ID: 655631
Sample Name:
test@somewhere.com.html
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 11:27:46
Date: 01/07/2022
Version: 35.0.0 Citrine

Table of Contents

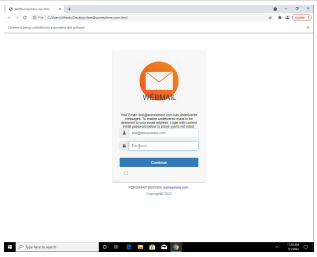
Windows Analysis Report

test@somewhere.com.html

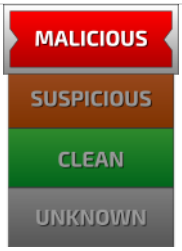
Overview

General Information

Sample Name:	test@somewhere.com.html
Analysis ID:	655631
MD5:	2d475c74396d3a..
SHA1:	8be111091be27e.
SHA256:	1dffbbe9eb7c804..
Infos:	YARA



Detection



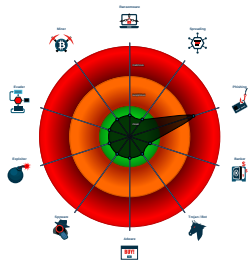
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish44
- Snort IDS alert for network traffic
- HTML body contains low number of ...
- None HTTPS page querying sensitiv...
- No HTML title found

Classification



Process Tree

- **System is start**
- chrome.exe (PID: 2452 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation --single-argument C:\Users\alfredo\Desktop\test@somewhere.com.html MD5: 74859601FB4BEEA84B40D874CCB56CAB)
  - chrome.exe (PID: 7724 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1728,15277383464472110615,3560837105709000163,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2108 /prefetch:8 MD5: 74859601FB4BEEA84B40D874CCB56CAB)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
test@somewhere.com.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query for .to TLD - Source IP: 192.168.2.3 - Destination IP: 1.1.1.1

Timestamp:	192.168.2.31.1.1.152544532027757 07/01/22-11:29:02.198300

SID:	2027757
Source Port:	52544
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish44

Networking

Snort IDS alert for network traffic

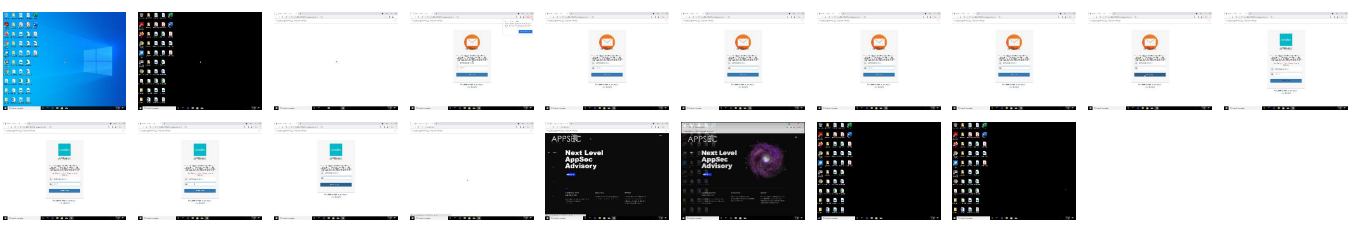
Mitre Att&ck Matrix

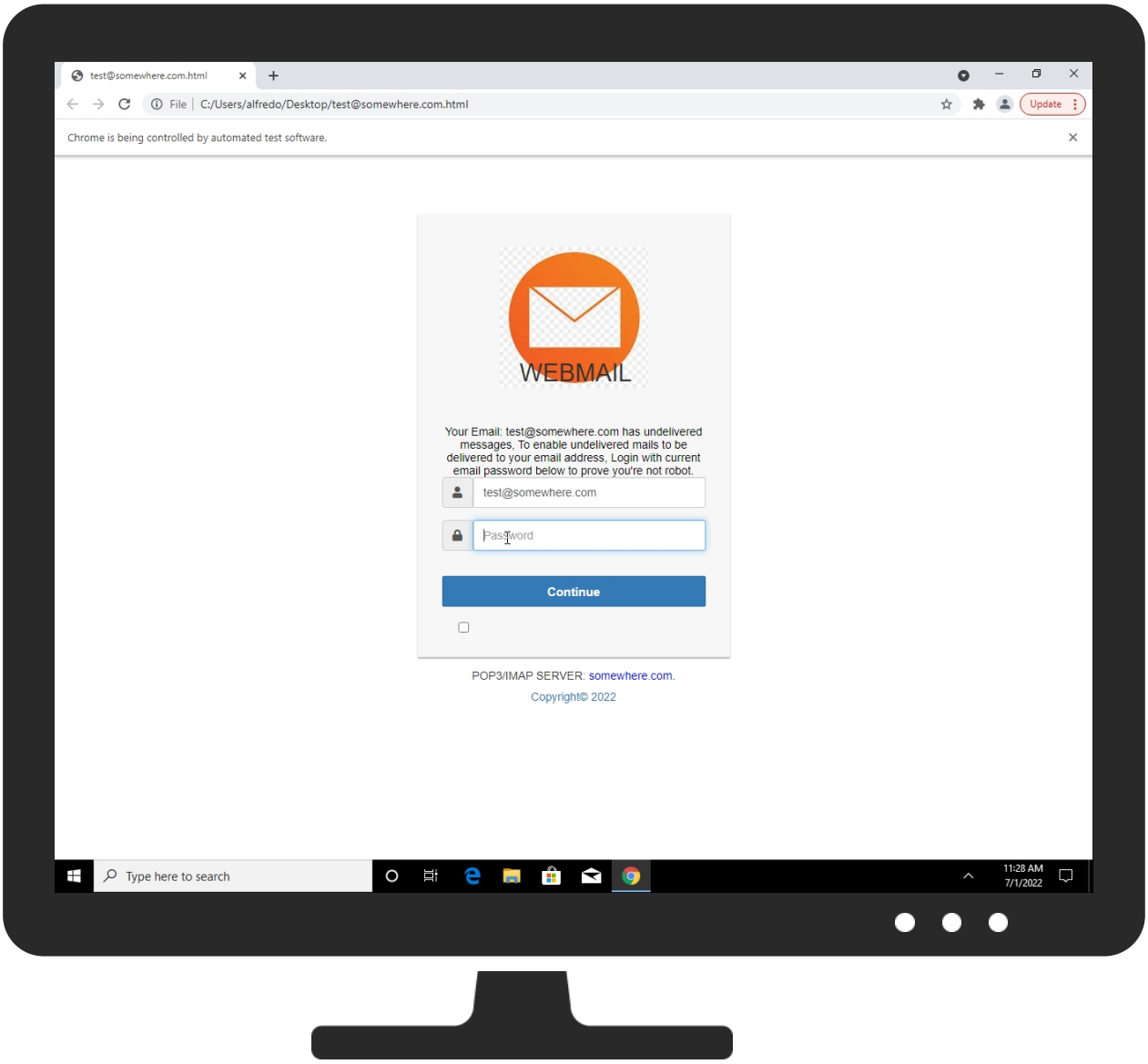
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Extra Window Memory Injection	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Extra Window Memory Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
us-east-1.route-1.000webhost.awex.io	1%	Virustotal		Browse
www.somewhere.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.somewhere.com/	0%	Virustotal		Browse
http://www.somewhere.com/	0%	Avira URL Cloud	safe	

Domains and IPs

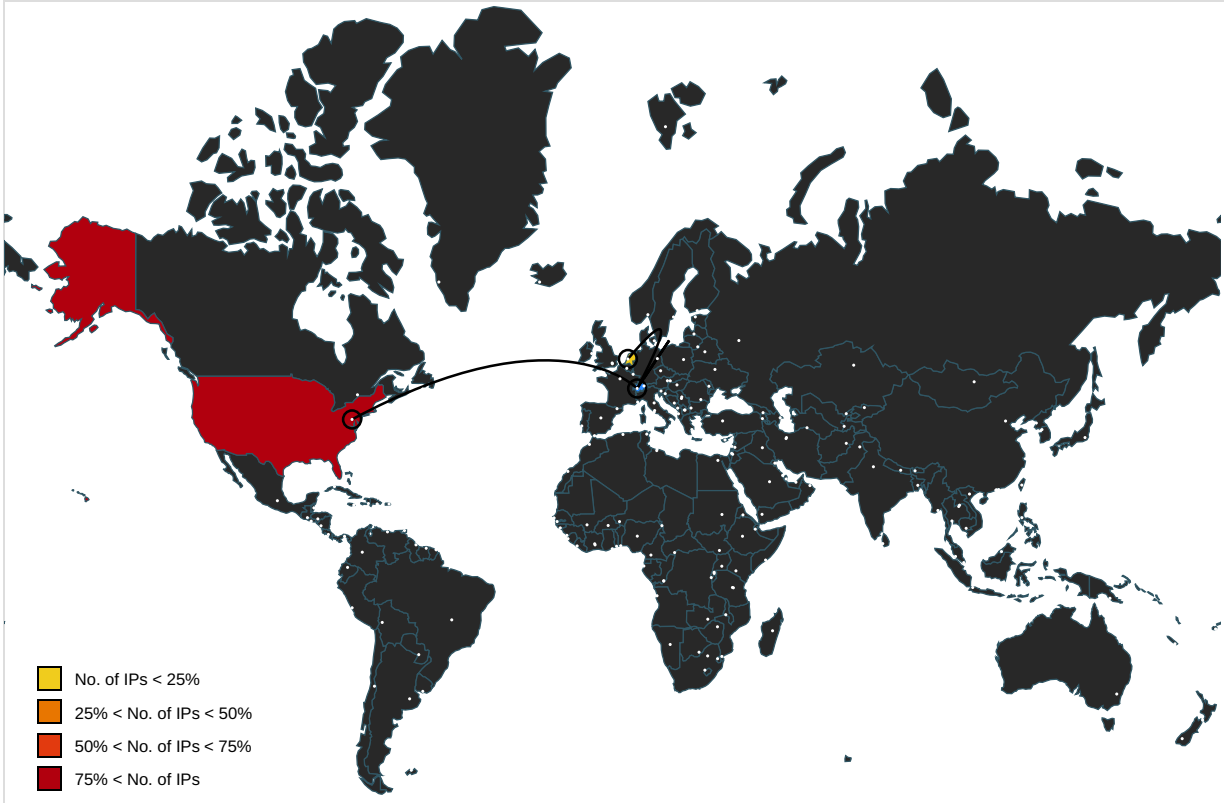
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.187.163	true	false		high
stackpath.bootstrapcdn.com	104.18.11.207	true	false		high
embed.tawk.to	172.67.38.66	true	false		high
d26p066pn2w0s0.cloudfront.net	13.224.189.91	true	false		high
accounts.google.com	172.217.16.205	true	false		high
cdnjs.cloudflare.com	104.17.24.14	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
www.applicationsecurity.ninja	192.34.58.29	true	false		unknown
clients.l.google.com	142.250.181.238	true	false		high
us-east-1.route-1.000webhost.awex.io	145.14.144.140	true	false	• 1%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
www.somewhere.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
deflation-community.000webhostapp.com	unknown	unknown	false		high
logo.clearbit.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.somewhere.com/	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
file:///C:/Users/alfredo/Desktop/test@somewhere.com.html	true		low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.150.137	unknown	United States		13335	CLOUDFLARENETUS	false
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.187.163	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
172.217.16.205	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.185.202	unknown	United States		15169	GOOGLEUS	false
104.18.11.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
69.16.175.42	unknown	United States		20446	HIGHWINDS3US	false
142.250.185.170	unknown	United States		15169	GOOGLEUS	false
142.250.181.238	clients.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.163	unknown	United States		15169	GOOGLEUS	false
13.224.189.91	d26p066pn2w0s0.cloudfront.net	United States		16509	AMAZON-02US	false
145.14.144.140	us-east-1.route-1.000webhost.awex.io	Netherlands		204915	AWEXUS	false
104.18.23.52	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.38.66	embed.tawk.to	United States		13335	CLOUDFLARENETUS	false
192.34.58.29	www.applicationsecurity.ninja	United States		14061	DIGITALOCEAN-ASNUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655631
Start date and time: 01/07/202211:27:46	2022-07-01 11:27:46 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	test@somewhere.com.html
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Number of analysed new started processes analysed:	8
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:	mal56.phis.winHTML@22/75@12/89
Cookbook Comments:	• Found application associated with file extension: .html • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): CompPkgSrv.exe, SIHClient.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 69.16.175.42, 69.16.175.10, 142.250.185.202, 104.18.23.52, 104.18.22.52, 142.250.185.170, 142.250.185.163, 34.104.35.123, 172.67.150.137, 104.21.30.41
- Excluded domains from analysis (whitelisted): login.live.com, slscr.update.microsoft.com, nexusrules.officeapps.live.com
- Not all processes where analyzed, report is missing behavior information

Created / dropped Files

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\0f78a17b-9996-400f-b421-0a7a1f967db2.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):	112061
Entropy (8bit):	6.032837857038768
Encrypted:	false
SSDEEP:	
MD5:	AF552FA4C0D0B8DD97833568437DD6C5
SHA1:	10E00BB6BFC21230A50AFBD0E3BCD47E20CCD523
SHA-256:	2E8B70C70D80CE352041FE45F35FF0AD752575ED9EC7C43C19996B6C874B694A
SHA-512:	3218F40F0229DFB18371BD81D2B3306F2C5F6CC66994A741A4A9654E0D895610628484E27CD12BF922C0F89B339A50B5A85B22617D9F8C864724397C8C93FF5C
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":1.656700107519781e+12,"network":1.656667708e+12,"ticks":174420361.0,"uncertainty":3725115.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"policy":{"last_statistics_update":"13301173704098823"},"profile":{"info_cache":{"Default":{"active_time":1656700105.909056,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\414ccee9-2cf0-45c1-bb36-d9c83977e708.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):	112070
Entropy (8bit):	6.033096239770172
Encrypted:	false
SSDEEP:	
MD5:	B0DBF85319A196DE91E50FD498534A9E
SHA1:	681BE3C481B53532D5375401FBEC0F2683CD9948
SHA-256:	D2BA9A8F25F4C6136CCA81D244BB9562D76A0131BC10B8DEF43D144CA3AE970F
SHA-512:	3EA8A414F287E28139B7C16AEE27DD7DFD85DE86DD83BEE3940BA9B9249E783F65A43BB4AF83BFEC1D55F9FE7E2460F73443E8BBD70A058625649578688144EC
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":1.656700107519781e+12,"network":1.656667708e+12,"ticks":174420361.0,"uncertainty":3725115.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"policy":{"last_statistics_update":"13301173704098823"},"profile":{"info_cache":{"Default":{"active_time":1656700105.909056,"avatar_icon":"chrom

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\1f1fe6c4-ff10-4a04-9b2a-80167bf3ee2d.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:	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...I..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\383315f1-4424-4c10-a80f-51361525d0b1.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):	4.939383392492717
Encrypted:	false
SSDEEP:	
MD5:	4A588EEF775A8467DE20E103B9A0F57E
SHA1:	917BFDD34CC4FA573A44116BD6165496CEC51410
SHA-256:	7FC3A1B66CC3994ED82FC1974CCC854881FE15CF1F0B73A7C5B89D43513A2256
SHA-512:	B9AB487F855BEBAC2374F869C7480DDC8B60B86CB210B595DCB1413CCCA0B8D5EBAAA3FF6EAD0CA6F1D815B202949A68F3643CDA3532510E4269BC8741FB2 052
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301173706173642","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_remov ed":true},"browser":{"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_righ t":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"this_week_number":2739},"default_apps_install_state":2,"domain_diversity":{"last_rep orting_timestamp":"13301173706165479"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"prod uct_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"35053183-b9c4-467c-92ed-c23c3b24472e"}},"intl":{"selected_lang uages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"CBF6F10023A999BB9DF DAAFC4356181F","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\398277b2-f9b9-4d0b-92cc-7f0287f61020.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):	16496
Entropy (8bit):	5.570045494726161
Encrypted:	false
SSDEEP:	
MD5:	DB7314A1F592B03FBD75A04CA6DC3096
SHA1:	E1F495EB07B089F87BA6D180AAE52724804AACBA
SHA-256:	55482995FBC9CA25595AA91C8F74D7C70CA7B035A854F52377753DB2AF1F1DB7
SHA-512:	5E6F28295F0D5B7764D2788C2BD7553E3CD75D6DA0052D23B02F1C45E701B074C85609DFC37B0F9339AEED68D6E13970FC7270DF41F37485743B4E4F18795FA
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":"13301173704685537","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\4580db1d-2ccd-48d9-a039-e424fbc2f45f.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):	4.944925811414315
Encrypted:	false
SSDEEP:	
MD5:	4AFA1A3CA6726DE25EFD37AF194E0751
SHA1:	0FE7317DD807A3CFB73840A25434F1A09581F1A8
SHA-256:	8951176CAD123DB4398EB21550B526011276FA36E51058D83E83FA77AED19498
SHA-512:	895CD70C0B0767C2C43BB5DB410A8F54294216FA547C62377A3FFBB553A845B4283550DE9B1D5B102B018534F90D94EC1B559CAE48615694B250146B64038F32
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\5d90d01d-bc05-40cc-b33f-a6838389ba07.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):	2935
Entropy (8bit):	4.962622307509093
Encrypted:	false
SSDEEP:	
MD5:	31FE409728477E74DF6C8B98B0A1DDA6
SHA1:	D7FB1794D429C1840E5FF66C97018E4FD9F9221D
SHA-256:	8B8656134AB6387596B9431DBC7F737CF1DA0FD32FFEFA3C1987819991B1B53D
SHA-512:	5C9180206E15D98A2A3DB8FF1072AF57C080B2AF74298A2EFF8C030E950F81D06F18FA02846BAA6CE950A05E04EB0BCB4FB2175EAF1B84A57426E744FAB9823B
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://update.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13301260108459472","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://maxcdn.bootstrapcdn.com"},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13303765708459726","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"1

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\7a0d8a11-0cce-469c-b939-58201d6e6967.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):	4093
Entropy (8bit):	4.988496858499349
Encrypted:	false
SSDEEP:	
MD5:	9E74F359F8F0C58C529992ABAF3C5527
SHA1:	4D9F0D9BA2D9D770E92BBB225B34D44D555E8306
SHA-256:	DDA6F506CCCC1F1B176F509D716D1ABA81159227A91648C56629F3F4C30A98A0
SHA-512:	47FD0B3F79E263730CD6BAD955DB98EB87D759DDF75D2051CB0D3EE845A1064240BC7E7CBEBB0B7A3C30F8354D4BD2AF4465ACDD0F645A3BF3A8BF159F138E64

Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301173706173642","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":2739,"this_week_services_downstream_foreground_kb":{"115188287":57,"21145003":243,"35565745":2,"5151071":2}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13301173706165479"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1656700108.825847,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm":{"product_category_for_subtypes":"com.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\8aa0e452-8ccd-4ec0-b7a9-35a13d916e4e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.060012149061901
Encrypted:	false
SSDEEP:	
MD5:	661760F65468E15DD28C1FD21FB55E6D
SHA1:	207638003735C9B113B1F47BB043CDCDBF4B0B5F
SHA-256:	0A5F22651F8FE6179E924A10A444B7C394C56E1ED6015D3FC336198252984C0E
SHA-512:	6454C5F69A2D7D7F0DF4F066F539561C365BB6B14C466F282A99BF1116B72D757BEF0BF03A0E0C68A7538A02A993FC070C52133CA2162C8496017053194F441C
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[],"version":2}

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	3.7077029244153246
Encrypted:	false
SSDEEP:	
MD5:	63A7722CA87718A11E40C69E5642DB4D
SHA1:	2F78B84638D5713EA71F265465737BB1F2267327
SHA-256:	1901EC5AF6A59EE40A922EF4E3D5EE2C0A941331091C157D446B75B867BADC43
SHA-512:	8982AC17E4EA334BFF109ED9F64252DFB1E735664BC10357CD6B342C4CB05DEDEC19E0FEA3CD5B6310BC0288A091D052D965189C69D78A6177103184F1E416I 0
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1140
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	
MD5:	914FD8DC5F9A741C6947E1AB12A9D113
SHA1:	6529EFE14E7B0BEA47D78B147243096408CDAAE4
SHA-256:	8BE3C96EE64B5D2768057EA1C4D1A70F40A0041585F3173806E2278E9300960B
SHA-512:	2862BF83C061414EFA2AC035FFC25BA9C4ED523B430FDEEED4974F55D4450A62766C2E799D0ACDB8269210078547048ACAABFD78EDE6AB91133E30F6B5EBFF BD
Malicious:	false
Reputation:	low

Preview:	.f.5...............f.5.......

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.19476130935549
Encrypted:	false
SSDEEP:	
MD5:	BA6252ED401E2FED83363DCE7FF26B07
SHA1:	1AD623A7C59EC97A47A6F08F0347C8435257090F
SHA-256:	E76737CA8EB830C2FDF0D3A5E7E77F956EABB672B58F8FAD37CDD56590C8F994
SHA-512:	812AE03BB8BBF107935ECA6CA7A305EFFBC1DA0B6890E4743D29E1F4F51BDFB4AFD7FD967724EA1F63ED59279FA05F5077109134FC559DFD64E769853E408E A
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:28:26.686 1d9c Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2022/07/01-11:28:26.687 1d9c Recovering log #3.2022/07/01-11:28:26.691 1d9c Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.199124139088918
Encrypted:	false
SSDEEP:	
MD5:	3A15DA4D1D0344028D8C1AF0C99B5737
SHA1:	CB0B82F9847F6EBA6336CDE62C13A4B8D103A0DF
SHA-256:	26DD260D9AE14FBAC462127D2350E73224997302204345FF2460819F968E6273
SHA-512:	08A036BC4FB45E5BF2661A6F3391F2E055FC826188581E0D4F9E2E80A517019E037164CD27C8779EB5D04C30AA29B3FE32B917E0C065E782B1E97CEE6F72377D
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:28:32.966 1e28 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2022/07/01-11:28:32.968 1e28 Recovering log #3.2022/07/01-11:28:32.969 1e28 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	270336
Entropy (8bit):	0.0018094250832613847
Encrypted:	false
SSDEEP:	
MD5:	C056E91E9B893E6B833704CB770DA095
SHA1:	216409B3390EBEE683E1458986F8CA6EF8988B7F
SHA-256:	8F4C14B28C46FE4B17B97136622BCE6F0BBCD38C7C43E89B4CEF47EB0B66E573
SHA-512:	418859A3B11D5C1E41FC7E0270788A32218DD7C6042DEF324E8EB3E591C04C5EAABB34B440D4011831279C3E0AE3661B31445BB6181C0E36998D588A4451D8F
Malicious:	false
Reputation:	low
Preview:	....

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:	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\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.5395342227551243
Encrypted:	false
SSDEEP:	
MD5:	061E825322AD0025EE0CF9C3AEDABD60
SHA1:	C676D0914BA39942F3B9879668752C73DA9EFF62
SHA-256:	2BEA86EBED891E2060DFBE3FDE426D6A168A25215E4F5D9E52AD31B7727C9E7F
SHA-512:	A04D707CD43A2EE96E0FF0E3AA82D54873C13FB25534BEEE44CCC8D437D62E894EAF3D25D3BCB9310F713497C3CAAB9EAF45E2E5A20BF53BF7D3B523BDB0AC8C
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....O}..... ....

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):	1828
Entropy (8bit):	5.742380834791009
Encrypted:	false
SSDEEP:	
MD5:	01305A315DE4763CE518E0B8D11630DF
SHA1:	16838C0583D11913CCFB45C98D3A93B0DE029BEF
SHA-256:	A905EBEC3F44C198B9EA46BF7DFB6B56D192F3A4644E52C2F46CC9983E8FF090
SHA-512:	4607181AF3763B323958CEA47DEC90F17D969A45220C1C7E1A4FF7CA8DDB13BEB6E00EBA91420E6547DD911BD902D1ED163C3FDB295260D4161437DDE732592
Malicious:	false
Reputation:	low
Preview:	....."......chaos..care..com..c..appsec..application..somewhere..and..alfredo..http..www..https..desktop..file..html..identification..mitigation..ninjas..of..security..taking..test..users..vulnerabilities..web..your*.....alfredo.....and.....application.....appsec.....c.....care.....chaos.....com.....desktop.....file.....html.....http.....https.....identification.....mitigation.....ninjas.....of.....security.....somewhere.....taking.....test.....users.....vulnerabilities.....web.....www.....your..2.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....w.....y......

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Login Data For Account	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.7766145155282294
Encrypted:	false
SSDEEP:	
MD5:	5BA75311B1B0D6276E298ECCD12B8B07
SHA1:	AD9ABB15695F177530511DFD188EB8C33B8F7929
SHA-256:	AEB7F25D09A00715C768CB87BA66EE544830347F998CCF218DE5C2072C4AAF3E
SHA-512:	B60C61AA8F0448365E90B8076A04BBCF945A289E4B851648925B53F9340B89C97553B28D63753A91E53AD64D34C19DB294913DB159A934DF9B5AFCBF951E0617
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2935
Entropy (8bit):	4.962622307509093
Encrypted:	false
SSDEEP:	
MD5:	31FE409728477E74DF6C8B98B0A1DDA6
SHA1:	D7FB1794D429C1840E5FF66C97018E4FD9F9221D
SHA-256:	8B8656134AB6387596B9431DBC7F737CF1DA0FD32FFEFA3C1987819991B1B53D
SHA-512:	5C9180206E15D98A2A3DB8FF1072AF57C080B2AF74298A2EFF8C030E950F81D06F18FA02846BAA6CE950A05E04EB0BCB4FB2175EAF1B84A57426E744FAB9823B
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://update.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13301260108459472","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://maxcdn.bootstrapcdn.com"},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13303765708459726","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"1

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):	4093
Entropy (8bit):	4.988496858499349
Encrypted:	false
SSDEEP:	
MD5:	9E74F359F8F0C58C529992ABAF3C5527
SHA1:	4D9F0D9BA2D9D770E92BBB225B34D44D555E8306
SHA-256:	DDA6F506CCCC1F1B176F509D716D1ABA81159227A91648C56629F3F4C30A98A0
SHA-512:	47FD0B3F79E263730CD6BAD955DB98EB87D759DDF75D2051CB0D3EE845A1064240BC7E7CBEBB0B7A3C30F8354D4BD2AF4465ACDD0F645A3BF3A8BF159F138E64
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301173706173642","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":2739,"this_week_services_downstream_foreground_kb":{"115188287":57,"21145003":243,"35565745":2,"5151071":2}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13301173706165479"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1656700108.825847,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm":{"product_category_for_subtypes":"com.

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):	16496
Entropy (8bit):	5.570045494726161
Encrypted:	false
SSDEEP:	
MD5:	DB7314A1F592B03FBD75A04CA6DC3096
SHA1:	E1F495EB07B089F87BA6D180AAE52724804AACBA
SHA-256:	55482995FBC9CA25595AA91C8F74D7C70CA7B035A854F52377753DB2AF1F1DB7
SHA-512:	5E6F28295F0D5B7764D2788C2BD7553E3CD75D6DA0052D23B02F1C45E701B074C85609DFC37B0F9339AEED68D6E13970FC7270DF41F37485743B4E4F18795FA
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":"13301173704685537","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\Sessions\Session_13301173707165807	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5227
Entropy (8bit):	3.1232027599888026
Encrypted:	false
SSDEEP:	
MD5:	CDAA4C19CB46224BF5411D79D9B4BF75
SHA1:	7A5CC8054F34646BE87455C5D9670422F80CFE19
SHA-256:	CA4E3A83467B3940AAB618DE3072E577C6554972A2096FBC0AA30EF7543C0CB9
SHA-512:	18FE085F12CF05ED14248D8A391CE12DF306E30A7B14FF6398F98AC486EC38BA74B586B26D71AE439C4810E4346919A12A6F3910B68AB4403F2BD06227A87630
Malicious:	false
Reputation:	low
Preview:	SNSS..... .....I.....1...,.....$...f844d256_00cf_49ad_8230_592e0100b41c.....L..... .....i..d.....8...file:///C:/Users/alfredo/Desktop/test@somewhere.com.html.....x..... .....W.....W.....0.....H.....@.....x...8...f.i.l.e.:././.C.:./.U.s.e.r.s./.a.l.f.r.e.d.o./.D.e.s.k.t.o.p./.t.e.s.t.@.s.o.m.e .w.h.e.r.e...c.o.m...h.t.m.l.....8.....0.....8..... .....P...$...8.9.a.c.1.1.8.c.-.6.c.1.a.-.4.8.2.1.-.b.5.f.b.-.0.9.1.2.1.9.3.3.a.2.f.5.....P...$...7.3.8.f.3.c.b.8.-.6.a

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Sessions\Tabs_13301173708720801	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9178
Entropy (8bit):	3.1125340019991556
Encrypted:	false
SSDEEP:	
MD5:	6DCC394E18916BE8E40CE342E82B5892
SHA1:	1E649F9F81C024949B4FFB1D2C522A968AB15F0A
SHA-256:	1F3C3F20B1771FB595E500BCFD893A94AF42B7A9CAEEF672F038ADCAED30647F
SHA-512:	A5842C09FDC7CE4EE76D51354D2FADD0B79039C1FCB551CACAF33063DDE3F3025E0DC8627C2324AF642FB0078E76913FA53A801A6FF6E119D44C47DCAC876 09
Malicious:	false
Reputation:	low
Preview:	SNSS.....s.k..'/.M..H.....chrome://welcome/.....W.e.l.c.o.m.e. .t.o. .C.h.r.o.m.e.....x.....p.....l. D.B...m.D.B... .....8.....8.....H.....*.....c.h.r.o.m.e.:././.w.e.l.c.o.m.e./.....o".route".landing".step".landing{.....8..... ..0.....8..... .....chrome://welcome.....P...$...4.a.a.d.f.5.d.b.-.2.6.5.a.-.4.e.9.f.-.a.1.9.b.-.9.f.f.4.d.3. 5.1.1.6.4.b.....P...$...8.5.e.e.d.4.1.b.-.e.5.c.1.-.4.3.5.0.-.8.2.e.e.-.c.1.4.b.f.d.f.4.c.4.a.1.....chrome://welcome/.....'/.....'/.....'/..... .....chrome://welcome/new-user...>...W.e.l.c.o.m.e. .t.o. .C.h.r.o.m.e. .-. .A.d.d. .b.o.o.k.m.a.r.k.s. .t.o. .y

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	352
Entropy (8bit):	5.16545096445371
Encrypted:	false
SSDEEP:	
MD5:	1DAC2625285273E787A93E8E05FB0D5C
SHA1:	DD70E1C92A8A984578257B7A3E76BAA648BA1284
SHA-256:	E00B938F606593838221E98C28551C69BBAD5B56808CA5A0FAA71A0502E2EB80
SHA-512:	8FEB00A7AE194E11CC853D39B9288A8FF5F3E56EC5E767C0B74D5852CBECFC395D470DB1F476C7366E46F0C0AECED5CD5EBAA47B6178200111752A7ED07B6CC7
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:28:24.597 1e54 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2022/07/01-11:28:24.598 1e54 Recovering log #3.2022/07/01-11:28:24.598 1e54 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.2232290623720425
Encrypted:	false
SSDEEP:	
MD5:	772B0961542CEE610795BE06121DB293
SHA1:	8219441ED02C6A08CB508712E1E628B19BC7B32C
SHA-256:	057CCCE6845662B994AC5E1EBFF548A32ED3BFA6BF2C9DDEB055BFCE345F0B19
SHA-512:	B2F665B0B9774F6AA4BC5C185AA950D2B3BC8169860BDC911F52667A460243A39B83D809F92ADE50A2355287D9C6D8DD68EF6C1A75594BAE1D4F5EA2A2702DB
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:28:26.235 1d78 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2022/07/01-11:28:26.237 1d78 Recovering log #3.2022/07/01-11:28:26.238 1d78 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.211706834479237
Encrypted:	false
SSDEEP:	
MD5:	F97E8684FB28683BE2CCA8EDEA881A57
SHA1:	7EAAEF4117340EE8DC779AE3FF4D0B8BE42069CB
SHA-256:	125C4FCF8FEB8AFBD87180EA62AD279DD4A196CA63408850E5BCD2ED1B32B945
SHA-512:	5F20130EEB916554B2540566295CC822D6FE71196F1B7170E70C97EF6EA9E35B91E611FDA7F176583BD0F815B77FC6D4EED46E68978ADAC0EC833073A7C872DD
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:28:24.672 1e54 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2022/07/01-11:28:24.674 1e54 Recovering log #3.2022/07/01-11:28:24.674 1e54 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.060012149061901
Encrypted:	false
SSDEEP:	
MD5:	661760F65468E15DD28C1FD21FB55E6D
SHA1:	207638003735C9B113B1F47BB043CDCDBF4B0B5F
SHA-256:	0A5F22651F8FE6179E924A10A444B7C394C56E1ED6015D3FC336198252984C0E
SHA-512:	6454C5F69A2D7D7F0DF4F066F539561C365BB6B14C466F282A99BF1116B72D757BEF0BF03A0E0C68A7538A02A993FC070C52133CA2162C8496017053194F441C
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[],"version":2}

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Visited Links

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.005582420312713277
Encrypted:	false
SSDEEP:	
MD5:	C002397D5AC6A58DA9DD80762BABA964
SHA1:	66F175F5991287AD144714BD0B2D2AD1E46ADC04
SHA-256:	3FDAB58268702BB59873E6B0A523E4AE6FE3E69611C6DECD1F05CB8542F54D10
SHA-512:	09F9191A0CE6FC12C6E048360AD9024B34AEB5022D4E01A8C6447873A5A5938677B5DF55787E1953D6D186E0E5F1DECD052894FAD7CFECF15F928E53774D785
Malicious:	false
Reputation:	low
Preview:	VLnk.....?.....j....l7..... ....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Web Data

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2402784174422696
Encrypted:	false
SSDEEP:	
MD5:	1FBF00B609BD2DE92671DC5D027AA065
SHA1:	FB42EC4850832D58DCECAF079FB480AE59C1B7B9
SHA-256:	33BF80B80D70C0FBCDC70221BF3E009C591C3D5C50CCC6EB47A3600719B9ED0B
SHA-512:	1DFE2500AD9D7FEF7AEB4CB8E2947BA2BD8B05F6C729F51491BA38B9FB98D0884B1B25340EF1B6769CE26DFAAAFF73C34E9EB49C91ABEB6F4E1B8289D3908A1F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....-.....&.....O}.....)..... ....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\cccec9b9-da4e-4700-a3fa-b754474ae6d3.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):	15765
Entropy (8bit):	5.57345418691476
Encrypted:	false
SSDEEP:	

MD5:	4F9B6FF15DB21D0DDBF975EA20D70B9D
SHA1:	39FAA0688BF4B9B382152BCE11008D0F5AA115BC
SHA-256:	15EEAAD2E952C3FBEB7281B7B3DE82C3746AFEF58E1359AEEDFDBA0B6268253F
SHA-512:	DE84B4D8FD7466257B4A3D98794C5141E3B84F3F2F67AA371554BEDA86D8E6B821535F2432271917045369486 99BDA6E4C2400459777A2A406534D79F1B20BDB
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":"13301173704685537","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\data_reduction_proxy_leveldb\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.488546888865446
Encrypted:	false
SSDEEP:	
MD5:	5C4287ECC73F41787DE65F33A7A576B5
SHA1:	C1CD30B6012E36C8690672EB119512ACE1F68FB1
SHA-256:	E0A41514C74E1C5890FB07FE527CA2E296783261B094755123C35DED07E7976A
SHA-512:	61DDAB614A26B3F3F3A48017703E62AF421DA4CE19C1CD7B32EBF8BA15AC3EF9329143144A15998E8CA5F8503997B5F86078D548F29A2C56D9164985E017F3F7
Malicious:	false
Reputation:	low

Preview:	2022/07/01-11:28:32.463 1b50 Recovering log #5.2022/07/01-11:28:32.751 1b50 Delete type=0 #5.2022/07/01-11:28:32.752 1b50 Delete type=3 #4.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\dda4d149-5076-4fa0-a2c0-abce23289ca1.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):	4.939576898686151
Encrypted:	false
SSDEEP:	
MD5:	854005CD4A92ED8259CAB8EF470A7AEB
SHA1:	DA8C905DC30FE1AFB19FFE714F58E0EF91C029F0
SHA-256:	88EA3F156E4A38E3394ED3C8C90222F5D61D531939AB42AFA88B0F1D69FB930F
SHA-512:	35230CAEA629D998F61F385794C64CFA93C277E4B16AA3AD5E1E0DED7DA3C3946FA5971ECD86E35ABCBD511934CAB4AD1ACC3A244B0BF589DAEB29D4000D1F9F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301173706173642","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":2739},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13301173706165479"},"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":"35053183-b9c4-467c-92ed-c23c3b24472e"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"CBF6F10023A999BB9DFDAAFC4356181F","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\e704e804-c1a7-4116-a9b7-70aa1fc9725b.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\f129bee2-386e-47f6-ba47-14271f33047b.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):	16478
Entropy (8bit):	5.570660764926655
Encrypted:	false
SSDEEP:	
MD5:	28DC1164E1B6C7D30C4F716E2A5C3761
SHA1:	CD0B2E28CE5074B8A44D9A0076A8C6A05C40FBD4
SHA-256:	86C58C6A5E4619B72E47D550D77C9EFB4C95174D38AD9AE3B4D892C5F29EE81E
SHA-512:	23E82590E5035283F3A815EDEAC9602CFAFAF192B5341424EABAA348FFD0195A7FD07672D900A4D10E68181C1983FBAA146D7B1E7C7A7A43E5A0D8440F925A2C
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":"13301173704685537","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\shared_proto_db\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.252682680024658
Encrypted:	false
SSDEEP:	
MD5:	8DDB8ECCEDEA26E9315796657D20FE02
SHA1:	DA6313976F49188D6E9F2456598821F9B45ECA1A
SHA-256:	67626C29664B00DA47B733D97DF4B2ECE697D055B4CFEBF8258F82A90AC25DFE
SHA-512:	6928D9A52E50DB3EB52D5959A046563A6487A0DA12BAE95FA5FFEAAE2B4B9A0B83C31963EDD0B30BB6A099FA96B8EF6CF887678A4DA3AC5CDAC621F301AE627C
Malicious:	false
Reputation:	low
Preview:	.v}.x.....4_IPH_DesktopTabGroupsNewGroup"..IPH_DesktopTabGroupsNewGroup.....4_IPH_LiveCaption...IPH_LiveCaption...f.7.....20_1_1...1..I=.....20_1_1...1V.e.....<C).m.....4_IPH_PasswordsAccountStorage!..IPH_PasswordsAccountStorage.....4_IPH_DesktopTabGroupsNewGroup

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.175385428921088
Encrypted:	false
SSDEEP:	
MD5:	AFBB35F34236B242A690E2C93DA4AE97
SHA1:	794E72251F0F7B09020A7F9A6F3C3E8515836FAC
SHA-256:	ED4662BD70C27C7FEAABE41A8840FD85733CCB92D8F7725EA4B67D940FBF969A
SHA-512:	01D00E11512BC7A00BEDD6A89528C1E43D931AB3E296A7BB788C94C533B4A6C1492190F87C0B16E385381F23638E2199A03C470F8C789F9A83322B1BA5BC6AF
Malicious:	false
Reputation:	low
Preview:	2022/07/01-11:28:33.343 1d20 Reusing MANIFEST C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db/MANIFEST-000001.2022/07/01-11:28:33.345 1d20 Recovering log #3.2022/07/01-11:28:33.345 1d20 Reusing old log C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db/000003.log .

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\GrShaderCache\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0018094250832613847
Encrypted:	false
SSDEEP:	
MD5:	D691E1B7FA0EFE695E77424F3D01ED9F
SHA1:	5013384C7B365AFD4FD81B92FD725EF0CCB89B9B
SHA-256:	D23162AF8B97283DFB3BD83CF31D2B8AD1BB151FE7E0AF46F9DD12C97BDE9686
SHA-512:	25E7DC3BF3D564CE6084B6082F5437572BED6B5AA110B5D0C40B80D470C45350ECCB73B350C9169BFDFF8526209350D003F0CBE1179B845F8F550A8DFA46893
Malicious:	false
Reputation:	low
Preview:	....

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):	112070
Entropy (8bit):	6.033096239770172
Encrypted:	false
SSDEEP:	
MD5:	B0DBF85319A196DE91E50FD498534A9E
SHA1:	681BE3C481B53532D5375401FBEC0F2683CD9948
SHA-256:	D2BA9A8F25F4C6136CCA81D244BB9562D76A0131BC10B8DEF43D144CA3AE970F
SHA-512:	3EA8A414F287E28139B7C16AEE27DD7DFD85DE86DD83BEE3940BA9B9249E783F65A43BB4AF83BFEC1D55F9FE7E2460F73443E8BBD70A058625649578688144EC
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":1.656700107519781e+12,"network":1.656667708e+12,"ticks":174420361.0,"uncertainty":3725115.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"policy":{"last_statistics_update":"13301173704098823"},"profile":{"info_cache":{"Default":{"active_time":1656700105.909056,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

Size (bytes):	270336
Entropy (8bit):	0.0018094250832613847
Encrypted:	false
SSDEEP:	
MD5:	465AFDF525F59768075E2976EDEBBF41
SHA1:	AE4A070CC81B3D248443D1B1BAA44027A88017B1
SHA-256:	B9E5C85DA5F560B0B75649BEE57463C729890B547AF027CA75A091C6F0CD0688
SHA-512:	33D9A4EB86A55F25ED871B182BC3C52A63F486CF2EDA9951533477C1DBBDA053796AB233EBE420AE36C39B96ECC4CE69D93ADC85182B26741AF3D3B5858639 3A
Malicious:	false
Reputation:	low
Preview:	.....

C:\Users\alfredo\AppData\Local\Temp\7669c153-0ea1-45bd-899e-6c92688a2fdc.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:	AD1CD5B804C08C4C25BD6F97153D3371156848A83682DF1829B0B113B60ED0B01D67B5CD737CB414C8B825E12C7E0D6B5F9B338F4AF7FC82BE8AAF4CA8E279 BA
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\e1ca661c-2bca-4dbc-9294-9e5713ad3c2e.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):	249577
Entropy (8bit):	**7.998368705248363**
Encrypted:	**true**
SSDEEP:	
MD5:	1BC19ADD6624A17181030E661D883F78
SHA1:	5A4FFBCAEA16813EB260B8C15117C04274E044EB
SHA-256:	94AC703B5444114EE6E8B254A420350B4AFBD117831A9F7E6124E23F54317E63
SHA-512:	A2819B460C164AD5E987B97EE93D0891123E8DAB420B51CC0F4349E20C09A9377BD012842631DD1CEAC3C6E85697C3E1CBA3E7660250EEDEF9F22B1DCD60C F2
Malicious:	false
Reputation:	low
Preview:	.....<kw.6...+..HF.,eo....:N.n.g.h.*:.-B.....$(.Nv.i-....g0..o..Q.H~.RAt...X.$_..7~)r.<.....)....`S..@.X....._..bA.....R.T.+....X..%6r..B^...1,.....G.M.P\..#*.....l.BJ.M.. 2`.....B.}....G.s-.M..gh.R..I.mV2.{=.;L...<F*N..(K&q....W.....,b.dj#.. ....gv..6.....oajq1\.y.sv..../....lX....pc..l>.Le ..S'b]"....6&.&...]M.L...,.....|...._.k6ep..HU.W...JT..^.t... .db.Y....n&..W.U.....,_.g(..&.....AXL$.Cq..2.W..^~!.....q.n..V.).K.C.*..~./c8z.!v<2H<..4..`].+.^k..NE.'.-8.\.....<. -g.!..=...i8.r`..e...J../.4*.$,E.5..S..8...j.q.[.9.$...9\...< ....O.z.....F.K.+....Y.<....Q.X.U.i..5xS.....Bp.A.....r.zm.....O.N.<}....go..{~...gg/^.}x....1@.H..*a$..v..R.....l:..x.R."NF1..E...A.i...E.X...y".....8..d....P.YEE.NZFy<...?z. %ED;.[jl.f.y.,&.....<$....Ry..T.sV\.U.w)x.....k6.O..$T.....9c...z..}~..*..z...5..s.v[s.7....l...?...Z...n...9..S..\c 7lfX.....di..FA..._r<3.%..'..Q}..H.ZL).vo8.O...

C:\Users\alfredo\AppData\Local\Temp\e20301b0-2c8c-4b36-970c-0d674f002fb7.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..l..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....l....).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir2452_179984024\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_dir2452_179984024\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:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CBB4
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_dir2452_179984024\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:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488 CB
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir2452_179984024\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:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir2452_179984024\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:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80 552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir2452_179984024\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_dir2452_179984024\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_dir2452_179984024\CRX_INSTALL_locales\es\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir2452_179984024\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	510
Entropy (8bit):	4.719977015734499
Encrypted:	false
SSDEEP:	
MD5:	1FD5DAF46C4D7C4F571C263EC37B943B
SHA1:	A57EE5EF6861F88005C2230EA3D633A1B4CA105A
SHA-256:	BCC2CF06F66E9E3BB4B7887D0EE0AE4A72A6C49F4B2A578A7733B78208984417

SHA-512:	79C3104F1DC51B17B062803209029C8165DBD391FBE0B69BB406D7B4F92FE1898CAC30E20C2E5CFB65D643B978095626C68EAA0CFCA064354D52D52D16BF21A9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Esta aplicaci\u00f3n no est\u00e1 disponible en este momento."},"craw_connect_to_network":{"message":"Con\u00e9ctate a una red."},"app_name":{"message":"Sistema de pagos de Chrome Web Store"},"app_description":{"message":"Sistema de pagos de Chrome Web Store"},"iap_unavailable":{"message":"En este momento, Pagos En-Apps no est\u00e1 disponible."},"please_sign_in":{"message":"Accede a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir2452_179984024\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:	9AEAFC3ECE295678242D81D71804E370900A6D4C6A618C5A81CACD869B84346FEAC92189E01718A7BB5C8226E9BE88B063D2ECE7CB0C84F17BB1AF3C5B1A3C4
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfbG9jYWxlcy9iZy9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiZHUtdGRPdUNWcmxDY254Q0poRkg2NXpLU05vb1RiUE56bDNHbzdRMGJ3SSJ9LHsicGF0aCI6Il9sb2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJ6ZGtWaF9XdkxJWlhkck5xWHBvSHNRMGh1ZGtSM2d1QlMzb2VsTEZLNklVIn0seyJwYXRoIjoiX2xvY2FsZXMvY3MvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6Ik9nUkNHFfaEhvTTQxNzNMelJyYkVpUVdsRXNRSzhscFkifSx7InBhdGgiOiJfbG9jYWxlcy9kYS9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiN2JVWW1LYkhQUUNRMXBGcmUzTHJySEhwWk9xN1c2Zk5hT0laWmdKUERTTSJ9LHsicGF0aCI6Il9sb2NhbGVzL2RlL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJOV3FkU3Rfc1NFMm9KT2VuSUZtM0pMRm9iOGtBZ3ZTa3RtZGpCRGJWazdBIn0seyJwYXRoIjoiX2xvY2FsZXMvZWwvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6ImgyaEZ0YUJoLXJQUEtoUm00QkFWM0VEZmhFbnh5MElGOVhYT3Z0aHhlNjAifSx7InBhdGgiOiJfbG9jYWxlcy9lbi9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoid0pSZDFmM3NxMERFVTJHLXd

C:\Users\alfredo\AppData\Local\Temp\scoped_dir2452_179984024\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:	A5F2B1F47502836130D8083F757B7773C1E1CB36B76AD298CC29AB2B428C8002D2F15BD839838FC326DAC3681C2F48AB25A3E7631D33726C4B25E8EC14170912
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a.....IDATx..yp.....gF#.:,[H.l.l..8...`/.k....,!a7Km...E...Te..T.....J...p....%.(....+...3....eY.e...L.o...5....h4...\....{?....~.u.`0.....`0.....`0.....`.Y.....[(.....).4....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.l".L~mhh.R.@).FFF~.L&...~.B.....u.....}.....~.....f..yUU.....^M...6.....].,w.e..~.!$.C.R.....E(%e9.,....k..@...W8.....@.....O..@%.~..@.S..P.....`Tp...."...?ME..c.....s...`..S1...7.b..aNE..k...3.yP.}.Ch.}.....B.....IPE..C.<....T....k.....Z..o_.....g.....P..A=y.J.)h..@.q.-.*].AU.4...F.M.....y%B]+ .\.~..9.....:..=...r.....E].o...F..P.....i...|....

C:\Users\alfredo\AppData\Local\Temp\scoped_dir2452_179984024\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$.y^.....y*...\..Z..t6..oRj.@&.u..G.qN).t.-V*.>(.N .Ep]wFk.60o.]0.`Y..cT..Y.Tb.`DF.d..s.Z..E..9.4._C..._...%..*.^....4.I...Y..X..R..../...Wj+w0[.]..._B.k.${.\.>.%.....lz .w.ALxo.2;..a...".p..S..&..uXS...<..6..[..zD.._.N+w.WbM7y e6X<..'(,=.r}.....$f..5..P....k..."..8.s.<zgSm@.....).Y.....:e..\|.....F...I..A$.....T?.....m....8.....N...z.....V..vd.h'....C.?.....H.;]..C.M.....9.b.....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir2452_179984024\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_dir2452_179984024\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

General

File type:	HTML document, ISO-8859 text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.4407530316650954
TrID:	
File name:	test@somewhere.com.html
File size:	431900
MD5:	2d475c74396d3a17455856e03750e639
SHA1:	8be111091be27e9caa1902c9aa38e6469985dcaf
SHA256:	1dffbbe9eb7c804144f3fd8744cee452450d7c6bbf0209f258e7507c08d2ef6b
SHA512:	2ca0c26d4725293dc3e2d2831bdaa52e3076a053e997eeb5e5972e6eb321a1890a449a369b9e37eae81866ae62d90451bb892b57d8ccd7dd5de28a9013d13b3d
SSDEEP:	1536:6LFKC9Bu59svDU7jDqlvlx3oc1pT9bfx+Bx2pX1fTuhHv8u4PlwCgYT13K313t31:OuhHv8u4PlwCr1y1d8K
TLSH:	DF94A23C6302CC4DAD776A7FFCA46B115018AF57EDCAB7C8086D80972AE09BA35147D6
File Content Preview:	<script language="javascript">.. ..// == Begin Free HTML Source Code Obfuscation Protection from https://snapbuilder.com == //..document.write(unescape('%3C%21%64%6F%63%74%79%70%65%20%68%74%6D%6C%3E%0A%3C%68%74%6D%6C%20%6C%61%6E%67%3D%22%65%6E%22%3E%0A

File Icon

Icon Hash:	e8d6a08c8882c461