....B..V.....D.Y.I....q 3...sm.b..!..E....a. &.w.-.s..>..M_...`..0..k.!<SH...9$.....V.\A$..}..8....#`...,...3.W..k...\..xH.1).~.Y.L1.O...\.....k.....s..i+.....).0

C:\Users\alfredo\AppData\Local\Temp\83e67817-03b7-49e0-988d-1f43779420a4.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	234520
Entropy (8bit):	**7.998840139867434**
Encrypted:	**true**
SSDEEP:	
MD5:	71FF1204B60B0B391231CE253D7AF19B
SHA1:	FA096C9999E5C2B2307F06548B8A95032FB76ACF
SHA-256:	CBBB8EEA8095E9D7B1862F98FF03056C8B9DB3B5E7AC9DB6AD3BD38CF257A967
SHA-512:	131994DC031AE0CE49C90266F6EE272F5ABA9C179800C0F91FD2A211FF19F6582D9E3CB91BF0EDD0DB2B81F6560A8C7ACE040A494810A7754D83A9F464D6DE2
Malicious:	false
Reputation:	low
Preview:	.....Z{s...?.h.(..8...e.M.....P...V*E.[.....tg..}....$]{.j:..\|t....W..E.sC..g/iqg.....3bs.....?...Y.[.I...8.i..$..9..id.{...wy./..\.{Qd$.Z.....9.n=.3k...,...7pjV)....b\|4.....U..4.../.I.x.a..... ...a...N2.V...-.W....2.:..k..N$!_.u....Oi).5.Mn. ...M..b.X.. +....]qp|..^.w:.p.....:.....G.%...q.3.N..../.P..S0.'....Y.....I...cJ`..."A.%.N!...$C..K-da...f.....4..%.:...2"..[.../..fi_1.;..\|t.AEQ.j...v .de.....# }..s.J..BD.$.1..z...w^.Ky...=..y.b.....D.[[/.R.'..,?.\.,y.}.^.o}..8.'.~.2..z....Y..B.((u~3s...M..v.Z(v..~q..P...n.vTP....F.w#.Z.`..K.b.H1.(.F..F.5R.4.o..s..b.Q,.).5.u#.B...)6...b. ..w2.W@J..HJ...4\..^w...../Y..r.Z..k..g..}vvv..{`..O.5..DPzH.!*$.....X.v...=.).v./.....K9.c....Y....Lc.?..JP.$..[(.n.7....G.....gg4..1.(|..5..G..?.....1.E.....z..a...m.>.;.m.B.f....8`. ....o.y.UT.DP..e.+.....^....R...:.....&....z.j...~s(1VNh.....o.....#..M..n.....y.q... .~L .8.....Q.....-nqo.....f[..6.{zJ7B._..<mb.....S}A.M.NDd.g.

C:\Users\alfredo\AppData\Local\Temp\8b86b677-e793-4955-89c0-50d83b300d38.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	5168
Entropy (8bit):	7.956694278195136
Encrypted:	false
SSDEEP:	
MD5:	3E5CCD9B583763AF68E28C5101373167
SHA1:	2005CDC0A8070B65E321A197D576698ECC267496
SHA-256:	41412C0863920BA95E9FDBD3AF000CBE926A73C078997A233DF55379A5C4D274
SHA-512:	04BF4F7320326B085C40527797577D8770A30A1ED24A8587A000A5AE1D8F39E0B7F187DB14603295AC7A2901A4698683CC3BED2C2611539293A1927AB31BEAE1
Malicious:	false
Reputation:	low
Preview:	.....[ks.8..._.....#..,.G..8.;.55;.%..&5$e.....)..d._...%.....s.....+..Uv}...]rq.....luK.).zJh..3.&..Uu...W...s.H. .MV..\U3Ef.\.\|...TU.9.z)I...u.+.g3U`Zs.6d...JiJ.rU.IV.".'L\|8 .d..j.J..q.....O."..<,...n...~\|E.dV.u.O..'"...e.uyJ?..?]~.?.....M.,.7...j.,.fz].. >+o.gz....<^(5.Jg_.Ap.U.i.....?.8.....,.*.*./.iQ..8.....A.DO/....?.~..N.~a.-...g.N~.....o.^...L.mW.]:{..... ./.....[VkTu[wki.gK...;-.<...\.".3]..}V...)9i.V.P="m?.....V.i...7..S.U.d..(..\....g....bU.....}.....P9$.A...N..ckV..Qz..A....7..{pd.f.7....}6on.....7J;...Y..l>W...H.Z.....j..... Wk9vj+V.W.zAm.....P.oYo..|.....}.g.^.p...Z....l%cT|LN3..H.....{...~.J.%.!k.(.)..."....q.%.V.. d..MZ.`.....o..m3....1.../..jeH.....Q....X...j..o..|.o.r..nVw._...9 .....o...l....!...{....xU5.. }.x.I..3.vT%z.k..o.....^.S*.t(....+r\.u<...G.`.....g...r..?...}7.=.....c~.F.e..w.v$sC/.B.p.D~..J...:....7Vl3w...s.-"....]+..KO.~....%.I..?.&.o...\?.9..

C:\Users\alfredo\AppData\Local\Temp\ffc15e06-a205-4a54-a19b-fb5ba8b6890a.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)

Category:	dropped
Size (bytes):	101891
Entropy (8bit):	**7.9971613680976565**
Encrypted:	**true**
SSDEEP:	
MD5:	173CA02E5B06065771DEB2F28E4E5A9E
SHA1:	20F1774FB280C94C13082A255C27D7A786EFD5C7
SHA-256:	634557AE2916F2FAA0CBF2557F8F96E26845ABE94D2784FD73B169EC5618B186
SHA-512:	D947E3ED56BE1F3C668943E8F066F39650D2E0D76BF64BAD167E100B8B1066B88D8E851346AFBD9777E90445F41C5108A0A2F1514A3F28F02D4EC39978121E71
Malicious:	false
Reputation:	low
Preview:	...........{..0......&xqH.....zyIBv9....=...+......I6....3#.l.@..9.s].W7...h4..H...7.^.........Bg.....`.;.S...P............z.3.........9~.P..{..-.z........b.:......>..'....I8.......'v.M'E.?bA...N8.'.8I.._...< v&.pT{.L'Ne...#.S!].T.-+...r)5.j.U.8q....X..VPo.....F.o..A.~~.?.w......eNJ..a)....i....:?._^..v.<=ei...i.......Q...8k......~j.c.W......~...Q.yq..^9..z.......S..b.E..L3|.9S.pa...a....5...J.\. 2l..s..4.....S.u..o.|.Q.K.0.=........0....xj.4....Mie..C..3..... ....WN........4Vs.B..N.bD...VK%...mb...{{....pd..7..G.....}.J;"..4,.......A.R|0d..)..M......;;.8.h.C.u..pkM..Z@.......r..U....H.. .],..l:~p..8`....3....5.*.t../S{.{`.^kB=f......ZR..L.$t..D%I..xB../.{rb..h8.!.........Z.0........{PuK%Vv...RR.*.......j.vw.[B..$..|&..eZEW.Z[&..d>.o......@..t.z.O.12C......Kk..oS.[.0.M...<.z q#*g.r......"0+.[.....Tb.E....F...U..U0...G.........t!.+...&K.@.N.#R.]...+.;.M[..x,...J.l........&y.n.....j>..0.|W.+.S.0X.S.E..L....R.....W.u.g.S.&^.g..N/..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1293
Entropy (8bit):	4.132566655778463
Encrypted:	false
SSDEEP:	
MD5:	D7A97183BCBD5FB677AA84D464F0C564
SHA1:	CDBB279B864E2C0A51E0892B8714131802586506
SHA-256:	76EFAD74EB8256B942727C42261147EB9CCA48DA284DB3CDCE5DC6A3B4346F02
SHA-512:	36F0310DD06319E4A51F77E4C3D64F6276891CE6410FE2571324BB71F2FBCDA368EAC4267FF8268086BE6912E41787D0F70771755E3D49E3E8C26648EAC6EFC9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u043e\u043d\u0430\u0441\u0442\u043e\u044f\u0449\u0435\u043c \u043d\u044f\u043c\u0430 \u0434\u043e\u0441\u0442\u044a\u043f \u0434\u043e \u043f\u0440\u0438\u043b\u043e\u0436\u0435\u043d\u0438\u0435\u0442\u043e."},"craw_connect_to_network":{"message":"\u041c\u043e\u043b\u044f, \u0441\u0432\u044a\u0440\u0436\u0435\u0442\u0435 \u0441\u0435 \u0441 \u043c\u0440\u0435\u0436\u0430."},"app_name":{"message":"\u041f\u043b\u0430\u0449\u0430\u043d\u0438\u044f \u0432 \u0443\u0435\u0431 \u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0430 \u043d\u0430 Chrome"},"app_description":{"message":"\u041f\u043b\u0430\u0449\u0430\u043d\u0438\u044f \u0432 \u0443\u0435\u0431 \u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0430 \u043d\u0430 Chrome"},"iap_unavailable":{"message":"\u041f\u043e\u043d\u0430\u0441\u0442\u043e\u044f\u0449\u0435\u043c \u043d\u044f\u043c\u0430 \u0434\u043e\u0441\u0442\u044a\u043f \u0434\u043e \u0432\u0433\u0440\u0430\u0434\u0435\u043d\u0430\u0442\u0430 \

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	556
Entropy (8bit):	4.768628082639434
Encrypted:	false
SSDEEP:	
MD5:	58BA5F65ED971591D1F9D81848EE31D0
SHA1:	BDA3C8B74653334FC8F060CAFBCEA58DF0113AB7
SHA-256:	CDD91587F5AF2C865776B36A5E9A07B10D21B9D911DE0B814B7A1E94B14AE885
SHA-512:	BA2A6BAA3011A54E6B07E29DFD133009D66B6CFFF525DEC0024BDE55A9BED463AD130307EE64BFB4A983A11FFD6B44BD53ED38EB144083A2CBEFA8D85C4D5D41
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Ara mateix aquesta aplicaci\u00f3 no est\u00e0 disponible."},"craw_connect_to_network":{"message":"Connecteu-vos a una xarxa ."},"app_name":{"message":"Sistema de pagaments de Chrome Web Store"},"app_description":{"message":"Sistema de pagaments de Chrome Web Store"},"iap_unavailable":{"message":"La funci\u00f3 Pagaments a l'aplicaci\u00f3 no est\u00e0 disponible actualment."},"please_sign_in":{"message":"Inicieu la sessi\u00f3 a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped

Size (bytes):	550
Entropy (8bit):	4.905634822460801
Encrypted:	false
SSDEEP:	
MD5:	43161EFFA28A0DBFC67B8F7DBE1B5184
SHA1:	FE0A9235A59B51B7F564F14FF564344927F035B8
SHA-256:	3A04421DF5218E8ABD3B0E2AFE11E8338D7BDCBCD1ADB122416944B102BC9696
SHA-512:	FC6A391A4B37FFEE2182F29C1590E32766A1820DC58D0A70A8DD96D7ABE74B47181B24AFFF8ADAE12686CCB1B898DCDDB882EFD205C3387B5B6F3CFBE6E5E A78
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikace v sou\u010dasn\u00e9 dob\u011b nen\u00ed dostupn\u00e1."},"craw_connect_to_network":{"message":"P\u0159ipojte se pros\u00edm k s\u00edti."},"app_name":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"app_description":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"iap_unavailable":{"message":"Platby v aplikaci aktu\u00e1ln\u011b nejsou k dispozici."},"please_sign_in":{"message":"P\u0159ihlaste se do Chromu."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	505
Entropy (8bit):	4.795529861403324
Encrypted:	false
SSDEEP:	
MD5:	31264DDBF251A95DE82D0A67FA47DB3A
SHA1:	3A48DC7AF26A153594C7849E1D92AAC31296459B
SHA-256:	EDB51898A6C73D0090D6916B7B72EBAC71E964EABB5BA7CD68E21966024F0D23
SHA-512:	B97D61BD71E3F0A91FF1048D2ACAD4BC092CCAF157B7A96029B6AB5AF1812B01814E3153CD894307CB13DC132523EAC22B19CADA6B97F4B81B0D1132562317 B5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen er ikke tilg\u00e6ngelig i \u00f8jeblikket."},"craw_connect_to_network":{"message":"Opret forbindelse til et netv\u00e6rk."},"app_name":{"message":"Betalinger i Chrome Webshop"},"app_description":{"message":"Betalinger i Chrome Webshop"},"iap_unavailable":{"message":"Betaling i appen er ikke tilg\u00e6ngelig i \u00f8jeblikket."},"please_sign_in":{"message":"Log ind p\u00e5 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	516
Entropy (8bit):	4.809852395188501
Encrypted:	false
SSDEEP:	
MD5:	7639B300B40DDAF95318D2177D3265F9
SHA1:	BF9EFDF073231CB3FCFCA5CCCA25B079ECFC45BD
SHA-256:	356A9D4ADFEC484DA824E7A72059B724B1686FC90082F4A4B667630436D593B0
SHA-512:	70593318C6626B5D25729E8D8109D5611B95283266621BE60ADD7E60C0DD5BC43848E956C767251B7B3CCDF5A0929922DE38F90CC8632CCD0C1CCFC7D6DEFE 9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Die App ist momentan nicht verf\u00fcgbar."},"craw_connect_to_network":{"message":"Bitte stellen Sie eine Verbindung zu einem Netzwerk her."},"app_name":{"message":"Chrome Web Store-Zahlungen"},"app_description":{"message":"Chrome Web Store-Zahlungen"},"iap_unavailable":{"message":"In-App-Zahlungen sind momentan nicht m\u00f6glich."},"please_sign_in":{"message":"Bitte melden Sie sich in Chrome an."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1236
Entropy (8bit):	4.338644812557597

Encrypted:	false
SSDEEP:	
MD5:	3026E922B17DBEE2674FDAEE960DF584
SHA1:	76602B1E3449F1B67DE42FD31A581B0821BFEFF0
SHA-256:	876845B5A061FAB3CF2A1466E01015DC40DF8449F1CB4205F575CEBED8717BAD
SHA-512:	0C4DCB2589553F9F75534E6C702EBF9095665C93D213564265E39220A99B61BB112A3B20980CE0377C7E98878E3240EB87312B5ECE874382B7E9CA90A0016992
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0397 \u03b5\u03c6\u03b1\u03c1\u03bc\u03bf\u03b3\u03ae \u03c0\u03c1\u03bf\u03c2 \u03c4\u03bf \u03c0\u03b1\u03c1\u03cc\u03bd \u03b4\u03b5\u03bd \u03b5\u03af\u03bd\u03b1\u03b9 \u03b4\u03b9\u03b1\u03b8\u03ad\u03c3\u03b9\u03bc\u03b7."},"craw_connect_to_network":{"message":"\u03a3\u03c5\u03bd\u03b4\u03b5\u03b8\u03b5\u03af\u03c4\u03b5 \u03c3\u03b5 \u03ad\u03bd\u03b1 \u03b4\u03af\u03ba\u03c4\u03c5\u03bf."},"app_name":{"message":"\u03a0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03c3\u03c4\u03bf Chrome Web Store"},"app_description":{"message":"\u03a0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03c3\u03c4\u03bf Chrome Web Store"},"iap_unavailable":{"message":"\u039f\u03b9 \u03c0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03b5\u03bd\u03c4\u03cc\u03c2 \u03b5\u03c6\u03b1\u03c1\u03bc\u03bf\u03b3\u03ce\u03bd \u03b4\u03b5\u03bd \u03b5\u03af\u03bd\u03b1\u03b9 \u03b1\u03c5\u03c4\u03ae\u03bd \u03c4\u03b7 \u03c3\u03c4\u03b9\u03b3\u03bc\u03ae \u03b4\u03b9\u03b1\u03b8

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	450
Entropy (8bit):	4.679939707243892
Encrypted:	false
SSDEEP:	
MD5:	DBEDF86FA9AFB3A23DBB126674F166D2
SHA1:	5628AFFBCF6F897B9D7FD9C17DEB9AA75036F1CC
SHA-256:	C0945DD5FDECAB40C45361BEC068D1996E6AE01196DCE524266D740808F753FE
SHA-512:	931D7BA6DA84D4BB073815540F35126F2F035A71BFE460F3CCAED25AD7C1B1792AB36CD7207B99FDDF5EAF8872250B54A8958CF5827608F0640E8AAFE11E0071
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App currently unavailable."},"craw_connect_to_network":{"message":"Please connect to a network."},"app_name":{"message":"Chrome Web Store Payments"},"app_description":{"message":"Chrome Web Store Payments"},"iap_unavailable":{"message":"In-App Payments is currently unavailable."},"please_sign_in":{"message":"Please sign into Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	542
Entropy (8bit):	4.704430479150276
Encrypted:	false
SSDEEP:	
MD5:	3F4B0F56C2839839FC3E3270ED4CB7B6
SHA1:	0D74EA655EAE3990E95BD26F6E1467EDF3EB3478
SHA-256:	1912EA5E0A62BBC669DC14AB5A5BD5514B0502C483EE1F27C3F8834384187079
SHA-512:	4E6A828FE73FC4AB03F0EE966CE7BD8061575A059E90709F908D8D91C5F4EB6A8D25BBFA100E48AD7AC94E76D3BCD3547C277B4150D515222757CC9906AD202
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Esta aplicaci\u00f3n no est\u00e1 disponible en este momento."},"craw_connect_to_network":{"message":"Con\u00e9ctate a una red."},"app_name":{"message":"Sistema de pagos de Chrome Web Store"},"app_description":{"message":"Sistema de pagos de Chrome Web Store"},"iap_unavailable":{"message":"Los pagos en la aplicaci\u00f3n no est\u00e1n disponibles en este momento."},"please_sign_in":{"message":"Inicia sesi\u00f3n en Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	510
Entropy (8bit):	4.719977015734499
Encrypted:	false
SSDEEP:	

MD5:	1FD5DAF46C4D7C4F571C263EC37B943B
SHA1:	A57EE5EF6861F88005C2230EA3D633A1B4CA105A
SHA-256:	BCC2CF06F66E9E3BB4B7887D0EE0AE4A72A6C49F4B2A578A7733B78208984417
SHA-512:	79C3104F1DC51B17B062803209029C8165DBD391FBE0B69BB406D7B4F92FE1898CAC30E20C2E5CFB65D643B978095626C68EAA0CFCA064354D52D52D16BF21A 9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Esta aplicaci\u00f3n no est\u00e1 disponible en este momento."},"craw_connect_to_network":{"message":"Con\u00e9ctate a una r ed."},"app_name":{"message":"Sistema de pagos de Chrome Web Store"},"app_description":{"message":"Sistema de pagos de Chrome Web Store"},"iap_unavailable": {"message":"En este momento, Pagos En-Apps no est\u00e1 disponible."},"please_sign_in":{"message":"Accede a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	460
Entropy (8bit):	4.679279844668757
Encrypted:	false
SSDEEP:	
MD5:	0293A7BAE6EEE62C4067A80E262D6A2D
SHA1:	E76B07BD49FFBBFB6841B7335CBE7A9620714402
SHA-256:	D06F20D4D68D1DBB89EF7D8E405D9499CB2EB2560217CD5B4A51AB1DD50CAB44
SHA-512:	8BF97DA4038A9C4426A285D5FEF0953F4E7E6D0667091A39DE4D4C5B4C35FC7B6A804425DBB4B82356A93950738E4F0937DE1AD777AE75AAC9BFB97D63F771E 0
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Rakendus pole praegu saadaval."},"craw_connect_to_network":{"message":"Looge \u00fchendus v\u00f5rguga."},"app_name": {"message":"Chrome'i veebipoe maksed"},"app_description":{"message":"Chrome'i veebipoe maksed"},"iap_unavailable":{"message":"Rakendusesisesed maksed ei ole praegu saadaval."},"please_sign_in":{"message":"Logige Chrome'i sisse."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	568
Entropy (8bit):	4.768364810051887
Encrypted:	false
SSDEEP:	
MD5:	E5BBE7DBBE75F45BDCD49DB8C797106E
SHA1:	0F069D7D19768180945F0D8B67DC71262FD586A2
SHA-256:	BFFB2248B4C66306133FA6ECBB1541F44B3BE22CC8D9A338D690E0B1D0C85532
SHA-512:	F6FE20B7A3B99BDBBF6F4737C8C63FE3098F060E6791BC40ED0E95FA5F93AA55C2643766EA2BE099E42EC378CB6E4B6FE7B5F2DA56C03A6A990B94A1F872B8 25
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Sovellus ei ole t\u00e4ll\u00e4 hetkell\u00e4 k\u00e4ytett\u00e4viss\u00e4."},"craw_connect_to_network":{"message":"Muodosta verkkoyhteys."},"app_name":{"message":"Chrome Web Storen maksut"},"app_description":{"message":"Chrome Web Storen maksut"},"iap_unavailable":{"messag e":"Sovelluksen sis\u00e4iset maksut eiv\u00e4t ole t\u00e4ll\u00e4 hetkell\u00e4 k\u00e4ytett\u00e4viss\u00e4."},"please_sign_in":{"message":"Kirjaudu sis\u00e 4\u00e4n Chromeen."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	515
Entropy (8bit):	4.699741311937528
Encrypted:	false
SSDEEP:	
MD5:	658DAD2AF2DC3AC1567D84E8B95F68B0
SHA1:	EE1121215960EC5ED5F7B6BDB8E4680731EBF83D
SHA-256:	978BA6D814CF290016833BBAC22DC7C05C2C575B1D6429B9BB14F8C2156BCF29

SHA-512:	F2FB93245D80E2CB2CA1BB2B0654FE92AD9041A558850D78AF4031CB83D2AD3BF5ABCFE6BC32160D028CA3914FA69A64784858A34FA56389C08D52B316346A0 5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Kasalukuyang hindi available ang app."},"craw_connect_to_network":{"message":"Mangyaring kumonekta sa isang network."},"app_ name":{"message":"Mga Pagbabayad sa Chrome Web Store"},"app_description":{"message":"Mga Pagbabayad sa Chrome Web Store"},"iap_unavailable":{"message" :"Kasalukuyang hindi available ang Mga Pagbabayad na In-App."},"please_sign_in":{"message":"Mangyaring mag-sign in sa Chrome."},"jwt_retrieve_failed":{"message" :"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	562
Entropy (8bit):	4.717150188929866
Encrypted:	false
SSDEEP:	
MD5:	1E32A78526E3AC8108E73D384F17450B
SHA1:	BFE2E47D888BA530A27DD1BDE25C46433C2A545C
SHA-256:	80F6EE69F1E022812BCCC1DE1CDC53772CDF90F4E93224161B23FA607D45136A
SHA-512:	5504F6D440779BC96571863D60B1E175EEDDC2E65B1ABBCFCFD19123F329F2E025FBA4D49BD23E33B77FFB6061BA6645132E04D4A7DEDE77F514B2151CDDF8 96
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Application indisponible pour le moment."},"craw_connect_to_network":{"message":"Veuillez vous connecter \u00e0 un r\u00e9se au."},"app_name":{"message":"Paiements via le Chrome\u00a0Web\u00a0Store"},"app_description":{"message":"Paiements via le Chrome\u00a0Web\u00a0Store"} ,"iap_unavailable":{"message":"Les paiements via l'application ne sont pas disponibles pour le moment."},"please_sign_in":{"message":"Veuillez vous connecter \u00e0 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL_locales\hi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1055
Entropy (8bit):	4.454461505283053
Encrypted:	false
SSDEEP:	
MD5:	B739E3B798D3EEB8AFB3E368455A8E97
SHA1:	56E206DD0AC7EB7B179911BE3F7DD78059CBD4F3
SHA-256:	BA7A53A1398168719F2ACD58CC5FE06AB0B769ECA896D70E7208B18085B42FFA
SHA-512:	181A3B1275D1D17BD48EAA77805981A96E22589A38990214AF3ED029C4A37C2F05ECF747D8FCF816C2AAED6EF82403757F234D67C360A3A6E5DB6C3F59CA1A0 C
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0910\u092a\u094d\u0932\u093f\u0915\u0947\u0936\u0928 \u0907\u0938 \u0938\u092e\u092f \u0909\u092a\u0932\u092c\u0 94d\u0927 \u0928\u0939\u0940\u0902 \u0939\u0948."},"craw_connect_to_network":{"message":"\u0915\u0943\u092a\u092f\u093e \u0928\u0947\u091f\u0935\u0930 \u094d\u0915 \u0938\u0947 \u0915\u0928\u0947\u0915\u094d\u091f \u0915\u0930\u0947\u0902."},"app_name":{"message":"Chrome \u0935\u0947\u092c \u0938\u094 d\u091f\u094b\u0930 \u092d\u0941\u0917\u0924\u093e\u0928"},"app_description":{"message":"Chrome \u0935\u0947\u092c \u0938\u094d\u091f\u094b\u0930 \u0 92d\u0941\u0917\u0924\u093e\u0928"},"iap_unavailable":{"message":"\u0907\u0928-\u0910\u092a \u092d\u0941\u0917\u0924\u093e\u0928 \u0905\u092d\u0940 \u 0909\u092a\u0932\u092c\u094d\u0927 \u0928\u0939\u0940\u0902 \u0939\u0948."},"please_sign_in":{"message":"\u0915\u0943\u092a\u092f\u093e Chrome \u092e\ u0947\u0902 \u0938\u093e\u0907\u0928 \u0907\u0928 \u0915\u0930\u0947\u0902."},"jwt_retrieve_failed":

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
MD5:	9CF848209FF50DBF68F5292B3421831C
SHA1:	D29880B7B15102469123D8747BF645706CE8595B
SHA-256:	EA1744C3CFBAA684A31A00067E8493ED114EFF3E878C797C9C55A7B122D855CD

SHA-512:	B784AEE4926F850F30072ABDA85E2E2E3966285F14BDF647BD2A41C5C06CAB04BC962584830E4E913896010396EAD02D90528235B9D9EDA1BDEFBFBB5333EDF5
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_name":{"message":"Pla\u0107anja u web-trgovini Chrome"},"app_description":{"message":"Pla\u0107anja u web-trgovini Chrome"},"iap_unavailable":{"message":"Pla\u0107anje u aplikaciji trenuta\u010dno nije dostupno."},"please_sign_in":{"message":"Prijavite se na Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
MD5:	4AD92AFDE3408FBBE43B0C3C71677650
SHA1:	3488901077F336A3196F9AE116E36DF1674E1ACA
SHA-256:	61258FE04C23AE14FDC99EE846CEA71CC703990CC0F80C3934299646E86C475E
SHA-512:	EB945FA455DEB9D70033DC0A8AA55D1F47AA00214B70AD34D5419A54F9C05B267F96F9785139F452BEE6972376DDF13EE51C681845A2B0818172FB75BA1FD09
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."},"please_sign_in":{"message":"Jelentkezzen be a Chrome-ba."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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":"Pembayaran 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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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":"Pagamenti 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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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_connect_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"},"iap_unavailable":{"message":"\u30a2\u30d7\u30ea\u5185\u30da\u30a4\u30e1\u30f3\u30c8\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u305b\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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
MD5:	41F2D63952202E528DBBB683B480F99C
SHA1:	9DD998542DBE6609299D4A5A25364A32FA7D7865
SHA-256:	FF7C083CD1E6134DD8263C634336EB852274BAD1BFAD18762814C42BC65309D8
SHA-512:	7BD2E2D4264C6BD62DF2584F3C1D3A910C5C5A28F4532F1E8F0C2235E93714EDD6074EA24960D4DEB4F9125DA81CA813F06330EFF66FA8DF1552D1DAC6864 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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
MD5:	1D21ED2D46338636E24401F6E56E326F
SHA1:	24497EDB25724BC4A57823C5CD06F50DB9647DD4
SHA-256:	434A375C32B8A21C435511C551F740FD4D170EC528A8F4EFC3D798EA4A07B606
SHA-512:	10A870718CC6281EE09DE01900D303B06589D9281C5849D6105C6FCF58BFFA3855F29C6ECA3689FFE6EF304BABCF41C5700EE2D8AFE711D57CB711194366FA6 A
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\u012bkl u."},"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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
MD5:	22F9E62ABAD82C2190A839851245A495
SHA1:	E7F79BD875918F0D0799DB5F45FAC6297FB66AF7
SHA-256:	9FC1167626C97BCBFDAFF23C6033A44252F89A501AF1DF41C43CB3A994FEB09F
SHA-512:	F577F2F0C344C4E4050AF025A9FB9AC78CADF7FE177F63AB9863826A9808B7FBF5D3363E3B61D7A6DB083EF5EBAC5474D710347B701640AB9C229A3E5D1F0A48
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\u043d\u043e."},"craw_connect_to_network":{"message":"\u041f\u043e\u0434\u043a\u043b\u044e\u0447\u0438\u0442\u0435\u0441\u044c \u043a \u0441\u0435\u0442\u0438."},"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\u0430-\u043c\u0430\u0433\u0430\u0437\u0438\u043d Chrome"},"app_description":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u0430 \u0418\u043d\u0442\u0435\u0440\u043d\u0435\u0442\u0430-\u043c\u0430\u0433\u0430\u0437\u0438\u043d Chrome"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u0442\u0435\u0436\u043d\u0430\u044f \u0447\u0430\u0441\u0442\u044c \u0437\u0430\u043a\u0430\u0437\u0430 \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0430."},"

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
MD5:	92C1FAC62EB7F92EC3794D4A141BEF32
SHA1:	2AFA41BF51BF9A1089B0B92A9D2DC74299B79813
SHA-256:	9DF154C93B02695AF1CC39F085D9D178EC6AF131A62C2AFC65F125F8F9A5B7AC
SHA-512:	D0709E4F586EAC03548A47D72156CF48D9B4EB9AF9ED8335DF75F541AE1B4172541647EC8BA081965647A9EAE10DB342F87558977BE6075B2D3CC5C3995ED6E E
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\u0430 \u0443c\u0440\u0435\u0436\u0443\u0432\u0430\u0447\u0438\u043c."},"app_name":{"message":"\u041f\u043b\u0430\u045b\u0430\u045a\u0430 \u0443 Chrome \u0432\u0435\u0431-\u043f\u0440\u0434\u0434\u0438\u0430\u0430\u0432\u043d\u0438\u0446\u0438"},"app_description":{"message":"\u041f\u043b\u0430\u045b\u0430\u045a\u0430 \u0443 Chrome \u0432\u0435\u0431-\u043f\u0440\u0434\u0434\u0438\u0430\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\u0430."},"please_sign_in":{"message":"\u041f\u04

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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 \u043c\u0435\u0440\u0435\u0436\u0456."},"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 \u0412\u0435\u0431-\u043c\u0430\u0433\u0430\u0437\u0438\u043d\u0443 \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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
MD5:	34A839BC40DEBC746BBD181D9EF9310C
SHA1:	8B4EAA74D31EED5B0BABA3CA5460201F6B10DA46
SHA-256:	BB8742615E4CD996AE5D0200E443AE6A6F0B473255F03AFFDB8FB4660DE4554D
SHA-512:	EE81E5509CBC2CB2B6C834224688C1E1B1AA9AA3866C52F8EAED040D5C390653C52D8D681E2E2CF62906643962ABAC823D5B622385B983B21E0DCCAFDF281BFF
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>. . . . . </body>.</html>.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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..l.)..eu.Q.`.e.....gr.?>.s.l0.....@.~.Tr.[8.+.,.;..EE....S.*f.....,.....B8/D..;.9.q.....ukC...r.l.....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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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):	3313
Entropy (8bit):	7.846746884883354
Encrypted:	false
SSDEEP:	
MD5:	30899B6C4E4A757B8EC6DD2208ACDFB4
SHA1:	F2C5880A724C6D75CCE1B5191E0D82C3BC7DE768
SHA-256:	4F17EFBD974A41D88CB36567AAB6BF4586579E78780F00B1826676819E14BFF4
SHA-512:	58539E3F0AD7FEF30792EFCDBBD955599E11E4261C9946E7C3DFF6267E01747354EA3B901C46FC8329F81C68AFBEB2D05FE3FCB266BC5948DE8BEFA5B8D040 EE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a.....IDATx.....S.d.....x{g..T...9..:.3...a.9..J.V....a...(.,..,...P@..)..d.\.)...D..i.f.yI..e{m..|.~...}.MC_oRz.....}.7...^o.,...I...V.....Z.....]... ...>.(..._..r_Z... .....4x.....|>`A../.x<..n.{..@....@../.X#.....D..X..@....c."..+^. ..>!H.....6..,.KJ...u.j..$I".L.....n.O.{0.<D0p.!.N...l6."..@.K.>A0d...?...."...\....H0d.d.'.l.;".>...`.&$I...P..6.!.xO... EQ...Y.F~BE..ea.e".~[.F.![..?..f.....,..... m.....$I....`..8.....@f>.....".Fw.....<...7.k.l!p.(..p...v...E.....\|...@.P,...D.B..@. ...E."..../.....\|...@. ...\|...@. ...\|.../.....\|.....\..^..,.n... ..8o.....ib>....zc.....\|h .5.<..+...`...._.....,.....p....EK.a.X0...9)...QO.a.4....k...>.A.....`y{.4L....W>M.....^.N..<.[...w]..>.FK.O~...`...K.][...eY...H.+..z9...A..O3.)r;..c.u.B.....`^2...}.i. ^}.\.....w.u0....x~.u.....>.....~../_..2....;6..`(....MKE...f0."."I>."99.....y....Q.W$I.8]J0..AC(.*.....9_...g..#.....%.....8.c.h..0..?\e..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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):	531
Entropy (8bit):	7.465541280375791
Encrypted:	false
SSDEEP:	
MD5:	344554D96E418120BD80EF5DE5194697
SHA1:	23E141C3A6CE368ACC1C299F062AB85914BCB17E
SHA-256:	0A4BD08DB6422F8E7A8A218EF39C1B99A5A675F12697F26BE88F9AFC2E1F9378
SHA-512:	7AE38853E5ACCA479D7FD81D48BB88C671CF4DCE63342209BCFF045AC581A04B7B0ED48F6C58253DB950935C0522CAAA4FBC6CF5A25151A8960BA56FC80456 9E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDATx....k.a..?.]...Z5.P...`G77.....Q'q.....u..E...%.$].\...P.m5.....$M...K...#..p.....|.{.-*...Z....=._.Dc<.J.R...A.@....I)...Lb..s&.q.T_..|a.....z ..0..m[.+ ..T.R9.7.`0..$~.....H.Q\|.wg..r...E6n_.Y.E..x.(.....?{H.Z3;..="X.F.w.:.h...Z..V.S.\|..V.....{T-.y....*..>.>.fQ...a.I.<;I..yr.....Un....7w.....S.3.Fg\|.O..\.~{...S....d.....R .%.A...$.g.y..f.IW/..JC.z.H..)#....A+. .k.wb...p.m:a.?D.1GD.&..N.....?..\..n....W.O...j.%.`.*H.s.Fxt.\.....Yv.?.....f....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
MD5:	8803665A6328D23CC1014A7B0E9BE295
SHA1:	9DA6EE729D5A6E9F30658B8EC954710F107A641F
SHA-256:	D5F9234DC36E7FFA85F35B2359A4F82276F8395EFA76E4553507EA990B27FC6C
SHA-512:	ECD9E71B8BA1ED8BD4CA5A0936CB66A83611C4ABCBDA76C250F4CDF4AD80320212E8F5EEB79A38910718F8346ECC1AD580A3FA835EC2B22BE497F36899FB5930
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\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:	
MD5:	232CE72808B60CBE0F4FA788A76523DF
SHA1:	721A9C98C835D2CD734153BBE07833C6637ECD68
SHA-256:	AFA4EA944CBDEC8543242E627EF46D5BFD3766DCAC664E7E50CDEEF2B352740C
SHA-512:	4048EEA5A78DD569521C488C4CE4F7B77AC0454C92EE9107A81A1B3AF91A4EE036039AC1A0A6B8DD26B12E7F1595DB80B7FAA7B6A25D9032BF385528A81A8654
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\alfredo\AppData\Local\Temp\scoped_dir1836_251390515\CRX_INSTALL\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1098
Entropy (8bit):	4.919185521409901
Encrypted:	false
SSDEEP:	
MD5:	6CA25F3EF585B63F01BCDF8635120704
SHA1:	00C063811E31EA5F9A00F175A71EA25E7821F621
SHA-256:	49D9DE983F7436BA786E6E04A5A20C10F41687AE06B266B1B6553F696719563D
SHA-512:	566BFD9BADBD8951EE52E5911EB68B51E86286989096D32DE6E32A2523761B0E0AFCA251EF3BEA36B5D51FB8354A5FCA567772A02C3F3B9D8DFE529609FA043 0
Malicious:	false
Reputation:	low
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "name": "__MSG_APP_NAME__",. "description": "__MSG_APP_DESCRIPTION__",. "manifest_versio n": 2,. "version": "1.0.0.6",. "minimum_chrome_version": "29",. "default_locale": "en",. "app": {. "background": {. "scripts": [. "craw_background.js".]. }. },. "permissions": [. "identity",. "webview",. "https://www.google.com/",. "https://www.googleapis.com/*",. "https://payments.google.com/payments/v4/js/integr ator.js",. "https://sandbox.google.com/payments/v4/js/integrator.js".],. "oauth2": {. "auto_approve": true,. "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.read only".],. "client_id": "203784468217.apps.googleusercontent.com". },. "icons": {. "16": "images/icon_16.png",. "128

C:\Users\alfredo\AppData\Roaming\Microsoft\Spelling\en-US\default.dic

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	low
Preview:	..

Static File Info

No static file info