ID: 626007
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 13:16:19
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://w2globaldata.cabildodeagayu.com/1/?e=bGVzLmZyZWVsYW5kQHcyZ2xvYmFsZGF0YS5jb20= 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Yara Signatures 4
HTML 4
Sigma Signatures 4
Snort Signatures 4
Joe Sandbox Signatures 5
Phishing 5
Mitre Att&ck Matrix 5
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
World Map of Contacted IPs 7
Public IPs 7
Private 8
General Information 8
Warnings 8
Created / dropped Files 8
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\2cad7255-ef11-4d17-a149-cb7cbc0da973.tmp 8
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\4848847f-91c1-4e53-b8ed-35fa07f882ed.tmp 9
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\530b95db-01aa-4bf9-8717-dc92f8cdbc21.tmp 9
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat 9
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\0ca448c9-78d2-460b-9c92-ce1cc512665a.tmp 10
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\32a9dd66-c894-44c4-8624-a3edad10457a.tmp 10
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\6e77c6dd-2af4-4f57-a3d0-7721bcc1bc78.tmp 10
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\75ec2c7c-8ea3-4d99-a90d-20e797765180.tmp 11
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\7892608a-3318-4060-8b5f-327240587eb5.tmp 11
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\81525b54-71fd-427a-9ba9-bf7057bb00ae.tmp 11
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\81fbe44b-d8ee-4aae-9bdd-6ae85132d5bb.tmp 12
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\85412a21-56a5-45f0-bad0-80e2c58194b2.tmp 12
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Google Profile.ico (copy) 12
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache 13
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy) 13
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy) 13
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\c580ce7c-653a-4d64-99a8-1fc899809a61.tmp 14
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\aa124b56-4f78-4ba5-94fa-b0cfa0122b79.tmp 14
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\b9c35b92-094a-442c-af34-b108b9a8340b.tmp 14
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000006.dbtmp 15
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy) 15
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\e9e2db75-66d5-4f7e-a7bd-c324c0c86402.tmp 15
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Last Browser 16
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Last Version 16
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Local State (copy) 16
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\e05789a2-3daf-4062-8dac-1827dbc15ed4.tmp 17
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\e67b92c7-a15c-44d6-bb1e-e59cd8228137.tmp 17
C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\fcc5d586-ccf0-4bc2-a2a6-ae982dfcd8a7.tmp 17
C:\Users\alfredo\AppData\Local\Temp\1576_1134994523\manifest.json 18
C:\Users\alfredo\AppData\Local\Temp\1576_1134994523\ssl_error_assistant.pb 18

C:\Users\alfredo\AppData\Local\Temp\25eb09e9-2886-4de2-8bde-0f87c16edbb5.tmp 18
C:\Users\alfredo\AppData\Local\Temp\3ecff3c8-ba34-4dea-b8a0-895d33f6caea.tmp 19
C:\Users\alfredo\AppData\Local\Temp\72e92281-8389-40f8-970f-816258898005.tmp 19
C:\Users\alfredo\AppData\Local\Temp\b8a22276-17a0-4de0-b7ae-e846d4c03999.tmp 19
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\bg\messages.json 20
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\ca\messages.json 20
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\cs\messages.json 20
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\da\messages.json 21
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\de\messages.json 21
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\el\messages.json 21
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\en\messages.json 22
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\es\messages.json 22
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\es_419\messages.json 22
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\et\messages.json 23
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\fi\messages.json 23
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\fil\messages.json 23
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_metadata\verified_contents.json 24
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\craw_background.js 24
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\craw_window.js 24
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\css\craw_window.css 25
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\html\craw_window.html 25
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\images\flapper.gif 25
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\images\icon_128.png 26
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\images\icon_16.png 26
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\images\topbar_floating_button.png 26
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\images\topbar_floating_button_close.png 27
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\images\topbar_floating_button_hover.png 27
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\images\topbar_floating_button_maximize.png 27
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\images\topbar_floating_button_pressed.png
C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\manifest.json 28 27
C:\Users\alfredo\AppData\Roaming\Microsoft\Spelling\en-US\default.dic 28
Static File Info 28

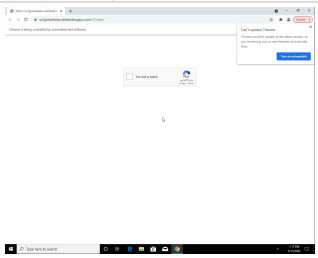
Windows Analysis Report

https://w2globaldata.cabildodeagayu.com/1/?e=bGVzLmZyZWVsYW5kQHcyZ2xvYmFsZGF0YS5jb20=

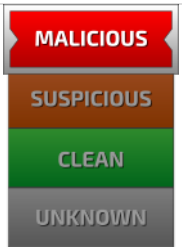
Overview

General Information

Sample URL:	https://w2globaldata.cabildodeagayu.com/1/?e=bGVzLmZyZWVsYW5kQHcyZ2xvYmFsZGF0YS5jb20=
Analysis ID:	626007



Detection



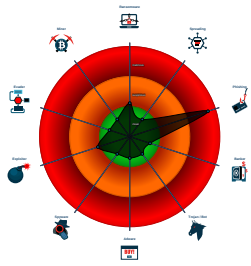
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Yara detected Captcha Phish
- Phishing site detected (based on im…
- HTML body contains low number of …
- Invalid T&C link found
- Suspicious form URL found
- No HTML title found

Classification



Process Tree

- **System is start**
- chrome.exe (PID: 1576 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation --single-argument https://w2globaldata.cabildodeagayu.com/1/?e=bGVzLmZyZWVsYW5kQHcyZ2xvYmFsZGF0YS5jb20= MD5: 74859601FB4BEEA84B40D874CCB56CAB)
  - chrome.exe (PID: 3584 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1740,8602215867310856610,17025399359111384958,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2096 /prefetch:8 MD5: 74859601FB4BEEA84B40D874CCB56CAB)
- **cleanup**

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
04956.1.pages.csv	JoeSecurity_CaptchaPhish_1	Yara detected Captcha Phish	Joe Security	
67398.3.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Yara detected Captcha Phish

Phishing site detected (based on image similarity)

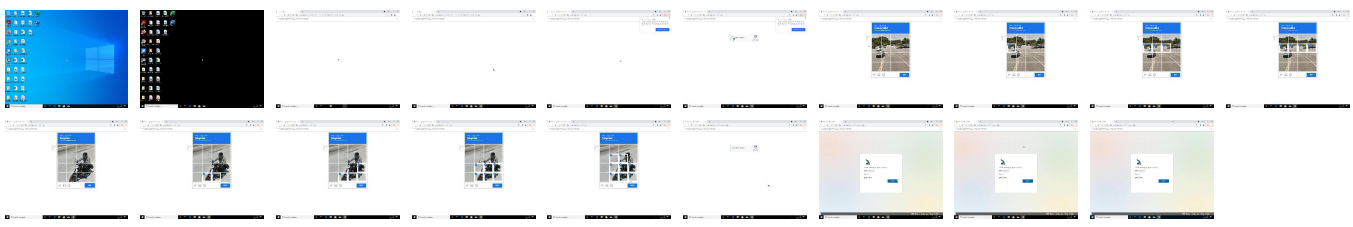
Mitre Att&ck Matrix

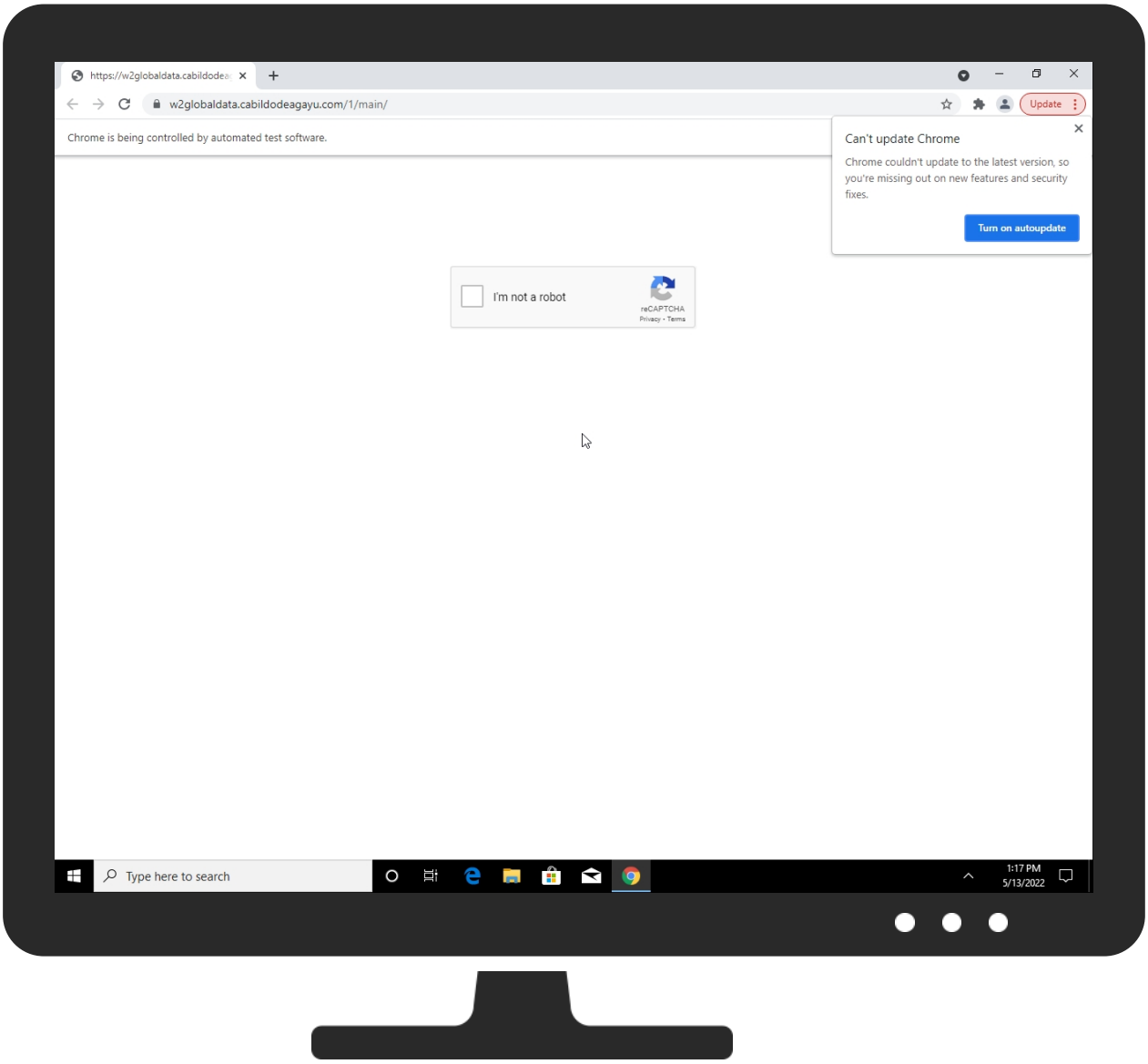
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	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	1 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	2 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	Protocol Impersonation	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://w2globaldata.cabildodeagayu.com/1/?e=bGVzLmZyZWVsYW5kQHcyZ2xvYmFsZGF0YS5jb20=	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

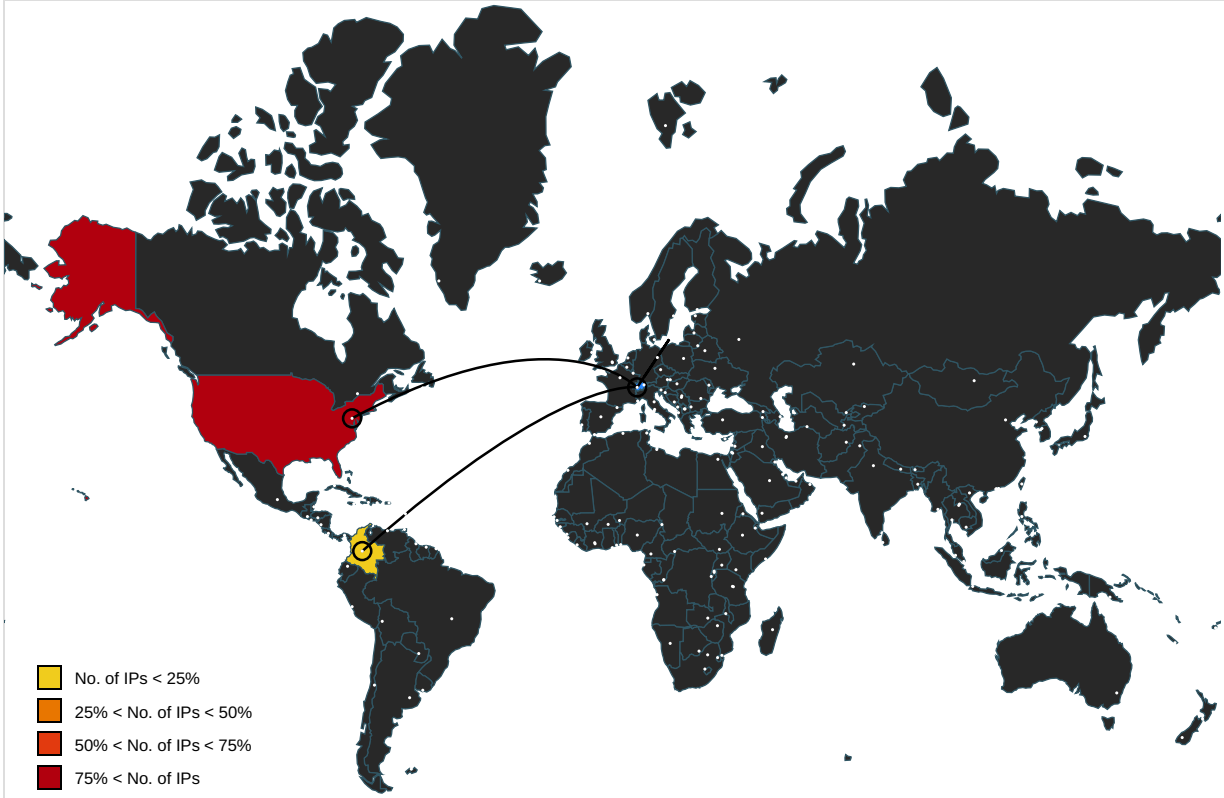
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.11.207	true	false		high
gstaticadssl.l.google.com	216.58.215.227	true	false		high
accounts.google.com	142.250.186.109	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.185.238	true	false		high
w2globaldata.cabildodeagayu.com	190.8.176.18	true	false		unknown
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://www.google.com/recaptcha/api2/bframe?hl=en&v=0aeEuuJmrVqDrEL39Fsg5-UJ&k=6LcJNLsfAAAAAFLIycbaJnhsCkE1TOU4w9VVo21f	false		high
https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcJNLsfAAAAAFLIycbaJnhsCkE1TOU4w9VVo21f&co=aHR0cHM6Ly93Mmdsb2JhbGRhdGEuY2FiaWxkb2RlYWdheXUuY29tOjQ0Mw..&hl=en&v=0aeEuuJmrVqDrEL39Fsg5-UJ&size=normal&cb=qvdjcd90eylf	false		high
https://w2globaldata.cabildodeagayu.com/1/main/	true		unknown
https://w2globaldata.cabildodeagayu.com/1/main/main.php	true		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.99	unknown	United States		15169	GOOGLEUS	false
142.250.203.106	unknown	United States		15169	GOOGLEUS	false
104.17.24.14	unknown	United States		13335	CLOUDFLARENETUS	false
104.18.10.207	unknown	United States		13335	CLOUDFLARENETUS	false
216.58.215.227	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	unknown	United States		15169	GOOGLEUS	false
142.250.185.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.185.227	unknown	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.11.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.109	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
65.9.63.90	unknown	United States		16509	AMAZON-02US	false
142.251.36.99	unknown	United States		15169	GOOGLEUS	false
190.8.176.18	w2globaldata.cabildodeagayu.com	Colombia		52335	ColombiaHostingCO	false
142.250.184.227	unknown	United States		15169	GOOGLEUS	false
74.125.162.166	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:	626007
Start date and time: 13/05/202213:16:19	2022-05-13 13:16:19 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://w2globaldata.cabildodeagayu.com/1/?e=bGVzLmZyZWVsYW5kQHcyZ2xvYmFsZGF0YS5jb20=
Number of analysed new started processes analysed:	13
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:	mal68.phis.win@26/78@5/211
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): CompPkgSrv.exe, SIHClient.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.251.36.99, 142.250.203.110, 74.125.162.166, 142.250.185.99, 142.250.203.106
- 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.
- Report size getting too big, too many NtSetInformationFile calls found.

Created / dropped Files

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\2cad7255-ef11-4d17-a149-cb7cbc0da973.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97592
Entropy (8bit):	3.756126954370138

Encrypted:	false
SSDEEP:	
MD5:	D43E217D38B30517C241DD35AAB238EA
SHA1:	3DEFD7A63BD161EC1604CD43DFA4876956034677
SHA-256:	5DCBDB55F51B3D8119DB6DF2CCB363C8FF1FB342F111FB0ADAB34B3FD14BE434
SHA-512:	2546BF1CB41E4526FFD113609CF9E143520920306A21C7C30B36DF7352FD2C1E4CD89F9D3CA04D1A77E06264DC257B121DB3B4E1AF7A5069C5EF6A0BA2588E A
Malicious:	false
Reputation:	low
Preview:	4}.....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....\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.....\8.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\4848847f-91c1-4e53-b8ed-35fa07f882ed.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):	102161
Entropy (8bit):	6.035907345314236
Encrypted:	false
SSDEEP:	
MD5:	85532D87604E7FFD74F76B888FCF35CD
SHA1:	912D9A09CCB746FE44AB4E4DEED493BBA4A86694
SHA-256:	56FDAD52DEB4F11AD82FBE49D8505DAA925E661A95F5E285ABDE6154EA3C26C4
SHA-512:	B9EB2DF68436200E6BD125F1D6A2EC33B8974385C656959781B6D1A047FECF2DA1612DF89830798008E5ACD5E7D9D29CD1FFB4C79D51CEF571BF706165779DI E
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":1.652473015952751e+12,"network":1.652440617e+12,"ticks":168866383.0,"uncertainty":3059637.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrda cpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtO EILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"policy":{"las t_statistics_update":"13296946613444869"},"profile":{"info_cache":{"Default":{"active_time":1652473014.739995,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\530b95db-01aa-4bf9-8717-dc92f8cdbc21.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):	106805
Entropy (8bit):	6.066535047060099
Encrypted:	false
SSDEEP:	
MD5:	A38124142048B310823921E6072907B6
SHA1:	B1B108004DF6A6F483579FB01DB97ED1FF933425
SHA-256:	0823BAE94060DED0E622769B8A7EC1C415C0F8D9D0F08CF4C9368305A034E892
SHA-512:	5047CADCE8B841CAA5ABB437FBF318777E37974D939153E2435943EBA07DC543EA769B04F112B6BE7646D6961B90CAF839D8C692ABF0DA9AA21FF90C73290A 6
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":1.652473015952751e+12,"network":1.652440617e+12,"ticks":168866383.0,"uncertainty":3059637.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrda cpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtO EILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_mana ger":{"os_password_blank":true,"os_password_last_changed":"13288110187799129"},"plugins":{"metadata":{"adobe-flash-player":{"displ

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:	modified

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\0ca448c9-78d2-460b-9c92-ce1cc512665a.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):	4453
Entropy (8bit):	5.040246155145368
Encrypted:	false
SSDEEP:	
MD5:	5AD290258A8015BB03E9BFEAE5228FD5
SHA1:	83070FC58E2C3E23BEC5B744EBF056641B0C84BC
SHA-256:	57A0D2D8EF4AD065A53F7DA9E5F9F2979DFC35D698A981714F0F5C6785877F1B
SHA-512:	EB4D1A2883B556C06CE0B1F247A95227240190B01A2B533B0DFC5A0525F7E64454082207369AD17A63D13EF98F5AAC365713F25F14C28A67BE2416E8170C1F0A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296946614970051","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":2732,"this_week_services_downstream_foreground_kb":{"112189210":19,"115188287":49,"21145003":243,"35565745":2,"49601082":3,"5151071":2,"54845618":23,"88863520":1}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13296946614948785"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1652473016.891464,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\32a9dd66-c894-44c4-8624-a3edad10457a.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):	5.555359798037096
Encrypted:	false
SSDEEP:	
MD5:	D0F5B1BB535D668B66C22F812F9053F5
SHA1:	C69FB20CA5114D24C93D7CF62636CAF85F0801D6
SHA-256:	2AD56F0D2A75B3AE503ECA4318F56C70AE4772E8A5F732FA7258D192D09A67FC
SHA-512:	9AC64358B47BC16D6BD9C5F1F72D31B5AAA77B3A568E28F7DBFF9F5C282A566F0EFCD174B34D61CF1C8CA7B554859A7DCBC24F95899CDD352760E3F9EFA02BCF
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":"13296946613773058","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\6e77c6dd-2af4-4f57-a3d0-7721bcc1bc78.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	181072

Entropy (8bit):	5.774426487043815
Encrypted:	false
SSDEEP:	
MD5:	1B40AC9ABB964672109D49ABFCFE2717
SHA1:	966E224F2887075825D42D2E7E0063BFAA81A99C
SHA-256:	503149B1B47F8296DEDB800251DBD9AF614856F0D7E6AB1C03DBC90EBCE53674
SHA-512:	00B50E49CAFD8246102BB460C7B96C20B50A2DDCB48A64C40D65901B517A2698DB9C5AA5EC7F143314DDB8D74624377F12A95C7F4D9FCE206473E8BBF12638B
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .2v...M..(..... .....]..X\.).H...>..Z.....\..._...V...F...A...A.....^..Wb...f.)...l...v.M...B...@..Wc...[.....z...`...J....9...E...k...R.D.....G...A.....;...E...h..XKd..KW.....D...>...=..X.... GQ.JW..;M..8K..@H..=;.....JV.YKV.IT.BS.Y.....(..... .....[..TZ.5.B...@..T.....X...]...`..\...K...D...A...;.....3...\...e... V...h.).d.G.<...F...@...3...^..Td...X.....e....v.....:...E...=..T`...d...h.B.....?...;...O...B...A...b.!.g...Ru.....9...8...P...C...C...l..U].M.5@.....6...C...@..T....EW..LX..=K..O b..Me..5R..AX..;V..++.....BL..KW..KW..DO..BL..EN..AJ..;1.....HT.UIV.FT.BQ.U.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\75ec2c7c-8ea3-4d99-a90d-20e797765180.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\7892608a-3318-4060-8b5f-327240587eb5.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):	16305
Entropy (8bit):	5.567780284200582
Encrypted:	false
SSDEEP:	
MD5:	CF0CA8828E330DA1BE47E15BE82EB0BE
SHA1:	C21CD5B9D29AF64ABB61FAF035595BE09433A847
SHA-256:	50E49CC4DE51599FE63CEFCD760AF95E68834C9D5D2C3E542F41D24AC68B4BF4
SHA-512:	6269AA114F25DB9F1F0666AE3AA59A69113DEFBC9513A5B37E00D042BBE83BD7D6F340BDD00B3AA0085F1DA5DB75B5FBC3F0CB3FF70338B175963D003864C96D
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":"13296946613773058","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\81525b54-71fd-427a-9ba9-bf7057bb00ae.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):	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\81fbe44b-d8ee-4aae-9bdd-6ae85132d5bb.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):	4.9389100345998305
Encrypted:	false
SSDEEP:	
MD5:	97220FDFBA04044D6A15DB4DAC8698E8
SHA1:	065BDBD3BA2F61AC2E4376DC8A37FF033C8863BC
SHA-256:	D5E528FE6CAD50AF7A8452EC7FCC86618E7AEDBFDD97DDCFB3E307E5882DA132
SHA-512:	07F7B6024972310DE476428AF832D2B2C275626284019A239F17F248DF8571BCFE59DBABAF5C65283E427BFA0E48943089654BC51400D0BA9BBA047C33EA60E4
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296946614970051","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":2732},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13296946614948785"},"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":"7a30a4e8-d622-4e59-8bb7-5bf95b7316fd"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"70E3BFF951D13519A71AB0B9C361F7DE","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\85412a21-56a5-45f0-bad0-80e2c58194b2.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):	4.939114239300741
Encrypted:	false
SSDEEP:	
MD5:	0F962A195AD8EE0F118BBD1E5AEB7F3E
SHA1:	0C863C1943DC1A19DC7FF48B37FE93F2B8A20FB2
SHA-256:	45C6B6284612483C61F5CE9CC3C15AA8E55B158E2FA201760592AB54F2570D90
SHA-512:	9D0B5DF540BC66756B2B93EA0B075DDC13C641DE5F7B3260E78FC7399E51256468A55E61A5234F69494AD04FD153DE2BC20463932A92919277885C1B1ED18BC
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296946614970051","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":2732},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13296946614948785"},"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":"7a30a4e8-d622-4e59-8bb7-5bf95b7316fd"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"70E3BFF951D13519A71AB0B9C361F7DE","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Google Profile.ico (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	181072

Entropy (8bit):	5.774426487043815
Encrypted:	false
SSDEEP:	
MD5:	1B40AC9ABB964672109D49ABFCFE2717
SHA1:	966E224F2887075825D42D2E7E0063BFAA81A99C
SHA-256:	503149B1B47F8296DEDB800251DBD9AF614856F0D7E6AB1C03DBC90EBCE53674
SHA-512:	00B50E49CAFD8246102BB460C7B96C20B50A2DDCB48A64C40D65901B517A2698DB9C5AA5EC7F143314DDB8D74624377F12A95C7F4D9FCE206473E8BBF12638 B
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... ....N..... .(....D..... .2v...M..(..... ....]..X\.).H...>..Z.....\..._...V...F...A...A.....^..Wb...f.)...l...v.M...B...@..Wc...[.....z...`...J....9...E...k...R.D.....G...A.....;...E...h..XKd..KW.....D...>...=..X.... GQ.JW..;M..8K..@H..=;.....JV.YKV.IT.BS.Y.....(..... .....[..TZ.5.B...@..T.....X...]...`...\...K...D...A...;.....3...\...e... V...h.).d.G.<...F...@...3...^..Td...X.....e....v.....:...E...=..T`...d...h.B.....?...;...O...B...A...b.!.g...Ru.....9...8...P...C...C...l..U].M.5@.....6...C...@..T....EW..LX..=K..O b..Me..5R..AX..;V..++.....BL..KW..KW..DO..BL..EN..AJ..;1.....HT.UIV.FT.BQ.U.....

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):	968
Entropy (8bit):	5.657492526324592
Encrypted:	false
SSDEEP:	
MD5:	1A9F23698EC98918476AAC655308C41A
SHA1:	A64588529AF9B2BCDD78A556C72A408790CEF23A
SHA-256:	11AA07A5D1491E081B31019A2B99655053FA2F8351854DF1C0BB7CB956782348
SHA-512:	D9DDA523AF3E0145F8237186F2463B714281CD8E903E42E3825C0F87526E44BEFBD242F24122F5C830988A1BCDFEF2896EBB3B84A8B3E81BE9A85DE0AD24C6E 5
Malicious:	false
Reputation:	low
Preview:	....."a....1.'bgvzlmzyzwvsyw5kqhcyz2xvymfszgf0ys5jb20..cabildodeagayu..com..e..https..w2globaldata..main*.....1...+.'bgvzlmzyzwvsyw5kqhcyz2xvymfszgf0ys 5jb20.....cabildodeagayu.....com.....e.....https.....main.....w2globaldata..2.....0.....1.....2.....5.....a.....b.....c.....d.....e.....f.....g.....h.....i..... ..j.....k.....l.....m.....n.....o.....p.....q.....s.....t.....u.....v.....w.....x.....y.....z...:U.....B.....y..... .....*Uhttps://w2globaldata.cabildodeagayu.com/1/?e=bGVzLmZyZWVsYW5kQHcyZ2xvYmFsZGF0YS5jb20=2.:.....W..... .....*.https://w2globaldata.cabildo deagayu.com/1/main2.:.....X..... .....*/https://w2globaldata.cabildodeagayu.com/1/main/2.:.....J'.....$(+-.....$(*.....$(*

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):	4453
Entropy (8bit):	5.040246155145368
Encrypted:	false
SSDEEP:	
MD5:	5AD290258A8015BB03E9BFEAE5228FD5
SHA1:	83070FC58E2C3E23BEC5B744EBF056641B0C84BC
SHA-256:	57A0D2D8EF4AD065A53F7DA9E5F9F2979DFC35D698A981714F0F5C6785877F1B
SHA-512:	EB4D1A2883B556C06CE0B1F247A95227240190B01A2B533B0DFC5A0525F7E64454082207369AD17A63D13EF98F5AAC365713F25F14C28A67BE2416E8170C1F0A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296946614970051","alternate_error_pages":{"backup":true},"autocomplete":{"retention_pol icy_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":2732,"this_wee k_services_downstream_foreground_kb":{"112189210":19,"115188287":49,"21145003":243,"35565745":2,"49601082":3,"5151071":2,"54845618":23,"88863520":1}}, "default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13296946614948785"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initiali zed":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1652473016.891464,"hash":"2jmj7l5rSw0yVb/vlW AYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a

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):	16305

Entropy (8bit):	5.567780284200582
Encrypted:	false
SSDEEP:	
MD5:	CF0CA8828E330DA1BE47E15BE82EB0BE
SHA1:	C21CD5B9D29AF64ABB61FAF035595BE09433A847
SHA-256:	50E49CC4DE51599FE63CEFCD760AF95E68834C9D5D2C3E542F41D24AC68B4BF4
SHA-512:	6269AA114F25DB9F1F0666AE3AA59A69113DEFBC9513A5B37E00D042BBE83BD7D6F340BDD00B3AA0085F1DA5DB75B5FBC3F0CB3FF70338B175963D003864C96D
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":"13296946613773058","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\c580ce7c-653a-4d64-99a8-1fc899809a61.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\aa124b56-4f78-4ba5-94fa-b0cfa0122b79.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):	4363
Entropy (8bit):	5.030675426775772
Encrypted:	false
SSDEEP:	
MD5:	B9C9FA52F410F961C9E2C5C9A60FE430
SHA1:	FE9AF36F2C916070D5F26E575EC0119567DE87A0
SHA-256:	90BC3A5A6719CE2FAEEDAD2CF52A87E5939FFB0AEFC21909BA013878CFBDE0ED
SHA-512:	32C4A12AE44991ED3411779B876445D30F39A5F8076FC824DEF488BE229211CF4B5858DE00F6739162461E9D3B57B79259E0F4CE3D64154D62E782BF2B1CAE4C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296946614970051","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":2732,"this_week_services_downstream_foreground_kb":{"112189210":2,"115188287":49,"21145003":243,"35565745":2,"5151071":2,"88863520":1}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13296946614948785"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1652473016.891464,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm":{"product_c

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\b9c35b92-094a-442c-af34-b108b9a8340b.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):	18395

Entropy (8bit):	5.555093006051866
Encrypted:	false
SSDEEP:	
MD5:	2DC7AF0DD852726CDF7BA0AAAEB59694
SHA1:	C80579155CBBC4B8F6849A26D4341BEC82FC97AF
SHA-256:	8EA2B6AF36C9BE136DF149781AD1E5DE7B28D47AC0FAF7AAA4130714583FA943
SHA-512:	B44F52A02D543B1949882833692331872 2BD28156A8A6DA388CFA509613023A24DAA456C1D33CB91351EC8E2643BF0EC5345D717589045B55B307B748BDB1851
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":"13296946613773058","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\e9e2db75-66d5-4f7e-a7bd-c324c0c86402.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):	5.5736730994543695
Encrypted:	false
SSDEEP:	
MD5:	503A210E9D5185E0D6C9D81D037B6033
SHA1:	AF2DEF9BFB8E5EACB2EDD5EF3E6A612D44D236F1
SHA-256:	E27B929B3FDAA219A7A489E11F7A5C258E073137F8CCF7AC3F88A352860D8743

SHA-512:	C269DE10371D2DBE9FFBE3F4779FBA78CD38D42EAA2D1BD51004B0104F3B88ACCBB4A8A1533FF5E72EB69537EE5566530C95D64A1E697ADE7550BCB7C8CC2BE9
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":"13296946613773058","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\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:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\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:	87BF9DB30598EC454A02A4A32E5458E83870524D4AA497CB167C8A92B7521204B7B75E2BE18D61F9FBE51CA7DE8E35782AA65E6F6F11E4A4926A9B6C85D6528A
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):	106805
Entropy (8bit):	6.066535047060099
Encrypted:	false
SSDEEP:	
MD5:	A38124142048B310823921E6072907B6
SHA1:	B1B108004DF6A6F483579FB01DB97ED1FF933425
SHA-256:	0823BAE94060DED0E622769B8A7EC1C415C0F8D9D0F08CF4C9368305A034E892
SHA-512:	5047CADCE8B841CAA5ABB437FBF318777E37974D939153E2435943EBA07DC543EA769B04F112B6BE7646D6961B90CAF839D8C692ABF0DA9AA21FF90C73290A46
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":1.652473015952751e+12,"network":1.652440617e+12,"ticks":168866383.0,"uncertainty":3059637.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187799129"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\e05789a2-3daf-4062-8dac-1827dbc15ed4.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):	106637
Entropy (8bit):	6.066225332720853
Encrypted:	false
SSDEEP:	
MD5:	465BD48390724C2AA3A188D8A6F2B3FC
SHA1:	C581267ACFB7E2A277EA5711CF710A6F260BF0BD
SHA-256:	8DD1ABD02E6CD4A10CEC5AC71099B2315A4E27BF0800399E3D09475552BA7581
SHA-512:	40F68508FF165273385CF1B928B37953CA6D2F4FA83CE8DD0DEEAFEEF698EE7E0CFFE54690C92547CFDC63FC6E2229BEC0FC0221BBC0FDCBFC1A418C454ED313
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":1.652473015952751e+12,"network":1.652440617e+12,"ticks":168866383.0,"uncertainty":3059637.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187799129"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\e67b92c7-a15c-44d6-bb1e-e59cd8228137.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):	102273
Entropy (8bit):	6.036823951976278
Encrypted:	false
SSDEEP:	
MD5:	6BB7B13B34F6D66910087AF9B6656C73
SHA1:	985EDE9D77CFD4F58F8ACF6D8BD2D288AEEF37D1
SHA-256:	E0A32C3EA4746CC6426AF92B4CCAD0E5A65633BA8BEF0FADA563B78E5354BC37
SHA-512:	681C57686BEB29DB181884A6FE26C15FD07520F3E2E4285DD492277C243689F32AACCBBE98F79E5D3AD6017E41994DDD14A37AE0492958E91534F4E31E27FB0
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":1.652473015952751e+12,"network":1.652440617e+12,"ticks":168866383.0,"uncertainty":3059637.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187799129"},"policy":{"last_statistics_update":"132969466134448

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\fcc5d586-ccf0-4bc2-a2a6-ae982dfcd8a7.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):	102273
Entropy (8bit):	6.036823569786087
Encrypted:	false
SSDEEP:	
MD5:	0810A8AB0145A8547EEFD26801979C93
SHA1:	713BB02CC2B8C07A4027E837026C1C96DD35A524
SHA-256:	D0C126D37B3FB40B28468BED61107EE86849E69BE5D1FA19D046BEC73B67EBEB

SHA-512:	A65823F6496D5FEC417AFC8F82E7EC2134799B886C64B0DDFE3D2FB590C435548BE6C71C23B274F28E120CFC955BCAB8F0E82C15F591263DEE3FF3BA4F847BDE
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":1.652473015952751e+12,"network":1.652440617e+12,"ticks":168866383.0,"uncertainty":3059637.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187799129"},"policy":{"last_statistics_update":"132969466134448

C:\Users\alfredo\AppData\Local\Temp\1576_1134994523\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	76
Entropy (8bit):	4.169145448714876
Encrypted:	false
SSDEEP:	
MD5:	4AAA0ED8099ECC1DA778A9BC39393808
SHA1:	0E4A733A5AF337F101CFA6BEA5EBC153380F7B05
SHA-256:	20B91160E2611D3159AD82857323FEBC906457756678AB73F305C3A1E399D18D
SHA-512:	DFA942C35E1E5F62DD8840C97693CDBFD6D71A1FD2F42E26CB75B98BB6A1818395ECDF552D46F07DFF1E9C74F1493A39E05B14E3409963EFF1ADA888971528
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "sslErrorAssistant",. "version": "7".}

C:\Users\alfredo\AppData\Local\Temp\1576_1134994523\ssl_error_assistant.pb

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2816
Entropy (8bit):	6.108955364911366
Encrypted:	false
SSDEEP:	
MD5:	E2F792C9E2DD86F39E8286B2EAD2FC70
SHA1:	8A32867614D2A23E473ED642056DED8E566687F9
SHA-256:	AC354A4723AAA4F06BEC385DDDE4A4D0983AD51456F52B31A8068EC97D5B5EA7
SHA-512:	6A7AF0CA1EFA65A89A9CA3B8DF0D2E24F21D91673C60CDFEEB02D33647442B01D535497249542F40E66E0D2DD3E9F8ED1F4A201FD97138D07A2B71366737E58
Malicious:	false
Reputation:	low
Preview:	...5.3sha256/fjZPHewEHTrMDX3l1ecEIeoy3WFxHyGplOLv28kIbtI=.5.3sha256/m/nBiLhStttu1YmOz7Y3D2u1iB1dV2CbIfFa3R2YW5M=.5.3sha256/8Iuf4xRbVCmCMQTJn3rxlgIIO1IOKoyuSUgmXyfaIKs=.5.3sha256/8IHdrS+r6IWzSMcRcD/GA6mBxk1ECX8tGRW0rtGWILE=.5.3sha256/k/2eeJTznE32mblA/du19wpVDSIReFX44M8wXa2JY30=.5.3sha256/urWd7jMwR6DJgvWhp6xfRHF5b/cba3iG0ggXtTR6AfM=.5.3sha256/IJPCDSE5tM9H3nuD5m6RU2i9KDdPXVn4qmC/ULlcZzc=.5.3sha256/0Gy8RMdbxHNWR2GQJ62QKDXORYf5JmMmnr1FJFPYpzM=.5.3sha256/8tTICtyaxIQrdbYYDdgZhTN0OpM9kYndvoImtw1Ys5E=.5.3sha256/F7HIlsaG0bpJW8CzYekRbtFqLVTTGqwvuwPDqnlLct0=.5.3sha256/zaV2Aw1A742R1+WpXWvL5atsJbGmeSS6dzZOfe6f1Yw=.5.3sha256/UwOkRGMlP0K/mKNJdpQ0sTg2ean9Tje8UTOvFYzt1GE=.5.3sha256/w7KUXE4/BAo1YVZdO3mBsrMpu4IQuN0mhUXUI//agVU=.5.3sha256/JnPvGqEn36FjHQlBXtG1uWwNtdMj1o2ojR/asqyypNk=.5.3sha256/AUSXlKDCf1X30WhWeAWbjToABfBkJrKWPL6KwEi5VH0=.5.3sha256/zSyVjjFJMIeXK0ktVTIjewwr6U5OePRqyY/nEXTI4P8=.5.3sha256/9dcHlrXN2WV/ehbEdMxMZ8IV4qvGejCtNC5r6nfTviM=.5.3sha256/E+0WZLGSIe5nddlVKZ5fYzaNHHCE3hNqi/OWZD3iKgA=.5.3sha2

C:\Users\alfredo\AppData\Local\Temp\25eb09e9-2886-4de2-8bde-0f87c16edbb5.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):	30948
Entropy (8bit):	**7.99105089802474**
Encrypted:	**true**
SSDEEP:	
MD5:	7F0FCE2F184F63FED8E9929FB106C282
SHA1:	0582EB5BFC7FCCCC1C77A860F00E351E61F5DC67
SHA-256:	7C33F333216849E50AFC9550DA7DA4450D221B837340716ACCEE3766FFD4A62B

SHA-512:	AD1CD5B804C08C4C25BD6F97153D3371156848A83682DF1829B0B113B60ED0B01D67B5CD737CB414C8B825E12C7E0D6B5F9B338F4AF7FC82BE8AAF4CA8E279BA
Malicious:	false
Reputation:	low
Preview:	.....y..../...*D4e.sH.v.{.....mv9MR...&..b.`.P."........r.....X...9s.s..w..;...>.}8...O.ep....O.]...$KO.tu...2?Yfi.'ove..T.....(.N7.R..<yr....t..}).....>[.....*."......'7.j.....#.n..e1..Fr.....j5xH.~.*...yvw....y.....vI.....IWT..)...|...\..<=.V.C..}.fF..T.....~.~..:).....i...2./D.}...]..<+3T..Z.Q9*0.....3..7.e..p.:..-.P..n.}j....U...."...|Gm...AdQ:*...gz%n..:...K.o[..."..n...(V..A...U.D.~x.Q..X.tw.F...,.Q...k.9.w.....2....t.....XF....E./...Hu.%..]....7.T...X.\$4.~.....`..e\....}.X...`A...J.....k...$IO..OS:...=...R...q.....FE.H.)M..WX/.....6..._..ry..J..`.q.'....x^..[r..Z.Y:..0..g.y....#.1.'...F7M.6...S....7.To.G.... `#.....-."...^....;..8..{.6VhL?%uU...K....O9.`Y....b.5.,zP.+\..!.1wK.j.P].....jW.!.j...i3.v.<..n.P..g....~.x..z.8...2^..U.f.bt#.+.U..N.....!.[.!#.C.A.xy.....p...n.mU,.....=.....h .ME..T/....IT\h,.U.....(.U ...Tf.?Zd8.2.V.....*..../....Oyh.j.._.I.k..u...).3.r.3...j.....O....+],...

C:\Users\alfredo\AppData\Local\Temp\3ecff3c8-ba34-4dea-b8a0-895d33f6caea.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):	20698
Entropy (8bit):	7.975385881517585
Encrypted:	false
SSDEEP:	
MD5:	9265F02CE35EA625F3F668EC99FD4C85
SHA1:	55EADB7E1B4757FFE05DA3C308EC043A9AB36EB2
SHA-256:	AFF12D4224C21AF5F3E8F3003FCA97A9E45E522E5B6CDCCB05E7CA99702F2D15
SHA-512:	FEB34353453FA022E9A9E31EC84540534A264B5CC9C8B7B2E9FF020214B9FA6BB5B254503C6E2490FE93936BACF8BC9BFC52FD5AEC329E45F4B20281B6505E41
Malicious:	false
Reputation:	low
Preview:	.....Ys.J.....:.t.O...G.&$..!SR.}.@!4.d#...N.l.r.{_.D. @.a.....?....!.....$k..eE...N.....{A...[....}|L.....}\l..h.K.r.1..n{Z.!.....FG..]5../..|...-..<].4a....9.]..+.~..HC...j.%O.T.*G.....EJRR...>...Q>.....:l..Dk...N....p*.%....x...R.em"..@....{.....L..\K..H.z.%5.S..D/.4..qM..lp....{Z..O.....X...6.R.X..F..fS.....E....tU.yr{.jh...Q.....Jv.o..BA.B.....ca9B..q..B.q...~..1....[v4@c.....>...C..2...h.sl..7....9...5Na..8.pZ.....}>X@C..8s..7.....Ku2.....:.u....8.6...6.4.%S;...I..M9YX...A; ..t....1...t...P...I|.&....#..~.....0..U.s.S..a..J.k}.M.r..#5=...["."S":C./kS....=+....dz.9^.....I>.6..W...S.|....g.f...c..6..{$.'.....Ji%.t.r.~..o....K...]..).L.i#..89.o..1.....o..u)m.J....R.om..V./...AGZz:fd(?.|cja..1..2..2v..9...S.8o.m].X#.}...b.sr..=|2.g.1..6....c.Ua..J.....=9e..?J...$].....jG.....7L..HS..o..*..q++.N^..\.;..9....t.,.^.....K...}N.-.|...#o.D9'..@..[.e6l..c..c..7W.....[|<.....mK0.#.

C:\Users\alfredo\AppData\Local\Temp\72e92281-8389-40f8-970f-816258898005.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..J,..l:~p..8`....3....5.*.t../S{.{`.^kB=f.....ZR..L.$t..D%l..xB../.{rb..h8.!.....Z.0.....{PuK%Vv...RR.*.....j.vw.[B..$..|&..eZEW.Z[&..d>.o.....@..t.z.O.12C.....Kk..oS.[.0.M...<.zq#*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\b8a22276-17a0-4de0-b7ae-e846d4c03999.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."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5SI..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488CB

Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\en\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BE/ D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF5 2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL_metadata\verified_contents.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	7780
Entropy (8bit):	5.791315351651491
Encrypted:	false
SSDEEP:	
MD5:	0834821960CB5C6E9D477AEF649CB2E4
SHA1:	7D25F027D7CEE9E94E9CBDEE1F9220C8D20A1588
SHA-256:	52A24FA2FB3BCB18D9D8571AE385C4A830FF98CE4C18384D40A84EA7F6BA7F69
SHA-512:	9AEAFC3ECE295678242D81D71804E370900A6D4C6A618C5A81CACD869B84346FEAC92189E01718A7BB5C8226E9BE88B063D2ECE7CB0C84F17BB1AF3C5B1A3 C4
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfbG9jYWxlcy9iZy9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiZHUtdGRPdUNWcmxDY254Q0poRkg2NXpLU05vb1RiUE56bDNHbzdRMGJ3SSJ9LHs icGF0aCI6Il9sb2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJ6ZGtWaF9XdkxJWlhkck5xWHBvSHNRMGh1ZGtSM2d1QlMzb2VsTEZLNklVIn0seyJwY XRoIjoiX2xvY2FsZXMvY3MvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6Ik9nUkNIZlVoam9xOU93NHFfaEhvTTQxNzNMelJyYkVpUVdsRXNRSzhscFkifSx7InBhdGg iOiJfbG9jYWxlcy9kYS9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiN2JVWW1LYkhQUUNRMXBGcmUzTHJySEhwWk9xN1c2Zk5hT0laWmdKUERTTSJ9LHsicGF0aCI6I l9sb2NhbGVzL2RlL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJOV3FkU3Rfc1NFMm9KT2VuSUZtM0pMRm9iOGtBZ3ZTa3RtZGpCRGJWazdBIn0seyJwYXRoIjoiX2x vY2FsZXMvZWwvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6ImgyaEZ0YUJoLXJQUEtoUm00QkFWM0VEZmhFbnh5MElGOVhYT3Z0aHhlNjAifSx7InBhdGgiOiJfbG9jY Wxlcy9lbi9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoid0pSZDFmM3NxMERFVTJHLXd

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\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:	FEDE6DB31F2AD242E7BC7B52A8859BA7F466A0B920A8DADCB32DCFB5B2A2742E98B767FF22E0C5BC5C11FEC021240AA9E458486C9039EB4EBE5CF6AF7BE9 7BF2
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.A SSUME_NO_NATIVE_SET=!1;e.SIMPLE_FROUND_POLYFILL=!1;e.ISOLATE_POLYFILLS=!1;e.FORCE_POLYFILL_PROMISE=!1;e.FORCE_POLYFILL_P ROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;.e.defineProperty=e.ASSUME_ES5||"function"==typeof Object.defineProperties?Object.defineProperty:funct ion(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,"obje ct"==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_dir1576_1677723441\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:	26835B4C050F53AD2DDB84469DF9A84BBB2786A655AB52DFC20B54BEDCB81D1ECD789198D5B7D8B940242E5CEAC818A177444D402397AE82C203438C4B1D19 CB
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_dir1576_1677723441\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_dir1576_1677723441\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_dir1576_1677723441\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]]$ueW.NyQ.IoL!AoF#9h>7.0t..%..,.@.m4..7..!.....,.....9.:.h0.bT(6.!l.&..("g*k..JL1.[....o. .(:..B(.6."...Z.CUyh0.....j.C.z8..S....2.T'...Q..4 g]]$ueW.NyQ.IoL!AoF#9h>7.0t..%..,.@.m4..7..!.....,.....'..w=.....\.)._6.k..OF...n.#\~"....2b3..I.)..eu.Q.`.e.....gr.?>.s.l0.....@.~.Tr.[8.+.,;..EE....S.*f.....,.....B8/D..;.9.q.....ukC...r.I.....j.....BGY...o2J....+O4....X4.....cH%7....I.....0H!.!.....!.,.....p8.a$....hh@.4....X,A.0L..(....JX.j...,.....z.X.Q....jB.d....B..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_16777234441\CRX_INSTALL\images\icon_128.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4364
Entropy (8bit):	7.915848007375225
Encrypted:	false
SSDEEP:	
MD5:	4DBC9F9E6F5A08D299BAC9E54DF07694
SHA1:	BB38F5DE34B1E0BE1109220BA55271087A4D9EA5
SHA-256:	91C2718DD23B4356D71F88F6146868369033291086DF327534546DFA459BEB0E
SHA-512:	A5F2B1F47502836130D8083F757B7773C1E1CB36B76AD298CC29AB2B428C8002D2F15BD839838FC326DAC3681C2F48AB25A3E7631D33726C4B25E8EC1417091
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a.....IDATx..yp.....gF#.:,[H.l.l..8...`/.k....,!a7Km...E...Te..T.....J...p....%.(....+...3....eY.e...L.o...5....h4...\....{?....~.u.`0.....`0.....`0.....`.Y.....[(.....).4....ai..w38.+....Bf././..]...{.....8...3.....3W~OJ.. /...u6V.C..U.0.+._=.c..9.X.?....L....S@.L...m.0..>.C...L|TF.p5..f4M.,.V....8..a.<...RP..@)E,..E"...h.....!...-....I..T.....m..._[[{w{{....{*.^.....M.x..h4.h.....\.R.E....j).7.....h4.A.E.....,. ...iii.Vj?2...=/.B.FK9P..@)=Rj..D".Y...2.B..x.}0...&J...2.....f.O..e.H.....!.J)'I..R....B.....QJ;K..L...L.I".L~mhh.R.@).FFF~.L&...~.B.....u.....}.....~.....f..yUU.....^M...6.....],w.e..~.!$.C.R.....E(%e9.,....k..@...W8.....@.....O..@%.~..@.S..P.....`Tp...."...?ME..c.....s...`..S1...7.b..aNE..k...3.yP.}.Ch.}.....B.....IPE..C.<....T....k.....Z..o_.....g.....P..A=y.J.)h..@.q.-.*].AU.4...F.M.....y%B]+ .\.~..9.....:..=...r.....E].o...F..P.....i...\....

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_16777234441\CRX_INSTALL\images\icon_16.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	558
Entropy (8bit):	7.505638146035601
Encrypted:	false
SSDEEP:	
MD5:	FB9C46EA81AD3E456D90D58697C12C06
SHA1:	5FC450F7D73CCFAC8F0D818CB3392BA4D91B69DE
SHA-256:	016CA659BA080E194FBFC0929602B16506ED60AA6019FAA51410C4FD93B583E8
SHA-512:	ADD810EE9EB7CAEC505B5FD90A1F184CE39D8F8C689DCC240F188FE353B9575489492E07D572A3B1C11A1555CE66AFCA5134903E4C1AA3D54BC7C5ED3E65B50C
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDAT8...Mk.Q...;... .....F..QW.....F....J.?.w..7~.....'.Q..B]... .QS...M&_w..b&.|`.....p...f.?.D$.y^.....y*...\..Z..t6..oRj.@&.u..G.qN).t.-V*.>(.N.Ep]wFk.60o.]0.`Y..cT..Y.Tb.`DF.d..s.Z..E..9.4._C.._...%..*.^....4.l...Y..X..R..../...Wj+w0[.]..._B.k.${.\.>.%.....lz .w.ALxo.2;..a..".p..S..&..uXS...<..6..[..zD.._.N+w.WbM7ye6X<..'(,=.r}.....$f..5..P....k..."..8.s.<zgSm@.....).Y.....:e..\.....F...I..A$.....T?.....m....8.....N...z.....V..vd.h'....C.?.....H.;]..C.M.....9.b.....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_16777234441\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_dir1576_1677723441\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_dir1576_1677723441\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_dir1576_1677723441\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_dir1576_1677723441\CRX_INSTALL\images\topbar_floating_button_pressed.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.46068685940762
Encrypted:	false
SSDEEP:	

MD5:	E0862317407F2D54C85E12945799413B
SHA1:	FA557F8F761A04C41C9A4BA81994E43C6C275DBB
SHA-256:	5C10CE0589EB115600F77381130B70AE0B7B3752614D86D4C89E857658AA222B
SHA-512:	07CB69327961FD0019BEF8EF7590B5524905AC373A815F73F6D9E0B26840929F919A96CAA977D4B5656704DACD0F352D568FB3997F80EE6BB94C95B58839DBFE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...A..0...+B..@wu...*.....$.<u..[.....h.....M..x(....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir1576_1677723441\CRX_INSTALL\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1322
Entropy (8bit):	5.449026004350873
Encrypted:	false
SSDEEP:	
MD5:	01334FB9D092AF2AA46C4185E405C627
SHA1:	47AD3C0E82362FFE5B881DF8D71D6F79AB7F5796
SHA-256:	F52714812D68C577A445169D11E84DF6751C2D6886BC429643072BB5D61C6C27
SHA-512:	888D96ADB7A847ABE472145258C8C46950EB2FA3BA7D596C2E90A17C8FB06FD0155C56CC8ABA5D076D89368417464BCB2D236F9E40E53241950A01F9F8ED548F
Malicious:	false
Reputation:	low
Preview:	{.. "app": {.. "background": {.. "scripts": ["craw_background.js"].. }.. },.. "default_locale": "en",.. "description": "__MSG_APP_DESCRIPTION__",.. "display_in_launcher": false,.. "display_in_new_tab_page": false,.. "icons": {.. "128": "images/icon_128.png",.. "16": "images/icon_16.png".. },.. "key": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrKfMnLqViEyokd1wk57FxJtW2XXpGXzIHBzv9vQI/01UsuP0lV5/lj0wx7zJ/xcibUgDeIxobvv9XD+zO1MdjMWuqJFcKuSS4Suqkje6u+pMrTSGOSHq1bmBVh0kpToN8YoJs/P/yrRd7FEtAXTaFTGxQL4C385MeXSjaQfiRiQIDAQAB",.. "manifest_version": 2,.. "minimum_chrome_version": "29",.. "name": "__MSG_APP_NAME__",.. "oauth2": {.. "auto_approve": true,.. "client_id": "203784468217.apps.googleusercontent.com",.. "scopes": ["https://www.googleapis.com/auth/sierra", "https://www.googleapis.com/auth/sierrasandbox", "https://www.googleapis.com/auth/chromewebstore", "https://www.googleapis.com/auth/chromewebstore.readonly"].. },.

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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	low
Preview:	..

Static File Info

No static file info