ID: 655307
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 22:11:03
Date: 30/06/2022
Version: 35.0.0 Citrine

Table of Contents

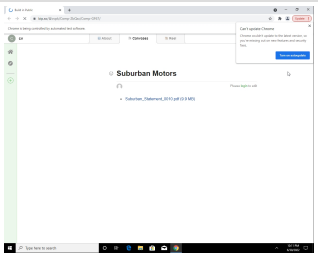
Windows Analysis Report

https://bip.so/@cvpk/Comp-ZbQsc/Comp-GF67/

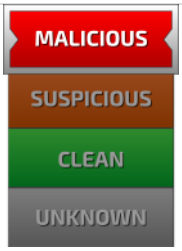
Overview

General Information

Sample URL:	https://bip.so/@cvpk/Comp-ZbQsc/Comp-GF67/
Analysis ID:	655307



Detection



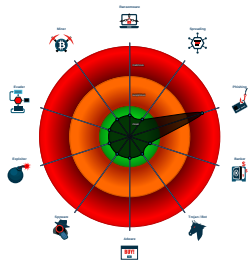
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- Invalid 'forgot password' link found
- HTML body contains low number of …
- Found iframes
- No HTML title found

Classification



Process Tree

- **System is start**
- chrome.exe (PID: 5180 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation --single-argument https://bip.so/@cvpk/Comp-ZbQsc/Comp-GF67/ MD5: 74859601FB4BEEA84B40D874CCB56CAB)
  - chrome.exe (PID: 7692 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1720,6791933579505511980,15657868459491720046,131072 --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
83811.3.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

Phishing site detected (based on image similarity)

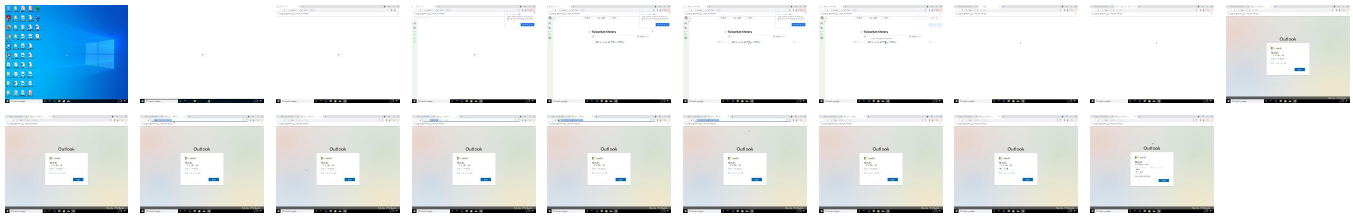
Mitre Att&ck Matrix

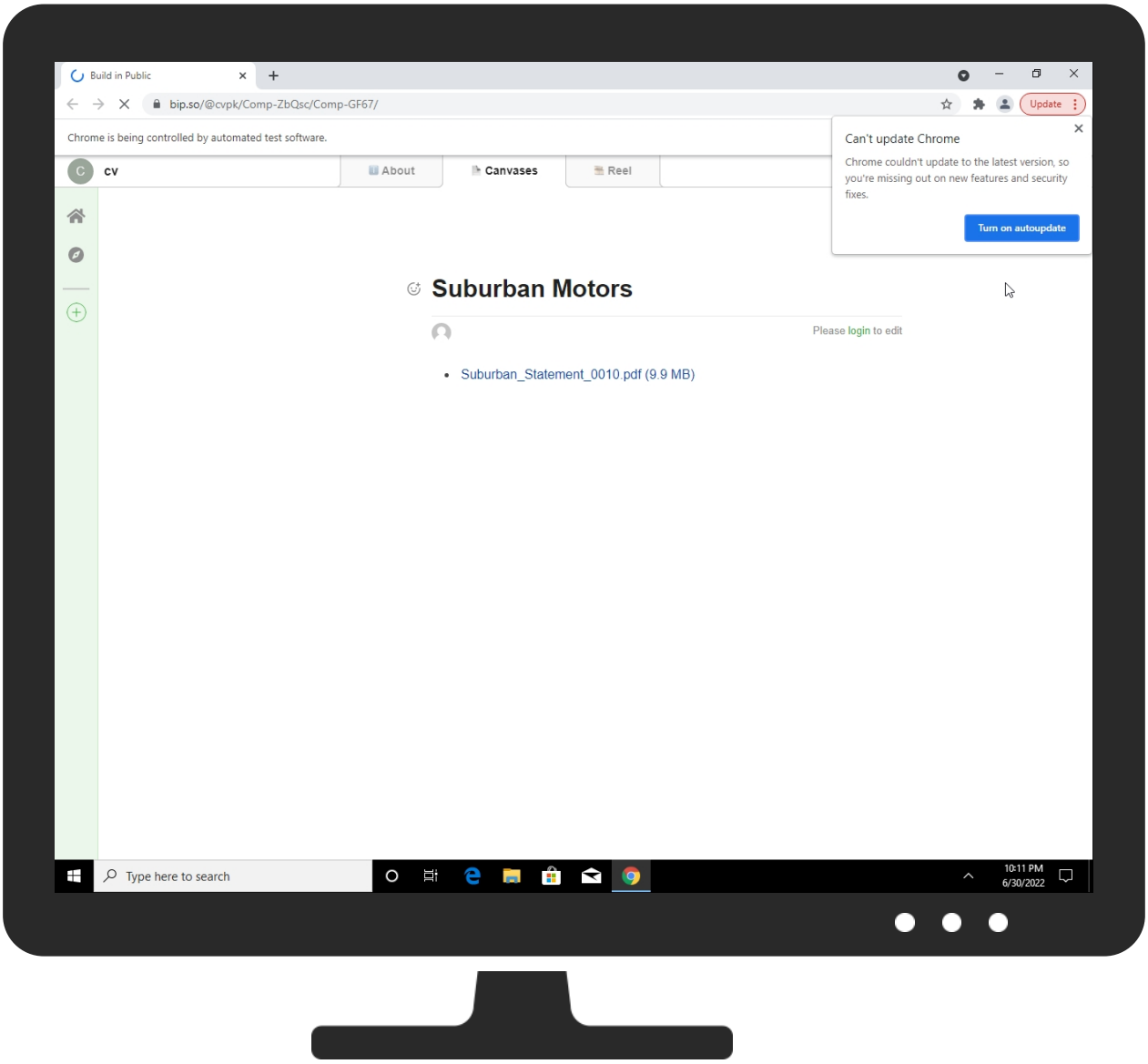
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Drive-by Compromise	Windows Management Instrumentation	Path Interception	1 Process Injection	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 Extra Window Memory Injection	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

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://bip.so/@cvpk/Comp-ZbQsc/Comp-GF67/	0%	Virustotal		Browse
https://bip.so/@cvpk/Comp-ZbQsc/Comp-GF67/	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\alfredo\AppData\Local\Temp\5180_1043184760_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\alfredo\AppData\Local\Temp\5180_1043184760_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.usetiful.com	0%	Virustotal		Browse
dualstack.osff.map.fastly.net	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.186.35	true	false		high
d1uyo0yzpsnvfq.cloudfront.net	18.66.92.15	true	false		high
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
dryesimgurel.com	5.9.161.82	true	false		unknown
bip-backend-prod-1840525834.eu-west-1.elb.amazonaws.com	34.243.225.21	true	false		high
edge-eu.customer.io	34.120.129.162	true	false		high
d296je7bbdd650.cloudfront.net	18.66.115.169	true	false		high
www.usetiful.com	23.88.55.245	true	false	• 0%, Virustotal, Browse	unknown
script.hotjar.com	108.157.4.45	true	false		high
cdnjs.cloudflare.com	104.17.24.14	true	false		high
bip.so	76.76.21.21	true	false		unknown
api.segment.io	35.161.125.23	true	false		high
www.google.com	142.250.186.68	true	false		high
dualstack.osff.map.fastly.net	151.101.2.217	true	false	• 0%, Virustotal, Browse	unknown
static-cdn.hotjar.com	18.66.97.49	true	false		high
client.relay.crisp.chat	134.209.238.18	true	false		high
accounts.google.com	142.250.185.109	true	false		high
www-googletagmanager.l.google.com	142.250.185.136	true	false		high
d1aadi0iayibtc.cloudfront.net	18.64.103.109	true	false		high
client.crisp.chat	104.18.29.91	true	false		high
o301059.ingest.sentry.io	34.120.195.249	true	false		high
vars.hotjar.com	108.157.4.122	true	false		high
in-live.live.eks.hotjar.com	54.74.116.255	true	false		high
clients.l.google.com	142.250.186.110	true	false		high
unpkg.com	104.16.123.175	true	false		high
api.bip.so	unknown	unknown	false		unknown
in.hotjar.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
cdn.segment.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
assets.customer.io	unknown	unknown	false		high
track-eu.customer.io	unknown	unknown	false		high
vjs.zencdn.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://vars.hotjar.com/box-63c3a81830bf549dafe40b369003f751.html	false		high
https://bip.so/@cvpk/Comp-ZbQsc/Comp-GF67/	true		unknown
https://dryesimgurel.com/surburban/	true		unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.109	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.186.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.16.138	unknown	United States		15169	GOOGLEUS	false
5.9.161.82	dryesimgurel.com	Germany		24940	HETZNER-ASDE	false
216.239.32.36	unknown	United States		15169	GOOGLEUS	false
104.16.123.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false
34.243.225.21	bip-backend-prod-1840525834.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
18.66.115.169	d296je7bbdd650.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
172.217.23.99	unknown	United States		15169	GOOGLEUS	false
34.120.129.162	edge-eu.customer.io	United States		15169	GOOGLEUS	false
104.18.29.91	client.crisp.chat	United States		13335	CLOUDFLARENETUS	false
23.88.55.245	www.usetiful.com	United States		18978	ENZUINC-US	false
142.250.186.110	clients.l.google.com	United States		15169	GOOGLEUS	false
108.157.4.122	vars.hotjar.com	United States		16509	AMAZON-02US	false
76.76.21.21	bip.so	United States		16509	AMAZON-02US	false
216.58.212.170	unknown	United States		15169	GOOGLEUS	false
142.250.186.35	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
18.66.97.49	static-cdn.hotjar.com	United States		3	MIT-GATEWAYSUS	false
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
134.209.238.18	client.relay.crisp.chat	United States		14061	DIGITALOCEAN-ASNUS	false
172.217.18.3	unknown	United States		15169	GOOGLEUS	false
142.250.185.136	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
35.161.125.23	api.segment.io	United States		16509	AMAZON-02US	false
69.16.175.42	unknown	United States		20446	HIGHWINDS3US	false
142.250.181.227	unknown	United States		15169	GOOGLEUS	false
151.101.2.217	dualstack.osff.map.fastly.net	United States		54113	FASTLYUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
108.157.4.45	script.hotjar.com	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.64.103.109	d1aadi0iayibtc.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
54.74.116.255	in-live.live.eks.hotjar.com	United States		16509	AMAZON-02US	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
34.120.195.249	o301059.ingest.sentry.io	United States		15169	GOOGLEUS	false
18.66.92.15	d1uyo0yzpsnvfq.cloudfront.net	United States		3	MIT-GATEWAYSUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655307
Start date and time: 30/06/202222:11:03	2022-06-30 22:11:03 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://bip.so/@cvpk/Comp-ZbQsc/Comp-GF67/
Number of analysed new started processes analysed:	14
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:	mal60.phis.win@28/107@28/329
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): CompPkgSrv.exe, SIHClient.exe, svchost.exe
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.23.99, 216.58.212.170, 34.104.35.123, 216.239.32.36, 216.239.34.36
- Excluded domains from analysis (whitelisted): login.live.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: https://bip.so/@cvpk/Comp-ZbQsc/Comp-GF67/

Created / dropped Files

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\027f08cf-fe13-4c7c-bc9d-8b5e42040703.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94804
Entropy (8bit):	3.7615897026399385
Encrypted:	false
SSDEEP:	

MD5:	9E1E9123196835C9AC630B6C1701586B
SHA1:	D3D693964392200CCCA837FA43F055CD7279B064
SHA-256:	2E64802A39F1840E6676DB63C8AE8D91E8220FC79712968F6D873F2CE22C1A54
SHA-512:	A20B879D4AE7AC9A641DE490552ADFE4298228B96B30B3BFB925E417CF4AC05D56AC2755B7AFC6D4478B5E4B964AFD901434CE87F720CF9D40FD1715C83AAC 49
Malicious:	false
Reputation:	low
Preview:	Pr.....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\2b09ffc9-d88e-4738-97c0-4d6ebec3c4ab.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):	112236
Entropy (8bit):	6.033273492224798
Encrypted:	false
SSDEEP:	
MD5:	7EC91D5487C4D5B470B65F21A26103EF
SHA1:	D246B9D7C00669ECD74554AAE77B4F874EFA2999
SHA-256:	7496D08AE599F07E6AD65EDB212CB9FDA14AB10CBF51BAFC18E4CB96611BD4D4
SHA-512:	E9B02A99EE5BAE0DAE514A29D7F642BEB6802D63C5D6E2E415B98351868880D0B2ADD78E5352DCFEF0C2A48DAC37C2C589E1BE4C701C52C454DBF0313FE0D F30
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":1.656652302596479e+12,"network":1.656619903e+12,"ticks":172510959.0,"uncertainty":3040608.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrda cpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtO EILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"policy":{"las t_statistics_update":"13301125899924943"},"profile":{"info_cache":{"Default":{"active_time":1656652301.310572,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\4030d090-51c1-4db1-86d7-e01b1434c9da.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):	116725
Entropy (8bit):	6.062284960076093
Encrypted:	false
SSDEEP:	
MD5:	4D241DD2197E708A30B5D11362519F4D
SHA1:	046DE053F97326F67C73980E020824A90161CE4D
SHA-256:	2B7E0093E611F81B17C07608ED8AA0AB82557BBB4F980BCE848D81854FE31F8A
SHA-512:	3920861D48804F5F0593778908A9398636EE2DB9AE7CDEB82E8E79AC8F1AA48313C4BCD728786BD0EA0B583DD9F6518E753A83E86A3AAB40400D3A4BA7E31C2 7
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":1.656652302596479e+12,"network":1.656619903e+12,"ticks":172510959.0,"uncertainty":3040608.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrda cpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtO EILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_mana ger":{"os_password_blank":true,"os_password_last_changed":"13288110187372457"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\9ef321b6-8107-4bc3-be56-b8dd1b9fb945.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97592
Entropy (8bit):	3.7621270192909058

Encrypted:	false
SSDEEP:	
MD5:	6B0600251DB3DEF8805FA43A308EFFD1
SHA1:	5312323805A8A6A7D1D6AE3C198CE120BAB8A7AF
SHA-256:	86A16D5CAFB6969099AFDCE7257C97099F7C7E894714B7590A674FC66C9F6899
SHA-512:	D63CDB127CADC698DFBD6FF14FF144E65F1732B1DEDFA0B60CA40D141A25F91F16FE0A6D10CC2940E46334BDE126E9B6395370760FD899482B0F6510CA77BCF
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\Crashpad\settings.dat

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	
MD5:	FA7200D6F80CD1757911C45559E59C0E
SHA1:	89C6E99BAEC4EBB3E9A97B928FB473D1498EBA88
SHA-256:	D9779EA4D6DD544A23C2A1C53146B6A4E596927F47DFA0680B0A7EE751D43BB2
SHA-512:	71D9B2DA8EAF404063D918812BA61C3EFB6A23A283B0332180A38C8137FBB21D7977C008D5A57A74469776945CD4ED42C0BCC09F923EDEC52D8F7FE90FA2D14
Malicious:	false
Reputation:	low
Preview:	sdPC.....A.>'..M..,.-.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\0f150be3-f161-4ba7-883b-047502718d0d.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):	5.573164704889125
Encrypted:	false
SSDEEP:	
MD5:	4C7A41E60BE7068343DD9D8E0C3A35CF
SHA1:	A12059E3A2877B75D5E0835521D0AA91F5932A3B
SHA-256:	387B292A6BF67A14EF3FD7A744ADF299F76DF5B04147C580493E3CBA4C9F9178
SHA-512:	E11B92F03201B906F9E4B00C00AD7828D498620A8CFEB3305FFC8D01A955E813351C5B6DF0882F249D1E82D3A2F9B959BECEBF213978775330A8248E0C89826E
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":"13301125900383345","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\1f81ace8-3761-47e1-b6f4-31f5e595b264.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):	4325
Entropy (8bit):	5.012050925990945
Encrypted:	false
SSDEEP:	

MD5:	D8C4EEEFC57C8D6049FDF41DE371162C
SHA1:	EC8EFB55FE6ECA404588C3E4FD2CB8C79CB6DC74
SHA-256:	7426C2A5767FA03978C5DA9388A40EDCA6335653AEFC4D00DAE86282371DDAD7
SHA-512:	188AC938410A6E2DB2BA83D5DF2BB06E54B49640CF055A9F8A28C0E39EDBAF8FDC3D4884FB9E6B24D90BC79CF8DB1F5D22A76E0759862214E77BDBF79457AE A3
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301125901598388","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":2739,"this_wee k_services_downstream_foreground_kb":{"112189210":26,"115188287":57,"21145003":243,"35565745":2,"5151071":2}},"default_apps_install_state":2,"domain_diversity": {"last_reporting_timestamp":"13301125901590566"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"la st_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1656652303.539468,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a .r\",[]]"},"gcm":{"product_category_for_

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\2040be2f-dc72-4bf0-8dda-5f0f0ea089bb.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 5F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\47db3825-4064-4ac5-905b-66b46c48bbf8.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):	4.925556609173254
Encrypted:	false
SSDEEP:	
MD5:	672637309E115619DC7CA34BC2419344
SHA1:	7BEA0F83CF5D5315BBD8037E25E8DEE81B7711B1
SHA-256:	9F6FCEC3126C7C8D260B85AAA571437918EE02048DAA525F18F569545F9A176E
SHA-512:	3765B5FCDF8AD8011587419956C227F294A03DD367583DCDA3DA8A434D923ABF7ED88E580E598F7994610426F39AE54FC153B1385E58775448A1FAB7331177EC
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301125901598388","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":"13301125901590566"},"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":"0453ea49-0247-4331-8ce3-37ea4325dfe3"}},"intl":{"selected_lang uages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"105F3C26B546A8FDF32 76A61E8950678","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\52b3b3b3-acd6-441f-afaa-8d8e65fc5db2.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):	18569
Entropy (8bit):	5.558062931259695
Encrypted:	false
SSDEEP:	
MD5:	9F589472212A4EFA701803E8192D8544

SHA1:	EFB7FDF201598C160BD4003ED98FA40BAFF75E9A
SHA-256:	9163F020A187C1159AEFF4A4B784F208000408D0D0FC525C5E47B3C4AAB5AC7A
SHA-512:	B3527D997F458AD1CB589DE5CA6FE5FB3191DE052F1401D6049263933B375B3D7801944B7EA9791F58C198FB20EB0403CD4D3DBBD9967B6B42F38602BDB64CE5
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":"13301125900383345","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\5508b1ee-c2e8-44a4-bec8-698cff59e383.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.396059376959472
Encrypted:	false
SSDEEP:	
MD5:	7386953D3266B574250440FF96171EBB
SHA1:	84CC9AE534FBDC04CE5A5BDECDC98370FAA32E26
SHA-256:	54981AA8CCD41C1AC6DE38A55B442A0FBC84EC14A4C46C1D5CCCFB3AEB982805
SHA-512:	49E810269344B66AD320B4141ACDB4C0C26CD1DF3B98CC7D26266B2C71340B0035DA1AC0A29595450F129AF1718E30550920AC0FCA10B300FBDE824C5F58FB
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1688188355.706121,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1656652355.706124}],"version":2}

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\623b0677-394d-4ec7-87f9-cdc0df74050c.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\66153d0a-8bbd-4504-9774-6ba0b8b7f6c0.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\8c268923-fc75-4081-8f82-4cfca4226c02.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):	16479
Entropy (8bit):	5.570366480570296
Encrypted:	false
SSDEEP:	
MD5:	786FF56ECEE7F6A62622B37138CEB4B6
SHA1:	D6DF900E46C530DAE984E050767C86A561FEF7B2
SHA-256:	756FE95ADF90F4F6D1D03DB4898D1FB606F7E3693CF4C75E0EE33233DA6A3615
SHA-512:	D29F8D8563C5A643677AAAB83EFDC5E5807DB6106632D03DC0D05995E8D06A13B1F0C9826EDFBD2DCA04624066F15A044FF215246B10B093DD6F3E200CC717B
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":"13301125900383345","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\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11336
Entropy (8bit):	6.0707244876366575
Encrypted:	false
SSDEEP:	
MD5:	2E2110A99AD3AE9721A458C95C64C868
SHA1:	72AE17599EDC0B2DC61C41D946E3E296864F2CBA
SHA-256:	BB46BA705D5F6F43F66B07EA5DA4CC7CC0BF8FE635CCC4EBBA30A5D4A54158DE
SHA-512:	29D95D043F3E529DD33F73B3207A9167D479D9FC404209497B53229CF68AA634CB8A1FE3FD08512FD7F48AFB567144DB873FBBDAD8171D42968B97357F06BC1
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["8D+nOE33nrpuAnTVcJlgMPWVo79reBkp3Z22WTJi5B8="],"block_size":4096,"path":"_locales/nb/messages.json"},{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R

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):	609
Entropy (8bit):	5.136310490201184
Encrypted:	false
SSDEEP:	
MD5:	4063DF879A0B502C89FE163C1BFE81E1
SHA1:	D4C99C6A18AF2425CEE9F21FD62F6B4C3BF6A2B6

SHA-256:	C913E85CF36832F3245B951A681E434BB7DFCC07E747D163CFA74DDD6F4299F6
SHA-512:	53C0A56F2E9B9B9FDC5DA304BD5AB22984BB27F8B8B1FD915187FE471B981C1FCAC3110C84828276EB2BB002BF2A0AD4AC5D920CF9AACA5095318EF9E68AE12F
Malicious:	false
Reputation:	low
Preview:	.....">....bip..build..comp..cvpk..gf67..https..in..public..so..zbqsc*f.....bip.....build.....comp.....cvpk.....gf67.....https.....in.....public.....so.....zbqsc..2.....6.....7.....b.....c.....d.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....q.....s.....t.....u.....v.....z...:\.....Ba...]..... .....**https://bip.so/@cvpk/Comp-ZbQsc/Comp-GF67/2.Build in Public:.....J..... %.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_bip.so_0.indexeddb.leveldb\000001.dbtmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_bip.so_0.indexeddb.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:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_bip.so_0.indexeddb.leveldb\MANIFEST-000001

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23
Entropy (8bit):	4.142914673354254
Encrypted:	false
SSDEEP:	
MD5:	3FD11FF447C1EE23538DC4D9724427A3
SHA1:	1335E6F71CC4E3CF7025233523B4760F8893E9C9
SHA-256:	720A78803B84CBCC8EB204D5CF8EA6EE2F693BE0AB2124DDF2B81455DE02A3ED
SHA-512:	10A3BD3813014EB6F8C2993182E1FA382D745372F8921519E1D25F70D76F08640E84CB8D0B554CCD329A6B4E6DE6872328650FEFA91F98C3C0CFC204899EE824
Malicious:	false
Reputation:	low
Preview:	.....idb_cmp1.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)

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

File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3343
Entropy (8bit):	4.945222848960228
Encrypted:	false
SSDEEP:	
MD5:	CAB8BEABE7E66A4015C98A3C77B3698B
SHA1:	C960AAAEA7014E105290C7D0F09BFCA837C8E8CC
SHA-256:	75431010BFE77818B8BEF4B0C4B328C00668DC6B13C09AAB769EBF58BDA4EDF7
SHA-512:	0D1E94E84294AEA4BF400FF9D0654748BFFEB92D3A1643A6A13B541ADB1BC13EA2F649560A27C8CC3D8AEF9DA5D6B668C7E3BE696091CE882A475B91A9A4CAC8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230891381309","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230891381310","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39697},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230887958662","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230887958664","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":52163},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230886326794","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230886326795","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4325
Entropy (8bit):	5.012050925990945
Encrypted:	false
SSDEEP:	
MD5:	D8C4EEEFC57C8D6049FDF41DE371162C
SHA1:	EC8EFB55FE6ECA404588C3E4FD2CB8C79CB6DC74
SHA-256:	7426C2A5767FA03978C5DA9388A40EDCA6335653AEFC4D00DAE86282371DDAD7
SHA-512:	188AC938410A6E2DB2BA83D5DF2BB06E54B49640CF055A9F8A28C0E39EDBAF8FDC3D4884FB9E6B24D90BC79CF8DB1F5D22A76E0759862214E77BDBF79457AEA3
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301125901598388","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":{"112189210":26,"115188287":57,"21145003":243,"35565745":2,"5151071":2}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13301125901590566"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1656652303.539468,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm":{"product_category_for_

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):	18568
Entropy (8bit):	5.558165916941754
Encrypted:	false
SSDEEP:	
MD5:	6233908FD486B206568C7C1AB3BDFEC2
SHA1:	E5731FF74DA518CDDA4EC2F98710F6C18B2F07B7
SHA-256:	D9C47396DAEB0CCF6350DA14074496B482E0607FF73561A510D1035887901090
SHA-512:	A71035F6A06DC27B71D084FA2A40B3C9492429C96417931FCCC911530ED329A06D702EB1CFA565A30BC1F159E72249F7D8D0D1E3AFD0CF498CC93A045CA95BC
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":"13301125900383345","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\5c42817e-6291-4351-84ba-c639d115aa96.tmp

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

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Reputation:	low
Preview:	....

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

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

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -

Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C23 75B
Malicious:	false
Reputation:	low
Preview:	.|.."....leveldb.BytewiseComparator.....

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):	204
Entropy (8bit):	5.396059376959472
Encrypted:	false
SSDEEP:	
MD5:	7386953D3266B574250440FF96171EBB
SHA1:	84CC9AE534FBDC04CE5A5BDECDC98370FAA32E26
SHA-256:	54981AA8CCD41C1AC6DE38A55B442A0FBC84EC14A4C46C1D5CCCFB3AEB982805
SHA-512:	49E810269344B66AD320B4141ACDB4C0C26CD1DF3B98CC7D26266B2C71340B0035DA1AC0A29595450F129AF1718E30550920AC0FCA10B300FBDE824C5F58FB6
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1688188355.706121,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1656652355.706124}],"version":2}

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\ac88775c-75d1-4550-8ae2-6dc3fa3547e7.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):	4662
Entropy (8bit):	5.044182970534659
Encrypted:	false
SSDEEP:	
MD5:	B25188B8BAFD346BBDE3B578ED8BC64E
SHA1:	3D26BE951F2F94F9410D0428218D3F8BEEFDFAA3
SHA-256:	FFC96E9FF584BA5330C906F3DE02F8B12CB82916CEADE265177CD75371F581E0
SHA-512:	211022B6132D46BC72C5342A78B7209A85B86CF500C84954C22DD58436EB55EC52361041BC991C2C51B170051073F5B5200B047EFD86DFDAB5B608C29F255C5F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301125901598388","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":{"112189210":43,"115188287":57,"21145003":243,"35565745":2,"47815025":2,"49601082":3,"5151071":2,"54845618":29,"88863520":1}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13301125901590566"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1656652303.539468,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data"

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\b3ca980c-a4fe-4cf7-8cec-7007c2002a5c.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):	4.925478117851532
Encrypted:	false
SSDEEP:	

MD5:	DD5F5EF0DFFE032775B8F898637DA11C
SHA1:	6CDED9E1E595133D4A2349E372B2ED40A55F0D7A
SHA-256:	FFF1B4CD5FFEBA130577FCC39A30901AF8AEDB353D20A8EB605E042E6635E009
SHA-512:	3043CE3A5929E9E55D07977C4B7DA797E225E57324E949A28CAD7E3B8660F425AE6391FE41C3EACE80B1475AC9BB21BA380767E683B512243FF1CB72FAC8E7E6
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13301125901598388","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":"13301125901590566"},"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":"0453ea49-0247-4331-8ce3-37ea4325dfe3"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"105F3C26B546A8FDF3276A61E8950678","engagement":{"schema_version":4}},

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\e4d8acdb-3d1f-4a17-9fb4-676ec38e0704.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):	18568
Entropy (8bit):	5.558165916941754
Encrypted:	false
SSDEEP:	
MD5:	6233908FD486B206568C7C1AB3BDFEC2
SHA1:	E5731FF74DA518CDDA4EC2F98710F6C18B2F07B7
SHA-256:	D9C47396DAEB0CCF6350DA14074496B482E0607FF73561A510D1035887901090
SHA-512:	A71035F6A06DC27B71D084FA2A40B3C9492429C96417931FCCC911530ED329A06D702EB1CFA565A30BC1F159E72249F7D8D0D1E3AFD0CF498CC93A045CA95BC
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":"13301125900383345","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):	116725
Entropy (8bit):	6.062284960076093
Encrypted:	false
SSDEEP:	
MD5:	4D241DD2197E708A30B5D11362519F4D
SHA1:	046DE053F97326F67C73980E020824A90161CE4D
SHA-256:	2B7E0093E611F81B17C07608ED8AA0AB82557BBB4F980BCE848D81854FE31F8A
SHA-512:	3920861D48804F5F0593778908A9398636EE2DB9AE7CDEB82E8E79AC8F1AA48313C4BCD728786BD0EA0B583DD9F6518E753A83E86A3AAB40400D3A4BA7E31C27
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":1.656652302596479e+12,"network":1.656619903e+12,"ticks":172510959.0,"uncertainty":3040608.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187372457"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\c9814282-dbaf-4435-b86f-726cb7515d49.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):	112217
Entropy (8bit):	6.0329789520930674
Encrypted:	false
SSDEEP:	
MD5:	C7E00E63C4753CBF7C3D03E4B542B113
SHA1:	4592D8DF6A79325237125FE812DC091BCA1E11B8
SHA-256:	0A3C1C05AE7D77BD3BEC3D557ADA952A6A5E2C66F6BC8CABF0A7B73954D154ED
SHA-512:	9C0DEBBAF89AF9F6DB427F27704706F8F19631C3CD223DC580F5A6FF5E65ED76B8070C5568DD810053DFEF1599D7FE9B080EDC47FB61D2E483D594FE78091C1
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":1.656652302596479e+12,"network":1.656619903e+12,"ticks":172510959.0,"uncertainty":3040608.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"policy":{"last_statistics_update":"13301125899924943"},"profile":{"info_cache":{"Default":{"active_time":1656652301.310572,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\e24447d8-a5ed-4a44-8b37-89121e485b24.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):	116817
Entropy (8bit):	6.062577911715299
Encrypted:	false
SSDEEP:	
MD5:	80CD57B27729049A8A5434AC3DD66D29
SHA1:	EC8087D6ED93105716F75E5720D20FCC445B96D2
SHA-256:	641847AFE55D7C8B3AC769B68B97B9471B5D5BC82A37235DA08A0333B22AC9E1
SHA-512:	B3F738920EF7966C3C3F3597D172CBAE5E5441AE86EF09A148850F49F6D14CD584D91B08A45E59FBA7784CC0C3F0F2D6B837911C03F3EE56BAE70D0DE1E31031
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":1.656652302596479e+12,"network":1.656619903e+12,"ticks":172510959.0,"uncertainty":3040608.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187372457"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\alfredo\AppData\Local\Temp\141e7c95-92aa-47a9-a1a1-e3584951e389.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	28748
Entropy (8bit):	**7.9918576871001425**
Encrypted:	**true**
SSDEEP:	
MD5:	2A37AD0EC191D53104BB46953AC6C43C
SHA1:	FD23FFC5B7E4A6B45FBD88A486D15FAA51DC07AE
SHA-256:	51F075EB69486CB23B32A0776782B4A1B2AF204429AB94510469E02B115E56CC

SHA-512:	AEB91CB7902A800D7B0C43627EC2B52121BC41BA29A1B6ABEDBFCFA4802254A0594ED239EA7A3F8D40241E43D436428D1E4AC117BD97269D78460F82F9BDCF68
Malicious:	false
Reputation:	low
Preview:	.....Zms.6..._..p..[.(.b[...M....N{..t ...S.....v...H.q.g:....]...p..6I8_d...C.\p.X$.2.p.g.8I}8.".D)$<..O...}.J9.3..a.i.'...x.....5O...x.....I.M.!.'\.l.2.0.cN.fq....\.....7..,.....>.p...w&.KS.....(O.V>.....O.r..V~J.`....U(..Y..MIy..w..g0e.....D.,L..y..N.+..._....O.h.]...V....r.....O.|.:....Li..>COy.....N.h.....R....Q%.,Xr.y...G8=.A....!8(..L....c....sA....t.Vl:...v...G;...^.l...#.t.>...k..d..kr...B.....Pb.0*..!..;9.....:~....j;....j.*O..!B.....?....^.]....;...[.g.B...%..'.7;.9.>..gP. p8...:.5l.Y.....Jp..R,.?..b..8O.....h.X(..G.).Cz.C..%....x.ET.....AEi.../..0.. ....k.*t..wl..e...H.i.F.....?.....z...?.....(../.O..R.?.4..7...j ..Q.....l..ob!..A..j...@..!).....K...MW.U.N.....W..Bh'8.'.y....Y.[o...PI..W.*...i...r.e..=.k^.WC..Uy.j..687^.z.#u5.4O.....-j.j3..L.1..F...8.....@I.9.c.aGC.R.&..j.Q-av?...[4.E..T8....u..+9.<.n.Qw.D..N..S..3.D..... .%C.j.7.Y.s(.0wq.ZI.#"#..[K.GJ ....4.....?

C:\Users\alfredo\AppData\Local\Temp\198e4b47-1bf6-4a9b-817c-7d99ee04ef69.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	101891
Entropy (8bit):	**7.9971613680976565**
Encrypted:	**true**
SSDEEP:	
MD5:	173CA02E5B06065771DEB2F28E4E5A9E
SHA1:	20F1774FB280C94C13082A255C27D7A786EFD5C7
SHA-256:	634557AE2916F2FAA0CBF2557F8F96E26845ABE94D2784FD73B169EC5618B186
SHA-512:	D947E3ED56BE1F3C668943E8F066F39650D2E0D76BF64BAD167E100B8B1066B88D8E851346AFBD9777E90445F41C5108A0A2F1514A3F28F02D4EC39978121E71
Malicious:	false
Reputation:	low
Preview:	.....{..0.....&xqH.....zyIBv9....=...+.....I6....3#.l.@..9.s].W7...h4..H...7.^.....Bg.....`.;.S...P.....z.3.....9~.P..{..-.z.....b.:.....>..'....I8.....'v.M'E.?bA...N8.'.8I._...<v&.pT{.L'Ne...#.S!].T.-+...r)5.j.U.8q....X..VPo.....F.o..A.~~.?.w.....eNJ..a)....i....:?._^..v.<=ei...i.....Q...8k.....~j.c.W.....~...Q.yq..^9..z.....S..b.E..L3|.9S.pa...a....5...J.\.2l..s..4.....S.u..o.|.Q.K.0.=.....0....xj.4....Mie..C..3..... .....WN.....4Vs.B..N.bD...VK%...mb...{{....pd..7..G.....}.J;"..4,.....A.R|0d..)..M.....;;.8.h.C.u..pkM..Z@.....r..U....H..,]...l:~p..8`....3....5.*.t../S{.{`.^kB=f.....ZR..L.$t..D%I..xB../.{rb..h8.!.....Z.0.....{PuK%Vv...RR.*.....j.vw.[B..$..|&..eZEW.Z[&..d>.o.....@..t.z.O.12C.....Kk..oS.[.0.M...<.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\22a167a6-7032-4b5c-ad19-ef3b89f6e959.tmp

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

C:\Users\alfredo\AppData\Local\Temp\5180_1043184760_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302

SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A158 40
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.l=....J.$<....f..... .....NaCl....x86-64.....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C .....p.....`....C....C..B..... .....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl- clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\alfredo\AppData\Local\Temp\5180_1043184760_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2776
Entropy (8bit):	3.5335802354066246
Encrypted:	false
SSDEEP:	
MD5:	88C08CD63DE9EA244F70BFC53BBCADF6
SHA1:	8F38A113A66B18BAA02E2C995099CF1145A29DAA
SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....X.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..SP..h..... ..fff.....J.$<[.,$J.l=....J.$<.....f.K.....`.....P.....z.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com /a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c9 4a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\alfredo\AppData\Local\Temp\5180_1043184760_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1 38B
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 94 `.....pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t"..A.D..... .....A.. .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163f dd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC. NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\alfredo\AppData\Local\Temp\5180_1043184760_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	3.21751839673526
Encrypted:	false
SSDEEP:	
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40

SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62CFC
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 30 `....._pnacl_wrapper_start..// 20 `.dummy_shim_entry.o/./0 0 0 0 644 1840 `..ELF.....>.....@.....@.....PH..,$J.l=....J.$<.....f..D.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x..... ....C....C..... .....rela.text..comment..bss..group..note.GNU-stack..rela.eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....

C:\Users\alfredo\AppData\Local\Temp\5180_1043184760_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped
Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....@.8...@.....0.....0.....Y.....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl....x86-64.....GNU.K..J.'..b.....<S...`...`.. ...@...@.....@.....@.....Y@.....p.....@.....?.....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... ...`.. ... .`..... ... ...@...`.....@... Z...[...[...e..... ...@... ...@.. .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\alfredo\AppData\Local\Temp\5180_1606430971\Recovery.crx3

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	145035
Entropy (8bit):	**7.995615725071868**
Encrypted:	**true**
SSDEEP:	
MD5:	EA1C1FFD3EA54D1FB117BFDBB3569C60
SHA1:	10958B0F690AE8F5240E1528B1CCFFFF28A33272
SHA-256:	7C3A6A7D16AC44C3200F572A764BCE7D8FA84B9572DD028B15C59BDCCBC0A77D
SHA-512:	6C30728CAC9EAC53F0B27B7DBE2222DA83225C3B63617D6B271A6CFEDF18E8F0A8DFFA1053E1CBC4C5E16625F4BBC0D03AA306A946C9D72FAA4CEB779F8FCAF
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.....S'.....2.{....'....+.'.."..Y.x.ISa...)....H.&92..?!..~..F.5."...n,.B.-|\.)..(.....]G..j.-M)...C.....o&L..0.K.....UtP.&.N...;..^w/a{}v...~KG;...?.1...k.c..D.U.....J.6.`.G.5.x.k..[...i.A.@I^..I.<A. J...j.'.G.`.$q.N..Tdq]2]p.OF..#.#.....'....8.3.....0.."0...*.H.....0.....O..(...':19..O/.>....=.....m.n\.z..q.....JW..F.....+H.Z+KGO.9....8.....U...&.y....,$...?.Eo.....\f/.Z..+M8...B.3'..Y.r...X.AS?.~..k..n..... Z...&.G....."n.....l.0v.x#<....Lx,-.w..-..d.....J.pT..('e~*{%kQ.Q.....rI.....Z....v.N.....J.d_.....rX.....w@.b.[.c../V.'c...!.~.k..}z...U.S..nC.....@.....Y..#.D.z.....5&.1O...X=p..2.F..P.6yP..>{.....HBX.*.E5....y..

C:\Users\alfredo\AppData\Local\Temp\5180_1606430971_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):	1765
Entropy (8bit):	6.027545161275716
Encrypted:	false
SSDEEP:	
MD5:	45821E6EB1AEC30435949B553DB67807
SHA1:	B3CADEB17FE5B76B5DBB428B8D3A07B341F8B1BC

SHA-256:	E5FAE91295BECF7F66BFA4BE1061CA5537ED763EB5D01485F23ECFB583304FEE
SHA-512:	BCBE40CAFAA4B14566D91E361D8FB7F0288D5C459FA478AA4C575444DA4D406E1076FC0B3A31D4A9E5EE034F0FE15A0EFE8A8A52B838DE94B96D3E488D28F0FE
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJSZWNvdmVyeS5jcngzIiwicm9vdF9oYXNoIjoiaGdCR051SzhNR2NKaDlfNmZQaFdEWmpVYUFKeklzeDlJS21DUEZvb0dfUSJ9LHsicGF0aCI6Im1hbmlmZXN0Lmpzb24iLCJyb290X2hhc2giOilwYXduVFBFQmdDRHkyV05hVVk3Um9mSWN3c3ZwNHFRNUxzZVMxVXRiVXY0In1dLCJmb3JtYXQiOiJ0cmVlaGFzaCIsImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiaWhubGNlbm9jZWhnZGFlZ2RtaGJpZGpobmhkY2hmbW0iLCJpdGVtX3ZlcnNpb24iOiIxLjMuMzYuMTQxIiwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"iFuMX_kOZ-zJ7KVu6Lxb3rHWZgQvkZhv25x_SGlBiDV_okALrGbj6rUOWyNNNsHXMnT118XZmA696XR8qkr4dwT5Gvez-9gi-WYBY7XBkgo7v6NspGgJF89BNCeI-P9k-zBHOGgrf-fCEiAcoM7xCx9_f8qlRy7nhQPyjOIHn5eEJEir0uSu6gdqR9afnVZ3UoR-VOLdOBt7fA4ee38MP2ut5qWU50F5dvIezfKkTVDMHwztvcLCy6R9SVkdSYv6jwWGccYRl-aclvkkHu6SnbZGI7fmDZdkcBAxBHYEZZMmvb76ro4SO15GDyEVAo_Qf4trdrY_GyN_Bm73imCTjgtoGc

C:\Users\alfredo\AppData\Local\Temp\5180_1606430971\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.7900469623255675
Encrypted:	false
SSDEEP:	
MD5:	2AE14F91312C4E8034366B09D49D5B18
SHA1:	AD4933A5D838D0FA0B960C327A5039A9E8249642
SHA-256:	4F122332EF0F2BB490EF59619D3602C1A7277C0A7A19C132202DB4803A09BFA2
SHA-512:	FB0CC467A4B8463F6A3BF42CDC11C23B34EB94A9397644B68714DCB819EE326BAE05022D59D23DC9907DF1E6928064D853FD0900BB6083417892D4D5A9BA771
Malicious:	false
Reputation:	low
Preview:	1.aeedb246d19256a956fedaa89fb62423ae5bd8855a2a1f3189161cf045645a19

C:\Users\alfredo\AppData\Local\Temp\5180_1606430971\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.682333395896383
Encrypted:	false
SSDEEP:	
MD5:	7A8E3A0B6417948DF4D49F3915428D7A
SHA1:	4FC084AABDB13483567D5C417C7ED8FD16726A80
SHA-256:	D1AC274CF1018020F2D9635A518ED1A1F21CC2CBE9E2A4392EC792D54B5B52FE
SHA-512:	064D84A57B28C19AD10742859DA493D0826B47ADC632F6C623DFB4DE36D72A9D29BE98518061A9FFD42D99FCF01F27DE39CE74782B3A5ACBBE11DFDDEEAB59A1
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "ImprovedRecoveryComponentInner",. "version": "1.3.36.141",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\alfredo\AppData\Local\Temp\a038723b-1bac-434a-b43b-a6638b3523ca.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT)
Category:	dropped
Size (bytes):	5168
Entropy (8bit):	7.956694278195136
Encrypted:	false
SSDEEP:	
MD5:	3E5CCD9B583763AF68E28C5101373167
SHA1:	2005CDC0A8070B65E321A197D576698ECC267496
SHA-256:	41412C0863920BA95E9FDBD3AF000CBE926A73C078997A233DF55379A5C4D274
SHA-512:	04BF4F7320326B085C40527797577D8770A30A1ED24A8587A000A5AE1D8F39E0B7F187DB14603295AC7A2901A4698683CC3BED2C2611539293A1927AB31BEAE1
Malicious:	false
Reputation:	low

Preview:	.....[ks.8..._.....#..,.G..8.;.55;.%..&5$e.....)..d._...%.....s.....+..Uv}...]rq.....luK.).zJh..3.&..Uu...W...s.H. .MV..\U3Ef.\.|...TU.9.z)I...u.+.g3U`Zs.6d...JiJ.rU.IV.''.'L\|8 .d..j.J..q.....O.''..<,...n...~\|E.dV.u.O..'"...e.uyJ?..?]~.?.....M.,.7...j.,.fz].. >+o.gz....<^(5.Jg_.Ap.U.i.....?.8.....,.*.*./.iQ..8.....A.DO/....?.~..N.~a.-..g.N~.....o.^...L.mW.]:{..... ./.....[VkTu[wki.gK...;-.<...\.".3]..}V...)9i.V.P="m?.....V.i...7..S.U.d..(..\....g....bU.....}.....P9$.A...N..ckV..Qz..A....7..{pd.f.7....}6on.....7J;...Y..l>W...H.Z.....j..... Wk9vj+V.W.zAm.....P.oYo..\.....}.g.^.p...Z....l%cT|LN3..H.....{...~.J.%.!k.(.)..."....q.%.V.. d..MZ.`.....o..m3....1.../..jeH.....Q....X...j..o..|.o.r..nVw._...9 .....o...l....!...{....xU5.. }.x.I..3.vT%z.k..o.....^.S*.t(....+r\.u<...G.`.....g...r..?...}7.=.....c~.F.e..w.v$sC/.B.p.D~..J...:....7Vl3w...s.-".....]+..KO.~....%.I..?.&.o...\?.9..

C:\Users\alfredo\AppData\Local\Temp\dbdc1e9b-b90e-4f4f-b3ee-5def2d2735b2.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..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t''i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....H''i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1293
Entropy (8bit):	4.132566655778463
Encrypted:	false
SSDEEP:	
MD5:	D7A97183BCBD5FB677AA84D464F0C564
SHA1:	CDBB279B864E2C0A51E0892B8714131802586506
SHA-256:	76EFAD74EB8256B942727C42261147EB9CCA48DA284DB3CDCE5DC6A3B4346F02
SHA-512:	36F0310DD06319E4A51F77E4C3D64F6276891CE6410FE2571324BB71F2FBCDA368EAC4267FF8268086BE6912E41787D0F70771755E3D49E3E8C26648EAC6EFC9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u043e\u043d\u0430\u0441\u0442\u043e\u044f\u0449\u0435\u043c \u043d\u044f\u043c\u0430 \u0434\u043e\u0441\u0442\u044a\u043f \u0434\u043e \u043f\u0440\u0438\u043b\u043e\u0436\u0435\u043d\u0438\u0435\u0442\u043e."},"craw_connect_to_network":{"message":"\u041c\u043e\u043b\u044f, \u0441\u0432\u044a\u0440\u0436\u0435\u0442\u0435 \u0441\u0435 \u0441 \u043c\u0440\u0435\u0436\u0430\u0442\u0430."},"app_name":{"message":"\u041f\u043b\u0430\u0449\u0430\u043d\u0435 \u0432 \u043c\u0435\u0441\u0435\u0446\u0430 \u0441\u0435\u043f\u0442\u0435\u043c\u0432\u0440\u0438 \u043c\u0430\u0439\u043a\u0440\u043e\u0441\u043e\u0444\u0442 Chrome"},"app_description":{"message":"\u041f\u043b\u0430\u0449\u0430\u043d\u0435 \u0432 \u043c\u0430\u0439\u043a\u0440\u043e\u0441\u043e\u0444\u0442 Chrome"},"iap_unavailable":{"message":"\u041f\u043e\u043d\u0430\u0441\u0442\u043e\u044f\u0449\u0435\u043c \u043d\u044f\u043c\u0430 \u0434\u043e \u0441\u0435\u0440\u0432\u044a\u0440\u0430 \u0432\u0433\u0440\u0430\u0434\u0435\u043d\u0430\u0442\u0430 \

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	556
Entropy (8bit):	4.768628082639434
Encrypted:	false
SSDEEP:	
MD5:	58BA5F65ED971591D1F9D81848EE31D0
SHA1:	BDA3C8B74653334FC8F060CAFBCEA58DF0113AB7
SHA-256:	CDD91587F5AF2C865776B36A5E9A07B10D21B9D911DE0B814B7A1E94B14AE885
SHA-512:	BA2A6BAA3011A54E6B07E29DFD133009D66B6CFFF525DEC0024BDE55A9BED463AD130307EE64BFB4A983A11FFD6B44BD53ED38EB144083A2CBEFA8D85C4D5D41
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"Ara mateix aquesta aplicaci\u00f3 no est\u00e0 disponible."},"craw_connect_to_network":{"message":"Connecteu-vos a una xarxa ."},"app_name":{"message":"Sistema de pagaments de Chrome Web Store"},"app_description":{"message":"Sistema de pagaments de Chrome Web Store"},"iap_un available":{"message":"La funci\u00f3 Pagaments a l'aplicaci\u00f3 no est\u00e0 disponible actualment."},"please_sign_in":{"message":"Inicieu la sessi\u00f3 a C hrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	550
Entropy (8bit):	4.905634822460801
Encrypted:	false
SSDEEP:	
MD5:	43161EFFA28A0DBFC67B8F7DBE1B5184
SHA1:	FE0A9235A59B51B7F564F14FF564344927F035B8
SHA-256:	3A04421DF5218E8ABD3B0E2AFE11E8338D7BDCBCD1ADB122416944B102BC9696
SHA-512:	FC6A391A4B37FFEE2182F29C1590E32766A1820DC58D0A70A8DD96D7ABE74B47181B24AFFF8ADAE12686CCB1B898DCDDB882EFD205C3387B5B6F3CFBE6E5E A78
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikace v sou\u010dasn\u00e9 dob\u011b nen\u00ed dostupn\u00e1."},"craw_connect_to_network":{"message":"P\u0159ipojte se pros\u00edm k s\u00edti."},"app_name":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"app_description":{"message":"Platby Internetov\u00e9ho obchodu Chrome"},"iap_unavailable":{"message":"Platby v aplikaci aktu\u00e1ln\u011b nejsou k dispozici."},"please_sign_in":{"message":"P\u0159ihlaste se do Chromu."},"jwt_re trieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	505
Entropy (8bit):	4.795529861403324
Encrypted:	false
SSDEEP:	
MD5:	31264DDBF251A95DE82D0A67FA47DB3A
SHA1:	3A48DC7AF26A153594C7849E1D92AAC31296459B
SHA-256:	EDB51898A6C73D0090D6916B7B72EBAC71E964EABB5BA7CD68E21966024F0D23
SHA-512:	B97D61BD71E3F0A91FF1048D2ACAD4BC092CCAF157B7A96029B6AB5AF1812B01814E3153CD894307CB13DC132523EAC22B19CADA6B97F4B81B0D1132562317 B5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen er ikke tilg\u00e6ngelig i \u00f8jeblikket."},"craw_connect_to_network":{"message":"Opret forbindelse til et netv\u00e e6rk."},"app_name":{"message":"Betalinger i Chrome Webshop"},"app_description":{"message":"Betalinger i Chrome Webshop"},"iap_unavailable":{"message":"Betaling i appen er ikke tilg\u00e6ngelig i \u00f8jeblikket."},"please_sign_in":{"message":"Log ind p\u00e5 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	516
Entropy (8bit):	4.809852395188501
Encrypted:	false
SSDEEP:	
MD5:	7639B300B40DDAF95318D2177D3265F9
SHA1:	BF9EFDF073231CB3FCFCA5CCCA25B079ECFC45BD
SHA-256:	356A9D4ADFEC484DA824E7A72059B724B1686FC90082F4A4B667630436D593B0
SHA-512:	70593318C6626B5D25729E8D8109D5611B95283266621BE60ADD7E60C0DD5BC43848E956C767251B7B3CCDF5A0929922DE38F90CC8632CCD0C1CCFC7D6DEFE 9
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"Die App ist momentan nicht verf\u00fcgbar."},"craw_connect_to_network":{"message":"Bitte stellen Sie eine Verbindung zu einem Netzwerk her."},"app_name":{"message":"Chrome Web Store-Zahlungen"},"app_description":{"message":"Chrome Web Store-Zahlungen"},"iap_unavailable":{"message":"In-App-Zahlungen sind momentan nicht m\u00f6glich."},"please_sign_in":{"message":"Bitte melden Sie sich in Chrome an."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1236
Entropy (8bit):	4.338644812557597
Encrypted:	false
SSDEEP:	
MD5:	3026E922B17DBEE2674FDAEE960DF584
SHA1:	76602B1E3449F1B67DE42FD31A581B0821BFEFF0
SHA-256:	876845B5A061FAB3CF2A1466E01015DC40DF8449F1CB4205F575CEBED8717BAD
SHA-512:	0C4DCB2589553F9F75534E6C702EBF9095665C93D213564265E39220A99B61BB112A3B20980CE0377C7E98878E3240EB87312B5ECE874382B7E9CA90A0016992
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0397 \u03b5\u03c6\u03b1\u03c1\u03bc\u03bf\u03b3\u03ae \u03c0\u03c1\u03bf\u03c2 \u03c4\u03bf \u03c0\u03b1\u03c1\u03cc\u03bd \u03b4\u03b5\u03bd \u03b5\u03af\u03bd\u03b1\u03b9 \u03b4\u03b9\u03b1\u03b8\u03ad\u03c3\u03b9\u03bc\u03b7."},"craw_connect_to_network":{"message":"\u03a3\u03c5\u03bd\u03b4\u03b5\u03b8\u03b5\u03af\u03c4\u03b5 \u03c3\u03b5 \u03ad\u03bd\u03b1 \u03b4\u03af\u03ba\u03c4\u03c5\u03bf."},"app_name":{"message":"\u03a0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03c3\u03c4\u03bf Chrome Web Store"},"app_description":{"message":"\u03a0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03c3\u03c4\u03bf Chrome Web Store"},"iap_unavailable":{"message":"\u039f\u03b9 \u03c0\u03bb\u03b7\u03c1\u03c9\u03bc\u03ad\u03c2 \u03b5\u03bd\u03c4\u03cc\u03c2 \u03b5\u03c6\u03b1\u03c1\u03bc\u03bf\u03b3\u03ce\u03bd \u03b4\u03b5\u03bd \u03b5\u03af\u03bd\u03b1\u03b9 \u03b1\u03c5\u03c4\u03ae\u03bd \u03c4\u03b7 \u03c3\u03c4\u03b9\u03b3\u03bc\u03ae \u03b4\u03b9\u03b1\u03b8

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\en\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\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 r ed."},"app_name":{"message":"Sistema de pagos de Chrome Web Store"},"app_description":{"message":"Sistema de pagos de Chrome Web Store"},"iap_unavailable": {"message":"En este momento, Pagos En-Apps no est\u00e1 disponible."},"please_sign_in":{"message":"Accede a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\et\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\fi\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	515
Entropy (8bit):	4.699741311937528
Encrypted:	false
SSDEEP:	
MD5:	658DAD2AF2DC3AC1567D84E8B95F68B0
SHA1:	EE1121215960EC5ED5F7B6BDB8E4680731EBF83D
SHA-256:	978BA6D814CF290016833BBAC22DC7C05C2C575B1D6429B9BB14F8C2156BCF29
SHA-512:	F2FB93245D80E2CB2CA1BB2B0654FE92AD9041A558850D78AF4031CB83D2AD3BF5ABCFE6BC32160D028CA3914FA69A64784858A34FA56389C08D52B316346A0 5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Kasalukuyang hindi available ang app."},"craw_connect_to_network":{"message":"Mangyaring kumonekta sa isang network."},"app_ name":{"message":"Mga Pagbabayad sa Chrome Web Store"},"app_description":{"message":"Mga Pagbabayad sa Chrome Web Store"},"iap_unavailable":{"message" :"Kasalukuyang hindi available ang Mga Pagbabayad na In-App."},"please_sign_in":{"message":"Mangyaring mag-sign in sa Chrome."},"jwt_retrieve_failed":{"message" :"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	562
Entropy (8bit):	4.717150188929866
Encrypted:	false
SSDEEP:	
MD5:	1E32A78526E3AC8108E73D384F17450B
SHA1:	BFE2E47D888BA530A27DD1BDE25C46433C2A545C
SHA-256:	80F6EE69F1E022812BCCC1DE1CDC53772CDF90F4E93224161B23FA607D45136A
SHA-512:	5504F6D440779BC96571863D60B1E175EEDDC2E65B1ABBCFCFD19123F329F2E025FBA4D49BD23E33B77FFB6061BA6645132E04D4A7DEDE77F514B2151CDDF8 96
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Application indisponible pour le moment."},"craw_connect_to_network":{"message":"Veuillez vous connecter \u00e0 un r\u00e9se au."},"app_name":{"message":"Paiements via le Chrome\u00a0Web\u00a0Store"},"app_description":{"message":"Paiements via le Chrome\u00a0Web\u00a0Store"} ,"iap_unavailable":{"message":"Les paiements via l'application ne sont pas disponibles pour le moment."},"please_sign_in":{"message":"Veuillez vous connecter \u00e0 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1055
Entropy (8bit):	4.454461505283053
Encrypted:	false
SSDEEP:	
MD5:	B739E3B798D3EEB8AFB3E368455A8E97
SHA1:	56E206DD0AC7EB7B179911BE3F7DD78059CBD4F3
SHA-256:	BA7A53A1398168719F2ACD58CC5FE06AB0B769ECA896D70E7208B18085B42FFA
SHA-512:	181A3B1275D1D17BD48EAA77805981A96E22589A38990214AF3ED029C4A37C2F05ECF747D8FCF816C2AAED6EF82403757F234D67C360A3A6E5DB6C3F59CA1A(C
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0910\u092a\u094d\u0932\u093f\u0915\u0947\u0936\u0928 \u0907\u0938 \u0938\u092e\u092f \u0909\u092a\u0932\u092c\u0 94d\u0927 \u0928\u0939\u0940\u0902 \u0939\u0948."},"craw_connect_to_network":{"message":"\u0915\u0943\u092a\u092f\u093e \u0928\u0947\u091f\u0935\u0930 \u094d\u0915 \u0938\u0947 \u0915\u0928\u0947\u0915\u094d\u091f \u0915\u0930\u0947\u0902."},"app_name":{"message":"Chrome \u0935\u0947\u092c \u0938\u094d\u091f\u094b\u0930 \u0938\u094 4d\u091f\u094b\u0930 \u092d\u0941\u0917\u0924\u093e\u0928"},"app_description":{"message":"Chrome \u0935\u0947\u092c \u0938\u094d\u091f\u094b\u0930 \u0 92d\u0941\u0917\u0924\u093e\u0928"},"iap_unavailable":{"message":"\u0907\u0928-\u0910\u092a \u092d\u0941\u0917\u0924\u093e\u0928 \u0905\u092d\u0940 \u 0909\u092a\u0932\u092c\u094d\u0927 \u0928\u0939\u0940\u0902 \u0939\u0948."},"please_sign_in":{"message":"\u0915\u0943\u092a\u092f\u093e Chrome \u092e\ u0947\u0902 \u0938\u093e\u0907\u0928 \u0907\u0928 \u0915\u0930\u0947\u0902."},"jwt_retrieve_failed":

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	503
Entropy (8bit):	4.819520019697578
Encrypted:	false
SSDEEP:	
MD5:	9CF848209FF50DBF68F5292B3421831C
SHA1:	D29880B7B15102469123D8747BF645706CE8595B
SHA-256:	EA1744C3CFBAA684A31A00067E8493ED114EFF3E878C797C9C55A7B122D855CD
SHA-512:	B784AEE4926F850F30072ABDA85E2E2E3966285F14BDF647BD2A41C5C06CAB04BC962584830E4E913896010396EAD02D90528235B9D9EDA1BDEFBFBB5333ED F5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikacija trenuta\u010dno nije dostupna."},"craw_connect_to_network":{"message":"Pove\u017eite se s mre\u017eom."},"app_nam e":{"message":"Pla\u0107anja u web-trgovini Chrome"},"app_description":{"message":"Pla\u0107anja u web-trgovini Chrome"},"iap_unavailable":{"message":"Pla\u0107 anje u aplikaciji trenuta\u010dno nije dostupno."},"please_sign_in":{"message":"Prijavite se na Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be c ompleted."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\hu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	612
Entropy (8bit):	4.865151680865773
Encrypted:	false
SSDEEP:	
MD5:	4AD92AFDE3408FBBE43B0C3C71677650
SHA1:	3488901077F336A3196F9AE116E36DF1674E1ACA
SHA-256:	61258FE04C23AE14FDC99EE846CEA71CC703990CC0F80C3934299646E86C475E
SHA-512:	EB945FA455DEB9D70033DC0A8AA55D1F47AA00214B70AD34D5419A54F9C05B267F96F9785139F452BEE6972376DDF13EE51C681845A2B0818172FB75BA1FD09
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Az alkalmaz\u00e1s jelenleg nem \u00e9rhet\u0151 el."},"craw_connect_to_network":{"message":"K\u00e9rj\u00fck, csatlakozzon egy h\u00e1l\u00f3zathoz."},"app_name":{"message":"Chrome Internetes \u00e1ruh\u00e1z Fizet\u00e9si rendszere"},"app_description":{"message":"Chrome Internetes \u00e1ruh\u00e1z Fizet\u00e9si rendszere"},"iap_unavailable":{"message":"Az alkalmaz\u00e1son bel\u00fcli fizet\u00e9s jelenleg nem \u00e9rhet\u0151 el."},"plea se_sign_in":{"message":"Jelentkezzen be a Chrome-ba."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\id\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\it\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	806

Entropy (8bit):	4.671841695172103
Encrypted:	false
SSDEEP:	
MD5:	96C8CBD161D3CE9CB1A46CB2CD0C6583
SHA1:	78BBFCF035B5B620E353C8E520653ADD3F4E7DB8
SHA-256:	81D8F1D9F72B3139BC5D9845BCF82990308FB6175D07514D8238B1E6D5D02E8A
SHA-512:	692468B7B44D961D8248BBC30CC11DE9F3F7E89D01A609E6CB71CAF653D8212C15DFA834C5FB6E8261FD21A25E9616861C0A3FC01DB27CBBE79C3FDE2C654 DD
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u30a2\u30d7\u30ea\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u305b\u3093\u3002"},"craw_connect_to_network":{"message":"\u30cd\u30c3\u30c8\u30ef\u30fc\u30af\u306b\u63a5\u7d9a\u3057\u3066\u304f\u3060\u3055\u3044\u3002"},"app_name":{"message":"Chrome \u30a6\u30a7\u30d6\u30b9\u30c8\u30a2\u6c7a\u6e08"},"app_description":{"message":"Chrome \u30a6\u30a7\u30d6\u30b9\u30c8\u30a2\u6c7a\u6e08"},"iap_unavailable":{"message":"\u30a2\u30d7\u30ea\u5185\u30da\u30a4\u30e1\u30f3\u30c8\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u305b\u3093\u3002"},"please_sign_in":{"message":"Chrome \u306b\u30ed\u30b0\u30a4\u30f3\u3057\u3066\u304f\u3060\u3055\u3044\u3002"},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\ko\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	576
Entropy (8bit):	4.846810495221701
Encrypted:	false
SSDEEP:	
MD5:	41F2D63952202E528DBBB683B480F99C
SHA1:	9DD998542DBE6609299D4A5A25364A32FA7D7865
SHA-256:	FF7C083CD1E6134DD8263C634336EB852274BAD1BFAD18762814C42BC65309D8
SHA-512:	7BD2E2D4264C6BD62DF2584F3C1D3A910C5C5A28F4532F1E8F0C2235E93714EDD6074EA24960D4DEB4F9125DA81CA813F06330EFF66FA8DF1552D1DAC6864 E
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Programa \u0161iuo metu negalima."},"craw_connect_to_network":{"message":"Prisijunkite prie tinklo."},"app_name":{"message":"\u201eChrome\u201c internetin\u0117s parduotuv\u0117s mok\u0117jimo sistema"},"app_description":{"message":"\u201eChrome\u201c internetin\u0117s pard uotuv\u0117s mok\u0117jimo sistema"},"iap_unavailable":{"message":"Mok\u0117jimai programoje \u0161iuo metu negalimi."},"please_sign_in":{"message":"Prisijunkite prie \u201eChrome\u201c."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	584
Entropy (8bit):	4.856464171821628

Encrypted:	false
SSDEEP:	
MD5:	1D21ED2D46338636E24401F6E56E326F
SHA1:	24497EDB25724BC4A57823C5CD06F50DB9647DD4
SHA-256:	434A375C32B8A21C435511C551F740FD4D170EC528A8F4EFC3D798EA4A07B606
SHA-512:	10A870718CC6281EE09DE01900D303B06589D9281C5849D6105C6FCF58BFFA3855F29C6ECA3689FFE6EF304BABCF41C5700EE2D8AFE711D57CB711194366FA6A
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Lietotne pagaid\u0101m nav pieejama."},"craw_connect_to_network":{"message":"L\u016bdzu, izveidojiet savienojumu ar t\u012bklu."},"app_name":{"message":"Chrome interneta veikala maks\u0101jumu sist\u0113ma"},"app_description":{"message":"Chrome interneta veikala maks\u0101jumu sist\u0113ma"},"iap_unavailable":{"message":"Maks\u0101jumi lietotn\u0113s pa\u0161laik nav pieejami."},"please_sign_in":{"message":"L\u016bdzu, pierakstieties p\u0101rl\u016bk\u0101 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\nb\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\nl\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	549
Entropy (8bit):	4.978056737225237
Encrypted:	false
SSDEEP:	
MD5:	E16649D87E4CA6462192CF78EBE543EC

SHA1:	53097D592B13F3C1370366B25024EA72208B136A
SHA-256:	EB435F7460A63576CA1ECB51948E7A3AD5168D2F175AE2B5836D469672923D84
SHA-512:	6EC702CEC6E312CAC6F33109A57F7D83A3F073F2F9A9BD42DB0F91A36F87D800EEB978C69023B6A0E00B86ECE3E1024C269F89D038F0926619F40D075F6689D
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikacja jest obecnie niedost\u0119pna."},"craw_connect_to_network":{"message":"Po\u0142\u0105cz si\u0119 z sieci\u0105."},"app_name":{"message":"P\u0142atno\u015bci w sklepie Chrome Web Store"},"app_description":{"message":"P\u0142atno\u015bci w sklepie Chrome Web Store"},"iap_unavailable":{"message":"P\u0142atno\u015bci w ramach aplikacji s\u0105 teraz niedost\u0119pne."},"please_sign_in":{"message":"Zaloguj si\u0119 w Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\pt_BR\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\pt_PT\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\ro\messages.json

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

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\ru\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1165
Entropy (8bit):	4.224419823550506
Encrypted:	false
SSDEEP:	
MD5:	22F9E62ABAD82C2190A839851245A495
SHA1:	E7F79BD875918F0D0799DB5F45FAC6297FB66AF7
SHA-256:	9FC1167626C97BCBFDAFF23C6033A44252F89A501AF1DF41C43CB3A994FEB09F
SHA-512:	F577F2F0C344C4E4050AF025A9FB9AC78CADF7FE177F63AB9863826A9808B7FBF5D3363E3B61D7A6DB083EF5EBAC5474D710347B701640AB9C229A3E5D1F0A4 8
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u0440\u0438\u043b\u043e\u0436\u0435\u043d\u0438\u0435 \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043 d\u043e."},"craw_connect_to_network":{"message":"\u041f\u043e\u0434\u043a\u043b\u044e\u0447\u0438\u0442\u0435\u0441\u044c \u043a \u0441\u0435\u0442\u044c \u0438\u043b\u0438 \u0438\u0441\u043f\u0440\u0430\u0432\u044c\u0442\u0435 \u0438\u043d\u0442\u0435\u0440\u043d\u0435\u0442\u043f\u043e\u0 438."},"app_name":{"message":"\u041f\u043b\u0430\u0433\u0438\u043d\u0430\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u043d\u0430\u044f \u0418\u043d\u0442\u0435\u0440\u043d\u0435\u0442\u043d\u0430 Chrome"},"app_description":{"message":"\u041f\u043b\u0430\u0433\u0438\u043d\u0430\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u043d\u0430\u044f \u0418\u043d\u0442\u0435\u0440\u043d\u0435\u0442\u043d\u0430 Chrome"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u0433\u0438\u043d\u0430\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u043d\u0430\u044f \u0418\u043d\u0442\u0435\u0440\u043d\u0435\u0442\u043d\u0430 Chrome"},"iap_unavailable":{"message":"\u041f\u043b\u0430\u0433\u0438\u043d\u0430\u044f \u0441\u0438\u0441\u0442\u0435\u043c\u043d\u0430\u044f \u0418\u043d\u0442\u0435\u0440\u043d\u0435\u0442\u043d\u0430 \u0447\u0435\u0440\u0435\u0437 \u043f\u0440\u0438\u043b\u043e\u0436\u0435\u043d\u0438\u0435 \u043d\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u0430."},''

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\sk\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\sl\messages.json

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

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\sr\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\sv\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\th\messages.json

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

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\tr\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\uk\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\vi\messages.json

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

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\zh_CN\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL_locales\zh_TW\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL\craw_background.js

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	544643
Entropy (8bit):	5.385396177420207
Encrypted:	false
SSDEEP:	
MD5:	6EEBED29E6A6301E92A9B8B347807F5F
SHA1:	65DFB69B650560551110B33DCBA50B25E5B876DE
SHA-256:	04CD9494B0ED83924DAD12202630B20D053D9E2819C8E826A386C814CC0A1697
SHA-512:	FEDE6DB31F2AD242E7BC7B52A8859BA7F466A0B920A8DADCB32DCFB5B2A2742E98B767FF22E0C5BC5C11FEC021240AA9E458486C9039EB4EBE5CF6AF7BE97BF2
Malicious:	false

Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var d,e=e||{};e.scope={};e.arrayIteratorImpl=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};e.arrayIterator=function(a){return{next:e.arrayIteratorImpl(a)}};e.ASSUME_ES5=!1;e.ASSUME_NO_NATIVE_MAP=!1;e.ASSUME_NO_NATIVE_SET=!1;e.SIMPLE_FROUND_POLYFILL=!1;e.ISOLATE_POLYFILLS=!1;e.FORCE_POLYFILL_PROMISE=!1;e.FORCE_POLYFILL_PROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;.e.defineProperty=e.ASSUME_ES5||"function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};e.getGlobal=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");};e.global=e.getGlobal(this);.e.IS_SYMBOL_NATIVE="func

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL\craw_window.js

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	261316
Entropy (8bit):	5.444466092380538
Encrypted:	false
SSDEEP:	
MD5:	1709B6F00A136241185161AA3DF46A06
SHA1:	33DA7D262FFED1A5C2D85B7390E9DBC830CBE494
SHA-256:	5721A4B3F8E09C869A629EFFD350B51C9D46F0AC136717D4DB6265C0EE6F9AC8
SHA-512:	26835B4C050F53AD2DDB84469DF9A84BBB2786A655AB52DFC20B54BEDCB81D1ECD789198D5B7D8B940242E5CEAC818A177444D402397AE82C203438C4B1D19CB
Malicious:	false
Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var b,k=k||{};k.scope={};k.createTemplateTagFirstArg=function(a){return a.raw=a};k.createTemplateTagFirstArgWithRaw=function(a,c){a.raw=c;return a};k.arrayIteratorImpl=function(a){var c=0;return function(){return c<a.length?{done:!1,value:a[c++]}:{done:!0}}};k.arrayIterator=function(a){return{next:k.arrayIteratorImpl(a)}};k.makeIterator=function(a){var c="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return c?c.call(a):k.arrayIterator(a)};.k.arrayFromIterator=function(a){for(var c,d=[];!(c=a.next()).done;)d.push(c.value);return d};k.arrayFromIterable=function(a){return a instanceof Array?a:k.arrayFromIterator(k.makeIterator(a))};k.ASSUME_ES5=!1;k.ASSUME_NO_NATIVE_MAP=!1;k.ASSUME_NO_NATIVE_SET=!1;k.SIMPLE_FROUND_POLYFILL=!1;k.ISOLATE_POLYFILLS=!1;k.FORCE_POLYFILL_PROMISE=!1;k.FORCE_POLYFILL_PROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;.k.objectCreate=k.ASSUME_ES5||"function"==typeof Object.cre

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\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_dir5180_1640304514\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:	EE81E5509CBC2CB2B6C834224688C1E1B1AA9AA3866C52F8EAED040D5C390653C52D8D681E2E2CF62906643962ABAC823D5B622385B983B21E0DCCAFDF281F FF
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <link href="/css/craw_window.css" rel="stylesheet">. <script src="/craw_window.js"></script>. </head>. <body>. <webview> </webview>. . . . . <div cl ass="craw_overlay" id="offline_overlay">. . . < /span>. . . . . </body>.</html>.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL\images\flapper.gif

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL\images\icon_128.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	3313
Entropy (8bit):	7.846746884883354
Encrypted:	false
SSDEEP:	
MD5:	30899B6C4E4A757B8EC6DD2208ACDFB4
SHA1:	F2C5880A724C6D75CCE1B5191E0D82C3BC7DE768
SHA-256:	4F17EFBD974A41D88CB36567AAB6BF4586579E78780F00B1826676819E14BFF4
SHA-512:	58539E3F0AD7FEF30792EFCDBBD955599E11E4261C9946E7C3DFF6267E01747354EA3B901C46FC8329F81C68AFBEB2D05FE3FCB266BC5948DE8BEFA5B8D040 EE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a.....IDATx.....S.d.....x{g..T...9..:.3...a.9..J.V....a...(.,..,...P@..)..d.\.)...D..i.f.yI..e{m..|.~...}.MC_oRz.....}.7...^o.,...I...V.....Z.....]... ...>.(..._..r_Z... .....4x.....|>`A../.x<..n.{..@....@../.X#.....D..X..@....c.."..+^. ..>!H.....6..,.KJ...u.j..$I".L.....n.O.{0.<D0p.!.N...l6."..@.K.>A0d...?...."...\....H0d.d.'.l.;".>...`.&$I...P..6.!.xO... EQ...Y.F~BE..ea.e".~[.F.![..?..f.....,..... m.....$I....`..8.....@f>....."..Fw.....<...7.k.l!p.(..p...v...E.....|...@.P,...D.B..@. ...E."..../.....|...@. ...|...@. ...|.../.....|.....\..^...,n...  ..8o.....ib>....zc.....|h .5.<..+...`...._.....,.....p....EK.a.X0...9)...QO.a.4....k...>.A.....`y{.4L....W>M.....^.N..<.[...w]..>.FK.O~...`...K.][...eY...H.+..z9...A..O3.)r;..c.u.B.....`^2...}.i.  ^}.\.....w.u0....x~.u.....>.....~../_..2....;6..`(....MKE...f0."..I>."99.....y....Q.W$I.8]J0..AC(.*.....9_...g..#.....%.....8.c.h..0..?\e..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\CRX_INSTALL\images\icon_16.png

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	531
Entropy (8bit):	7.465541280375791
Encrypted:	false
SSDEEP:	
MD5:	344554D96E418120BD80EF5DE5194697
SHA1:	23E141C3A6CE368ACC1C299F062AB85914BCB17E
SHA-256:	0A4BD08DB6422F8E7A8A218EF39C1B99A5A675F12697F26BE88F9AFC2E1F9378

SHA-512:	7AE38853E5ACCA479D7FD81D48BB88C671CF4DCE63342209BCFF045AC581A04B7B0ED48F6C58253DB950935C0522CAAA4FBC6CF5A25151A8960BA56FC8045E9E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDATx....k.a..?.]...Z5.P...`G77.....Q'q.....u..E...%.$].\...P.m5.....$M...K...#..p.....|.{.-*...Z....=.._.Dc<.J.R...A.@....I)...Lb..s&.q.T_..|a.....z ..0..m[.+ ..T.R9.7.`0..$~.....H.Q\|.wg..r...E6n_.Y.E..x.(.....?{H.Z3;..="X.F.w.:.h...Z..V.S.\|..V.....{T-.y....*..>.>.fQ...a.I.<;I..yr.....Un....7w.....S.3.Fg\|.O..\.~{...S....d.....R .%.A...$.g.y..f.IW/..JC.z.H..)#....A+. .k.wb...p.m:a.?D.1GD.&..N.....?..\..n....W.O...j.%.`.*H.s.Fxt.\.....Yv.?.....f....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir5180_1640304514\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_dir5180_1640304514\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_dir5180_1640304514\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_dir5180_1640304514\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`.

Static File Info

No static file info