

JOeSandbox Cloud BASIC



ID: 652377
Cookbook: browseurl.jbs
Time: 09:09:55
Date: 26/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report http://gossip-celeb-fashion.com	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Sigma Signatures	4
Snort Signatures	5
Joe Sandbox Signatures	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
URLs from Memory and Binaries	8
World Map of Contacted IPs	9
Public IPs	9
Private	9
General Information	9
Warnings	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASNs	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	11
C:\Users\user\AppData\Local\Google\Chrome\User Data\0faf90a8-b432-4bf7-9ce2-b1c5ff93022b.tmp	11
C:\Users\user\AppData\Local\Google\Chrome\User Data\95ccd9e-b7b7-4de9-b879-29eea5b4f977.tmp	11
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	12
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\35f92f69-a9a1-4552-b711-d37c3d9d6e2a.tmp	12
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\45d87001-0254-4f9c-a54e-a7640e725199.tmp	12
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\46bfd5a5-0783-42fb-826c-a115746fd6d0.tmp	13
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4d5866c4-9a45-4895-8131-52a1f57aa270.tmp	13
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\97cf04af-e5f0-49b2-a557-bb5438d7db71.tmp	13
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda1.0.0.6_0\metadata\computed_hashes.json	14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcapaomhbhbimeihdjnejgic\def\0d2f39e9-042e-4ab4-bd9f-15e56c7d8087.tmp	16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcapaomhbhbimeihdjnejgic\def\GPUCache\data_1	16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcapaomhbhbimeihdjnejgic\def\Network Persistent State (copy)	17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	18
C:\Users\user\AppData\Local\Google\Chrome\User Data\b8aa9d1a-c55d-4ca0-b604-46481ef1818e.tmp	19
C:\Users\user\AppData\Local\Temp\63139fbc-b2b0-46a8-9a88-495f5a059f99.tmp	19
C:\Users\user\AppData\Local\Temp\86ae616-600c-400d-8146-4898941be92c.tmp	19
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\bg\messages.json	20
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\ca\messages.json	20

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\cs\messages.json	20
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\da\messages.json	21
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\de\messages.json	21
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\el\messages.json	21
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\en\messages.json	22
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\en_GB\messages.json	22
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\es\messages.json	22
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\es_419\messages.json	23
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\et\messages.json	23
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\fi\messages.json	23
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\fil\messages.json	24
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\fr\messages.json	24
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\hi\messages.json	24
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\hr\messages.json	24
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\hu\messages.json	25
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\id\messages.json	25
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\it\messages.json	25
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\ja\messages.json	26
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\ko\messages.json	26
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\lt\messages.json	26
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\lv\messages.json	27
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\nb\messages.json	27
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\nl\messages.json	27
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\pl\messages.json	28
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\pt_BR\messages.json	28
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\pt_PT\messages.json	28
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\ro\messages.json	29
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\ru\messages.json	29
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\sk\messages.json	29
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\sl\messages.json	30
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\sr\messages.json	30
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\sv\messages.json	30
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\th\messages.json	30
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\tr\messages.json	31
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\uk\messages.json	31
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\vi\messages.json	31
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\zh_CN\messages.json	32
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\locales\zh_TW\messages.json	32
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\metadata\verified_contents.json	32
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\craw_background.js	33
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\craw_window.js	33
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\css\craw_window.css	33
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\html\craw_window.html	34
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\flapper.gif	34
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\icon_128.png	34
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\icon_16.png	35
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\topbar_floating_button.png	35
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\topbar_floating_button_close.png	35
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\topbar_floating_button_hover.png	36
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\topbar_floating_button_maximize.png	36
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\topbar_floating_button_pressed.png	36
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\manifest.json	36
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\fb86ae616-600c-400d-8146-4898941be92c.tmp	37
Static File Info	37
Network Behavior	37
Network Port Distribution	37
TCP Packets	38
UDP Packets	40
DNS Queries	40
DNS Answers	40
HTTP Request Dependency Graph	40
HTTP Packets	41
HTTPS Proxied Packets	42
Statistics	44
Behavior	44
System Behavior	45
Analysis Process: chrome.exePID: 1740, Parent PID: 5044	45
General	45
File Activities	45
Registry Activities	45
Key Value Modified	45
Analysis Process: chrome.exePID: 5564, Parent PID: 1740	46
General	46
File Activities	46
Disassembly	46

Windows Analysis Report

http://gossip-celeb-fashion.com

Overview

General Information

Sample URL:

http://gossip-celeb-fashion.com

Analysis ID:

652377

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

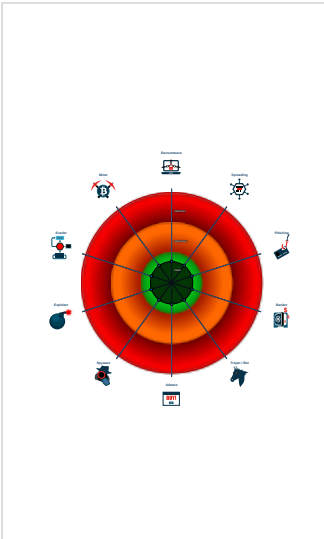
UNKNOWN

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

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 1740 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "http://gossip-celeb-fashion.com MD5: C139654B5C1438A95B321BB01AD63EF6)
 - chrome.exe (PID: 5564 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,978469522289147633,16330879895871495791,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1936 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

 No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, [click here to show all signatures](#).

Mitre Att&ck Matrix

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

Behavior Graph

Behavior Graph
ID: 652377
URL: http://gossip-celeb-fashion.com
Startdate: 26/06/2022
Architecture: WINDOWS
Score: 0

MALICIOUS

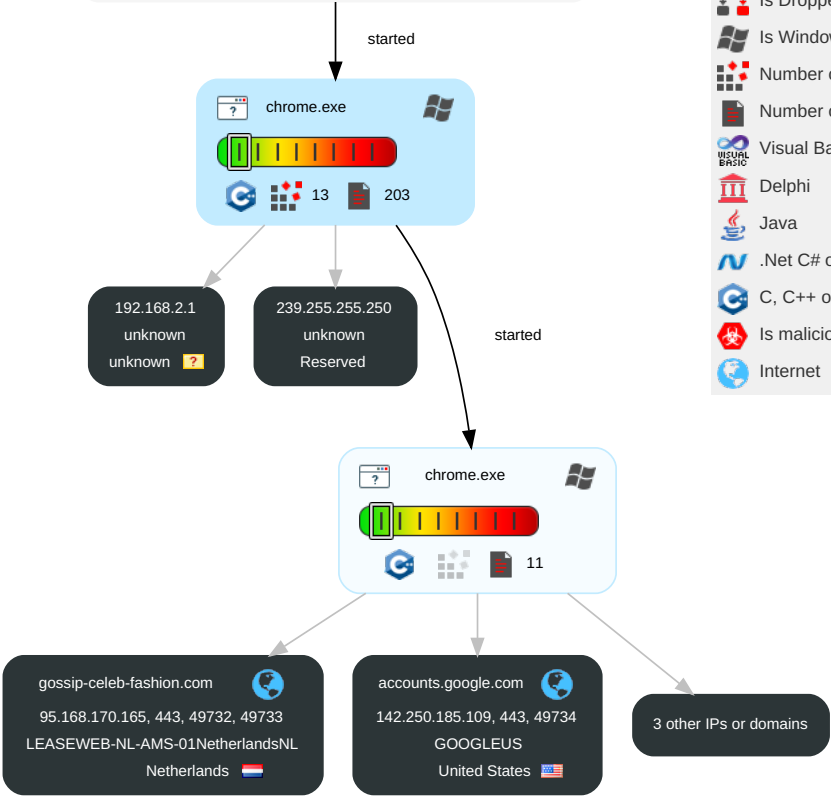
SUSPICIOUS

CLEAN

UNKNOWN

Legend:

- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

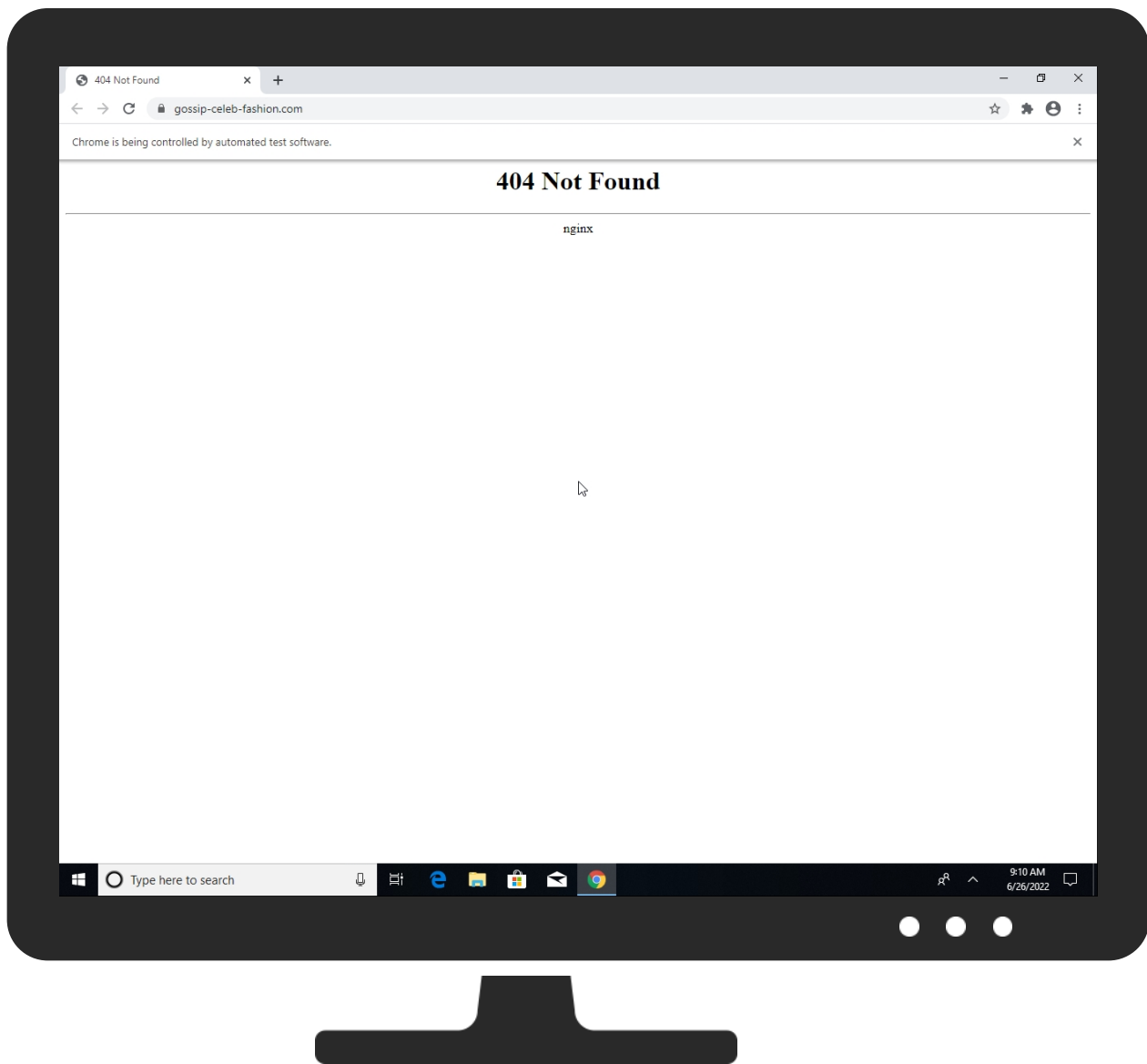


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://gossip-celeb-fashion.com	0%	Virustotal		Browse
http://gossip-celeb-fashion.com	0%	Avira URL Cloud	safe	

Dropped Files

 No Antivirus matches
--

Unpacked PE Files

 No Antivirus matches
--

Domains

 No Antivirus matches
--

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://gossip-celeb-fashion.com/favicon.ico	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://gossip-celeb-fashion.com/	0%	Virustotal		Browse
http://gossip-celeb-fashion.com/	0%	Avira URL Cloud	safe	
http://https://gossip-celeb-fashion.com/	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gossip-celeb-fashion.com	95.168.170.165	true	false		unknown
accounts.google.com	142.250.185.109	true	false		high
clients.l.google.com	142.250.186.174	true	false		high
clients2.google.com	unknown	unknown	false		high

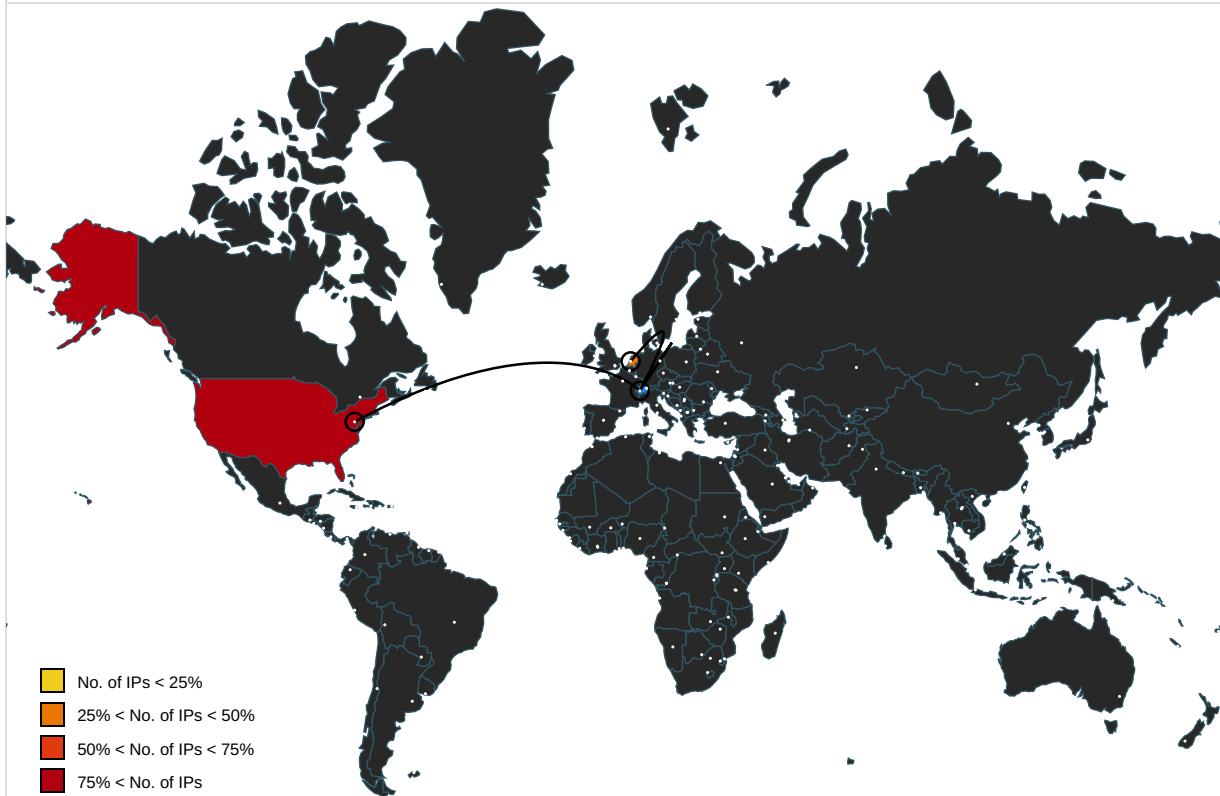
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://gossip-celeb-fashion.com/favicon.ico	false	Avira URL Cloud: safe	unknown
http://https://gossip-celeb-fashion.com/	false	0%, Virustotal, Browse	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmhkhkegcagldgiimedpiccmgmieda%26v%3D0.0.0.0%26install-edby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://gossip-celeb-fashion.com/	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://https://gossip-celeb-fashion.com/	false	0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	4d5866c4-9a45-4895-8131-52a1f57aa270.tmp.1.dr, 0d2f39e9-042e-4ab4-bd9f-15e56c7d8087.tmp.1.dr	false	URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.0.dr	false		high
http://https://ogs.google.com	4d5866c4-9a45-4895-8131-52a1f57aa270.tmp.1.dr	false		high
http://https://www.google.com/images/clear.dot.gif	craw_window.js.0.dr	false		high
http://https://play.google.com	4d5866c4-9a45-4895-8131-52a1f57aa270.tmp.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.0.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.0.dr	false		high
http://https://www.google.com	4d5866c4-9a45-4895-8131-52a1f57aa270.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://accounts.google.com	4d5866c4-9a45-4895-8131-52a1f57aa270.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	4d5866c4-9a45-4895-8131-52a1f57aa270.tmp.1.dr	false		high
http://https://apis.google.com	4d5866c4-9a45-4895-8131-52a1f57aa270.tmp.1.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.0.dr	false		high
http://https://www.google.com/	manifest.json.0.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://clients2.google.com	4d5866c4-9a45-4895-8131-52a1f57aa270.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.109	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.186.174	clients.l.google.com	United States		15169	GOOGLEUS	false
95.168.170.165	gossip-celeb-fashion.com	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	652377
Start date and time: 26/06/202209:09:55	2022-06-26 09:09:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://gossip-celeb-fashion.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@24/83@3/6
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 142.250.185.174, 74.125.108.201, 173.194.187.73, 142.250.185.163, 80.67.82.211, 80.67.82.235, 40.125.122.176
- Excluded domains from analysis (whitelisted): www.bing.com, r4---sn-1gi7znekv1.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, a1449.dscg2.akamai.net, arc.msn.com, r4---sn-4g5e6nsk.vgt1.com, e12564.dspb.akamaiedge.net, redirector.vgt1.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, r4.sn-4g5e6nsk.vgt1.com, img-prod-cms-rt-microsoft-com.akamaized.net, r4.sn-1gi7znekv1.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBIESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
Malicious:	false
Reputation:	low
Preview:	BDic.....6....".Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGND.S.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMD.S.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\0faf90a8-b432-4bf7-9ce2-b1c5ff93022b.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):	214022
Entropy (8bit):	6.070971348785279
Encrypted:	false
SSDEEP:	3072:d24yM9YYofxTphal4KW43mFyGAnJRXQeYJHj8ZmJrakasUCpqFcbXaflB0u1GOJl:Udtfp+eVMNAvHITaqflIUOoSiuRU
MD5:	70ACD12E76E868212372C94D9830763D
SHA1:	E2C3EBF232EB3649FBDE05CB6FFE544AB4EB1ACD
SHA-256:	501505A71F73AA1EB2E50BE3E83DDE2262D5A23B2FE023049F831497FD70F258
SHA-512:	ED4139450924A34EF3BCDEF8BEFD6A80B739492DFC238D99C7C32751FF29C14FF9D0FC95A354EE6F177B1023ECDF812F84EE8B91D18F7699DB2637735FCE431E
Malicious:	false
Reputation:	low
Preview:	{\"browser\":{\"last_redirect_origin\":\"\",\"shortcut_migration_version\":\"85.0.4183.121\"},\"data_use_measurement\":{\"data_used\":{\"services\":{\"background\":{},\"foreground\":{}},\"user\":{\"background\":{},\"foreground\":{}}},\"hardware_acceleration_mode_previous\":true,\"intl\":{\"app_locale\":\"en\",\"legacy\":{\"profile\":{\"name\":{\"migrated\":true}}},\"network_time\":{\"network_time_mapping\":{\"local\":\"1.656259859117958e+12\",\"network\":\"1.65622746e+12\",\"ticks\":\"116102039.0\",\"uncertainty\":\"4086985.0\"},\"os_crypt\":{\"encrypted_key\":\"RFBBUeKBAAAA0lyd3wEVORGMegDAT8KX6wEAAABL95WK194zTZq03WydZHLcAAAAAIAAAAAABBMAAAAQAIAAAABAL2tyan+lsWbxhoUVdUYrYi wg8iJkppNr2ZbBFie9UAAAAAA6AAAAAaGAAIAAAABDv4gjLq1dOS7lKRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQ j2xYeAnS1vCL4JXAsdfijw4oXIE4R7I0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYPp4zeP\"},\"password_manager\":{\"os_password_blank\":true,\"os_password_last_changed\":\"13245951016607996\"},\"plugins\":{\"metadata\":{\"adobe-flash-player\":{\"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\95ccdf9e-b7b7-4de9-b879-29eea5b4f977.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):	214022
Entropy (8bit):	6.070971348785279
Encrypted:	false
SSDEEP:	3072:d24yM9YYofxTphal4KW43mFyGAnJRXQeYJHj8ZmJrakasUCpqFcbXaflB0u1GOJl:Udtfp+eVMNAvHITaqflIUOoSiuRU
MD5:	70ACD12E76E868212372C94D9830763D
SHA1:	E2C3EBF232EB3649FBDE05CB6FFE544AB4EB1ACD
SHA-256:	501505A71F73AA1EB2E50BE3E83DDE2262D5A23B2FE023049F831497FD70F258
SHA-512:	ED4139450924A34EF3BCDEF8BEFD6A80B739492DFC238D99C7C32751FF29C14FF9D0FC95A354EE6F177B1023ECDF812F84EE8B91D18F7699DB2637735FCE431E
Malicious:	false
Reputation:	low

```

Preview: {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{"foreground":{},"user":{"background":{"foreground":{"local":{"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":"migrated":true},"network_info":{"network_time_mapping":{"fctt":1.656259859117958e+12,"network":1.65627246e+12,"uncertainty":{"4086985.0},"os_crypt":{"encrypted_key":"RFBbUEkBAaaa0lyd3wEV0RMegDAt8KX6wEAAABl95kWi94zTZq03WydzHLCAAAAAAIAAAAAABbmAAAAAQAAIAAABAL2tyan-HsWtxhoUvDyYrYwg8lQjppNr2zbFie9UJAAwAAAAA6AAaAIAAAABDv4gjlQ1dOS7lRGK21YVxojnHsRhNbP8/D1z78mXMAAAAB045Od5v4BxiF4bdrYjDjXn4W2fxYqJ2xfYeAnS1vcL4j3XAsdfjw4X0IE4R7l0AAABl36FqChftM9b7EtAPw98XR5Y944rd1WsgWCoPFYXajBl3GUXhUWxgJbG5bWcU4jEdaxkLxAYp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

```

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+fttE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C
SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6CF
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}....M..2!..%

[illegible]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\45d87001-0254-4f9c-a54e-a7640e725199.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17703
Entropy (8bit):	5.5772887980485075
Encrypted:	false
SSDEEP:	384:auYteLlrhXK1kXqKf/pUZNCgVLH2HfDPrUQGWYA/4K:DLI5K1kXqKf/pUZNCgVLH2HfTrUQn/h
MD5:	5EB54393B75553FFAF5471A8B0F5C334
SHA1:	D573032E3BFF8E4A33B5DB9C353ADC517B136F63
SHA-256:	2C92667E1714D90E14957F27182305EAAE22040C64CE55FC29504F2400EC8B8D
SHA-512:	A2DDDDBD735E45E42A6CDCA8BF37C3AF0DDA4A8813D9A6AA43707C8F70AA9104BE7D048B30EE818355058B6E9512754E2489E38DBCE7B1F1C2C61DDF8D9742B9
Malicious:	false
Reputation:	low

Preview:	{ "download":{ "always_open_pdf_externally":true, "directory_upgrade":true, "extensions_to_open":{ "pdf.doc:docx.docxm.docm.xls:xlsx.xlsm:xpml:ppt:pptx:pptm:mht:rtf.pub:vsd:mpp.mdb:dot:dotm.xlsm:xlw:show.cell:hwp:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe.html:htm:xhtml:tbz2:lz"}, "extensions":{ "settings":{ "ahfgeienlihckogmojhjhadlkjgocpleb":{ "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":"13300733456566945", "location":5, "manifest":{ "app":{ "launch":{ "web_url":"https://chrome.google.com/webstore"}, "urls":{ "https://chrome.google.com/webstore"}}, "description":"Discover great apps, games, extensions and themes for Google Chrome.", "icons":{ "128":"webstore_i
----------	---

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\46bfdda5-0783-42fb-826c-a115746fd6d0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFEC7FFCDB92598A0F13D313CC9EBC2A07E61F007BAF58BF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4d5866c4-9a45-4895-8131-52a1f57aa270.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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbslHt/soBDysKqnsIzMHpDCLsWJMHLSNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160;
Malicious:	false
Reputation:	low
Preview:	{ "net":{ "http_server_properties":{ "servers":{ {"alternative_service":{ "advertised_versions":{ }, "expiration":"13248543677350473", "port":443, "protocol_str":"quic"}, "advertised_versions":{ }, "expiration":"13248543677350474", "port":443, "protocol_str":"quic"}}, "isolation":{ }, "network_stats":{ "srtt":31344}, "server":"https://dns.google", "supports_spdy":true}, "alternative_service":{ "advertised_versions":{ "advertised_versions":{ }, "expiration":"13248543501474403", "port":443, "protocol_str":"quic"}, "advertised_versions":{ }, "expiration":"13248543501474403", "port":443, "protocol_str":"quic"}}, "isolation":{ }, "network_stats":{ "srtt":31656}, "server":"https://clients2.googleusercontent.com", "supports_spdy":true}, "alternative_service":{ "advertised_versions":{ "expiration":"13248543501454993", "port":443, "protocol_str":"quic"}, "advertised_versions":{ }, "expiration":"13248543501454994", "port":443, "protocol_str":"quic"}}, "isolation":{ }, "network_stats":{ "srtt":39369}, "server":"https://www.googleapis.com", "supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\97cf04af-e5f0-49b2-a557-bb5438d7db71.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17702
Entropy (8bit):	5.577183902137466
Encrypted:	false
SSDEEP:	384:auYtbLlrhXK1kXqKf/pUZNCgVLH2HfDPrUQTWYA/4i:QLi5K1kXqKf/pUZNCgVLH2HfTrUQq/N
MD5:	EB0A07B8BABF2747866089102E4303EC
SHA1:	C88FCE4EA711C2C953F5E2A82C192A928208BF61
SHA-256:	5A6A1459E949AE38C0453361C6FFDBB815E5169E3C56E8ABAA6688415143FE63
SHA-512:	5D2B0B86A810C4498AAC930CC858E6EC4E7F1FB47F49D03ED45ACD0B9E90B7305CCCA1D11E5425B880AA3BAE5183BA822F4A917FA898F2CF529FFBCEB0F40A51
Malicious:	false
Reputation:	low

Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":".pdf.doc:docx.docxm:docm:xls:xlsx:xlsm:xslm:ppt:pptx:pptm:pptm:htm:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwp: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":"13300733456566945","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]}],"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i
----------	--

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_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:	modified
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXltnLG48gcLg/Pkl:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9C8BCFD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2536382D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":{"block_hashes":{"A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpl0"=","WSOpQRkYTHjPSIG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0"=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY"=","LPxhhJiuU0lprt0T6flpS7TKaDg7MocrbmzO65xH6RI"=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE"=","wifibc1QMfBN2jrtUtlgsCefvuceTpAatmLvul11RJA"=","dHjWslldijjMWqg3T8MG58RuugRXk32vqi/13JqEGa"=","zD3DV7dbvfNvx1hdhU01fW5ily52DLN0CFU/ADaEeTI"=","DpjXcO85FFFY9KJFPkGNlFUtdQlOsGwO5jUckiUwY14"=","gqid6l1+mk/6yWgUECRofl9lMipXgXh2jEN2+CxmPE0"=","prDB91X2Mmfg/M/txVMITWbmEGbOGjqBTP7CMjYqdHs"=","YLPaQV4gqoyS/zFkEt3Cn2j0q2v9QOStHVFwN8EzCM"=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1Jdn/UtbnAmq6T0"=","+oOc6ca+ChKUPTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI"=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w"=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68"=","E3vWWLQxzmj+e5QxYbUscLj5n0lTpw5JBHV1Kph3/KM"=","i3l8ghdTf9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg"=","R8B8qYabnMSILPhrtu0hGYrHn3llsMHqBbi70gkljEE"=","rhIzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y"=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxIXNQxIX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC2269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEEF985Df
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.215228184605686
Encrypted:	false
SSDEEP:	6:IGG7gHqyq2PWXp+N23iKKdK25+Xqx8chl+HFUtqVAGG7z/1ZmwYVAGG7+RkwOWXc:kGKva5KkTXfchl3FUtyGf/1/MGG5f5KN
MD5:	FAC1BA32D8FF0D1880A2D5306640B0BD
SHA1:	3E85627D10AE792C37F3E0A438D9C06518C8D9EF
SHA-256:	51BBAC2B6D41D7C754C6F4EB7E93D4A370B590776ABB137FBA7176DF0258F6A1
SHA-512:	66EB12EC4EC625DA3D135C70361FE4D7940DA0EF8AA1FA7CAEED8AD8272934C7D61BD8A0677F77B80ECBCAE5CCFBAC5E37B1C27968B6C3214EF1212B356CD6D2
Malicious:	false
Reputation:	low

Preview:	2022/06/26-09:11:04.109 1bc0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2022/06/26-09:11:04.110 1bc0 Recovering log #3.2022/06/26-09:11:04.111 1bc0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log .
----------	--

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.215228184605686
Encrypted:	false
SSDEEP:	6:IGG7gHqyq2PWXp+N23iKdK25+Xqx8chl+HFU tqVAGG7z/1ZmwYVAGG7+RkwOWXc:kGKva5KkTXfchl3FUtyGf/1/MGG5f5KN
MD5:	FAC1BA32D8FF0D1880A2D5306640B0BD
SHA1:	3E85627D10AE792C37F3E0A438D9C06518C8D9EF
SHA-256:	51BBAC2B6D41D7C754C6F4EB7E93D4A370B590776ABB137FBA7176DF0258F6A1
SHA-512:	66EB12EC4EC625DA3D135C70361FE4D7940DA0EF8AA1FA7CAEED8AD8272934C7D61BD8A0677F77B80ECBCAEECCFBAC5E37B1C27968B6C3214EF1212B356CD6D2
Malicious:	false
Reputation:	low
Preview:	2022/06/26-09:11:04.109 1bc0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2022/06/26-09:11:04.110 1bc0 Recovering log #3.2022/06/26-09:11:04.111 1bc0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHbKsvxMHVzspxMHbslHt/soBDysKqnsllzMHPdCLsWJMHLSNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
Malicious:	false
Reputation:	low
Preview:	{ "net": { "http_server_properties": { "servers": [{ "alternative_service": { "advertised_versions": [], "expiration": "13248543677350473", "port": 443, "protocol_str": "quic" }, { "advertised_versions": [], "expiration": "13248543677350474", "port": 443, "protocol_str": "quic" }], "isolation": [], "network_stats": { "srtt": 31344, "server": "https://dns.google", "support_s_spdy": true }, { "alternative_service": { "advertised_versions": [], "expiration": "13248543501474403", "port": 443, "protocol_str": "quic" }, { "advertised_versions": [], "expiration": "13248543501474403", "port": 443, "protocol_str": "quic" }], "isolation": [], "network_stats": { "srtt": 31656, "server": "https://clients2.googleusercontent.com", "supports_spdy": true }, { "alternative_service": { "advertised_versions": [], "expiration": "13248543501454993", "port": 443, "protocol_str": "quic" }, { "advertised_versions": [], "expiration": "13248543501454994", "port": 443, "protocol_str": "quic" }], "isolation": [], "network_stats": { "srtt": 39369, "server": "https://www.googleapis.com", "supports_spdy": true },

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5158
Entropy (8bit):	4.985257414935564
Encrypted:	false
SSDEEP:	96:noCtff1pcKISook0JCKL8YkL1BbOTQVuwn:noCR1pcO4KvkLr
MD5:	410123AA107ECB860EE8D38B85F0873F
SHA1:	A031C3F0C3040CB05DCDBC2B60202B00BCF5853C
SHA-256:	6D69621C29821AB5144A57932F3E674F92A7FB7D92DA0001F8899CC94096A3DC
SHA-512:	59D0939F74D2C272C9F497A438AC5D425D091647A7B6FB82AB7627411C66B5983D74A7D797F96167AC479016D587085883884ED11CDA1F42EC16F1D3FD7FA3
Malicious:	false
Reputation:	low

Reputation:	low
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjneigcl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQIsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBDD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{ "net": { "http_server_properties": { "servers": [{ "alternative_service": { "advertised_versions": [50], "expiration": "13248543490879170", "port": 443, "protocol_str": "quic" }, { "advertised_versions": [73], "expiration": "13248543490879171", "port": 443, "protocol_str": "quic" }], "isolation": [], "server": "https://dns.google", "supports_spdy": true } }, "version": 5 }, "network_qualities": { "CAASABiAgICA+P////8B": "4G", "CAESABiAgICA+P////8B": "4G" } } }

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E089
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E089
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RIAl:tbdlmQxZaHiGi0R6l
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\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEDCC5A8A076B37703669C294C6D1BFAAE963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	214022
Entropy (8bit):	6.070971348785279
Encrypted:	false
SSDEEP:	3072:d24yM9YYofxTphal4KW43mFyGAnJRXQeYJHj8ZmJrakasUCpqFcbXaflB0u1GOJl:Udtfp+eVMNAvHITaqfllUOoSiuRU
MD5:	70ACD12E76E868212372C94D9830763D
SHA1:	E2C3EBF232EB3649FBDE05CB6FFE544AB4EB1ACD
SHA-256:	501505A71F73AA1EB2E50BE3E83DDE2262D5A23BF023049F831497FD70F258
SHA-512:	ED4139450924A34EF3BCDEF8BEFD6A80B739492DFC238D99C7C32751FF29C14FF9D0FC95A354EE6F177B1023ECD8F12F48EE8B91D18F7699DB2637735FCE43E
Malicious:	false
Reputation:	low
Preview:	{\"browser\":{\"last_redirect_origin\":\"\",\"shortcut_migration_version\":\"85.0.4183.121\"},\"data_use_measurement\":{\"data_used\":{\"services\":{\"background\":{},\"foreground\":{}},\"user\":{\"background\":{},\"foreground\":{}}},\"hardware_acceleration_mode_previous\":true,\"intl\":{\"app_locale\":\"en\"},\"legacy\":{\"profile\":{\"name\":{\"migrated\":true}}},\"network_time\":{\"network_time_mapping\":{\"local\":1.656259859117958e+12,\"network\":1.65622746e+12,\"ticks\":116102039.0,\"uncertainty\":4086985.0}},\"os_crypt\":{\"encrypted_key\":\"RFBbUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABl95WKi94zTZq03WydZHLcAAAAAIAAAAAABBMAAAAAQAAIAAABAL2tyan+lsWtxhoUVdUYrYi wG8iJkppNr2ZbFie9UAAAAA6AAAAAaGAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQ j2xYYeAnS1vCL4JXAsdflljw4oXIE4R7l0AAAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP\"},\"password_manager\":{\"os_password_blank\":true,\"os_password_last_changed\":\"13245951016607996\"},\"plugins\":{\"metadata\":{\"adobe-flash-player\":{\"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7460389223230637

Encrypted:	false
SSDEEP:	384:jLg/vVIYJ5OjaN7rQvXt3o3pIHREG8brWB/XxQJ1Vkr+TmuZCtTfz4Op53Nm1ri:/lqV1q1Yg0ej7V5037+tKzNPx1
MD5:	E678DF1823305D8568D2CAAE9176D2C7
SHA1:	B94A79AA88B9EC5FA9AE07B8BA1B2C7E7E88CD52
SHA-256:	A58B14685949CA93E4D81553FCA7FEF818537305B7C140C05FE0BD40C5D9BADC
SHA-512:	BE6183AE79AF8C68BCCFB9737CBC0AD9E25570471CB507210C1401BEB99E241A5BABBA8BA533F7D6458A26F432CF733C6D343AA6B3534FCAA0B477A9BC408D8A
Malicious:	false
Reputation:	low
Preview:	0j.....*...C::\P.R.O.G.R.A~1\M.I.C.R.O.S~1\O.f.f.i.c.e.1.6\G.R.O.O.V.E.E.X...D.L.L..P!...])...%p.r.o.g.r.a.m.f.i.l.e.s%\m.i.c.r.o.s.o.f.t..o.f.f.i.c.e.\o.f.f.i.c.e.1.6\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t..O.f.f.i.c.e..2.0.1.6...*...M.i.c.r.o.s.o.f.t..O.n.e.D.r.i.v.e..f.o.r..B.u.s.i.n.e.s.s..E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C::\P.R.O.G.R.A~1\M.I.C.R.O.S~1\O.f.f.i.c.e.1.6\G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t..C.o.r.p.o.r.a.t.i.o.n...8'8.D...C::\P.r.o.g.r.a.m..F.i.l.e.s\Co.m.m.o.n..F.i.l.e.s\M.i.c.r.o.s.o.f.t..S.h.a.r.e.d\O.F.F.I.C.E.1.6\m.s.o.s.h.e.x.t...d.l.l.@.....U/...%c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s%\m.i.c.r.o.s.o.f.t..s.h.a.r.e.d\o.f.f.i.c.e.1.6\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t..O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t..O.f.f.i.c.e..S.h.e.l.l..E.x.t.e.n.s.i.o.n..H.a.n.d.l.e.r.s.....1.6..0...4.2.6.6...1.0.0.1.....D...C::\P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\b8aa9d1a-c55d-4ca0-b604-46481ef1818e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7460389223230637
Encrypted:	false
SSDEEP:	384:jLg/vVIYJ5OjaN7rQvXt3o3pIHREG8brWB/XxQJ1Vkr+TmuZCtTfz4Op53Nm1ri:/lqV1q1Yg0ej7V5037+tKzNPx1
MD5:	E678DF1823305D8568D2CAAE9176D2C7
SHA1:	B94A79AA88B9EC5FA9AE07B8BA1B2C7E7E88CD52
SHA-256:	A58B14685949CA93E4D81553FCA7FEF818537305B7C140C05FE0BD40C5D9BADC
SHA-512:	BE6183AE79AF8C68BCCFB9737CBC0AD9E25570471CB507210C1401BEB99E241A5BABBA8BA533F7D6458A26F432CF733C6D343AA6B3534FCAA0B477A9BC408D8A
Malicious:	false
Reputation:	low
Preview:	0j.....*...C::\P.R.O.G.R.A~1\M.I.C.R.O.S~1\O.f.f.i.c.e.1.6\G.R.O.O.V.E.E.X...D.L.L..P!...])...%p.r.o.g.r.a.m.f.i.l.e.s%\m.i.c.r.o.s.o.f.t..o.f.f.i.c.e.\o.f.f.i.c.e.1.6\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t..O.f.f.i.c.e..2.0.1.6...*...M.i.c.r.o.s.o.f.t..O.n.e.D.r.i.v.e..f.o.r..B.u.s.i.n.e.s.s..E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C::\P.R.O.G.R.A~1\M.I.C.R.O.S~1\O.f.f.i.c.e.1.6\G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t..C.o.r.p.o.r.a.t.i.o.n...8'8.D...C::\P.r.o.g.r.a.m..F.i.l.e.s\Co.m.m.o.n..F.i.l.e.s\M.i.c.r.o.s.o.f.t..S.h.a.r.e.d\O.F.F.I.C.E.1.6\m.s.o.s.h.e.x.t...d.l.l.@.....U/...%c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s%\m.i.c.r.o.s.o.f.t..s.h.a.r.e.d\o.f.f.i.c.e.1.6\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t..O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t..O.f.f.i.c.e..S.h.e.l.l..E.x.t.e.n.s.i.o.n..H.a.n.d.l.e.r.s.....1.6..0...4.2.6.6...1.0.0.1.....D...C::\P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\63139fbe-b2b0-46a8-9a88-495f5a059f99.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A8331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCB9D2598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\f86ae616-600c-400d-8146-4898941be92c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRyKNgoldZ8GjCiUXZSk+QSVh85PxEalRVHmclD9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99FId9RBQYBVcaxInfL

MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCAS1EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0.. "0...*H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L]....3>/.....u.:T.7...(yM....?V.<?.....1.a...O?d.....A.H.. 'MpB..T.m..Vn Ip..>k. 1..n.<Fb..f.*Q1.....s..2..{*..6....Pp....obM..1.....b1.....(u^'z.....v.F.W.X4."*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r.%Z.vFm.9..5!..~g5...;t...]+A.....u...k...e...&...l.6r[yU...%f.....N..V....<+....l..){...z...}y.n..'').....,b....5.08K%..O.g..D.S.F5o..<(....>...f..X..l..2."l..w....7f ..~c.4.E.....0..0...*H.....0.....)'..b.*\$w\$.q&.]zF_2...;...?U...W...L1.2...R..#....W....c1k.\$W..\$.J....+M!Hz.n`U.I)N. b.l....{K@]6.LIP/....](A.....0.....l...).H....lQ.y.;MG.d..ix..#f.Z\$[.].]?...0K...t'i..s...Y..%Ky...0...{!+..~v;....J....Z....)(6...@?v;~..2..c....[0Y0...*H.=....*H.=....B.....r...2..+Y.l...k..bR.j5Sl..8.....H"i..l..`Q.{...FOD..0... !.A..L.+.=..kp.!1..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... Chrome".. },.. "app_name": {.. "message": "..... Chrome".. },.. "crawl_app_unavailable": {.. "message": ".....". },.. "crawl_connect_to_network": {.. "message": ".....". },.. "iap_unavailable": {.. "message": "..... Chrome".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgYGFoO8ZpU34+puiPmb03OyZnLAOfTYABK:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "crawl_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Iniciu la sessi. a Chrome.".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEI4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9

SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488! CB
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "crawl_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "crawl_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6iL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betaling i Chrome Webshop".. },.. "app_name": {.. "message": "Betaling i Chrome Webshop".. },.. "crawl_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i jeblikket".. },.. "crawl_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i jeblikket".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMICTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfqJ
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "crawl_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar..".. },.. "crawl_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her..".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWIOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152E0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8BE7D254F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40

Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... Chrome Web Store".. },.. "app_name": {.. "message": "..... Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "....." .. },.. "crawl_connect_to_network": {.. "message": "....." .. },.. "iap_unavailable": {.. "message": "....." .. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed." .. },.. "please_sign_in": {.. "message": "..... Chrome" .. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "crawl_app_unavailable": {.. "message": "App currently unavailable." .. },.. "crawl_connect_to_network": {.. "message": "Please connect to a network." .. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable." .. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed." .. },.. "please_sign_in": {.. "message": "Please sign into Chrome." .. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "crawl_app_unavailable": {.. "message": "App currently unavailable." .. },.. "crawl_connect_to_network": {.. "message": "Please connect to a network." .. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable." .. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed." .. },.. "please_sign_in": {.. "message": "Please sign into Chrome." .. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlBGGHlB+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdIVo03OyZnLAOfTY6xjD:1HEVaC6WYpcDeEFxq8ZpNI5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B629CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. }... "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. }... "crawl_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento..".. }... "crawl_connect_to_network": {.. "message": "Con.ctate a una red..".. }... "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento..".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. }... "please_sign_in": {.. "message": "Inicia sesi.n en Chrome..".. }..}..
----------	--

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYPuU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEVaC6WYpcDeEFxq8Zp4LIOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. }... "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. }... "crawl_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento..".. }... "crawl_connect_to_network": {.. "message": "Con.ctate a una red..".. }... "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible..".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. }... "please_sign_in": {.. "message": "Accede a Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYPuU34ZeZz+dgRW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqIWYPtEObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. }... "app_name": {.. "message": "Chrome'i veebipoe maksed".. }... "crawl_app_unavailable": {.. "message": "Rakendus pole praegu saadaval..".. }... "crawl_connect_to_network": {.. "message": "Looge .hendus v.rguga..".. }... "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval..".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. }... "please_sign_in": {.. "message": "Logige Chrome'i sisse..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYPuU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BED8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. }... "app_name": {.. "message": "Chrome Web Storen maksut".. }... "crawl_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. }... "crawl_connect_to_network": {.. "message": "Muudosta verkkoyhteys..".. }... "iap_unavailable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. }... "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfV:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "crawl_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpy8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AF4E046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "crawl_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "crawl_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\hi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA755F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome".. },.. "app_name": {.. "message": "Chrome".. },.. "crawl_app_unavailable": {.. "message": "..... ..".. },.. "crawl_connect_to_network": {.. "message": "..... ..".. },.. "iap_unavailable": {.. "message": "..... ..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\hr\messages.json

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

File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D096E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. }... "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. }... "craw_app_unavailable": {.. "message": "Aplikacija trenutno nije dostupna".. }... "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om".. }... "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenutno nije dostupno".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. }... "please_sign_in": {.. "message": "Prijavite se na Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVVJIGGVJi+WYpU34HpoO+dgMmfGijO8ZpU34Huo9O03OyZnLAOfTYBIAym:1HEVrk5WYpQzTug/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D56A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. }... "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. }... "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el".. }... "craw_connect_to_network": {.. "message": "K.r.j.k, csatlakozzon egy h.l.zathoz".. }... "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. }... "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA12
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. }... "app_name": {.. "message": "Pembayaran Chrome Webstore".. }... "crawl_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini".. }... "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan".. }... "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. }... "please_sign_in": {.. "message": "Harap masuk ke Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603

Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. }... "app_name": {.. "message": "Pagamenti Chrome Web Store".. }... "craw_app_unavailable": {.. "message": "App al momento non disponibile".. }... "craw_connect_to_network": {.. "message": "Collegati a una rete".. }... "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. }... "please_sign_in": {.. "message": "Accedi a Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AEAE551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome". }... "app_name": {.. "message": "Chrome". }... "craw_app_unavailable": {.. "message": "..... ..". }... "craw_connect_to_network": {.. "message": "..... ..". }... "iap_unavailable": {.. "message": "..... ..". }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. }... "please_sign_in": {.. "message": "Chrome". }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgH8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSI0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome". }... "app_name": {.. "message": "Chrome". }... "craw_app_unavailable": {.. "message": ".". }... "craw_connect_to_network": {.. "message": ".". }... "iap_unavailable": {.. "message": ".". }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. }... "please_sign_in": {.. "message": "Chrome.". }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1

SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "crawl_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "crawl_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\lv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfrYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF0
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "crawl_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "crawl_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.r.l.k. Chrome.".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\nb\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYID:1HEDIHlitWYpCYJ8ZpD1OGAOfrD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E7333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CF8EDC586E128ECBFC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "crawl_app_unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "crawl_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap_unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\nl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgIXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979564A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A7

Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "App momenteel niet beschikbaar.." },.. "crawl_connect_to_network": {.. "message": "Maak verbinding met een netwerk.." },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.." },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.." },.. "please_sign_in": {.. "message": "Log in bij Chrome.." }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\pl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHBI9+dgQUg6O8ZpU34bdbfilu03OyZnLAOfTYR5k:1HE5iVauIv6WYpIAyR8ZpxFiaOGAOfIC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299F6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.." },.. "crawl_connect_to_network": {.. "message": "Po..cz si. z sieci.." },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.." },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.." },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.." }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\pt_BR\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjlBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKIOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.." },.. "crawl_connect_to_network": {.. "message": "Conecte-se a uma rede.." },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.." },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.." },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.." }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\pt_PT\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpStnPIOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAD09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCa8C77FFFD808A2058602D3646FD8DAE2844406F24
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel".. },.. "crawl_connect_to_network": {.. "message": "Ligue-se a uma rede".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome".. }..}..
----------	---

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\ro\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.61125938671415
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344Hix2Z+dgVPIZO8ZpU34qT7hI3O03OyZnLAOFTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "cr aw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "crawl_connect_to_network": {.. "message": "Conectear.-te la o re.ea..".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be c ompleted..".. },.. "please_sign_in": {.. "message": "Conectear.-te la Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\ru\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSI3ZGG7OJHZMSI3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjTO3On:1HEIOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F6 32
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... Chrome".. },.. "app_name": {.. "message": "..... Chrome".. },.. "crawl_app_u navailable": {.. "message": ".....".. },.. "crawl_connect_to_network": {.. "message": ".....".. },.. "iap_unavailable": {.. "message": ".....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. },.. "please_sign_in": {.. "message": "..... Chrome..".. }.. }..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\sk\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.640777810668463
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOFTYCUAi0D:1HEI4G8WYpetPmD8ZpcH7aOGAOfzUeD
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F307E0C24F9EF2D18A9228EAF4DEDD9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59 D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. }.. "crawl_app_unavailable": {.. "message": "Aplik.cia moment.lne nie je dostupn..".. },.. "crawl_connect_to_network": {.. "message": "Pripojte sa k sieti..".. }.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be com pleted..".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\sl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	4.5101656584816885
Encrypted:	false
SSDEEP:	12:1HEJGcyymbZGgGcyymbZ+WYpU34OBOEtf+dgca1ZO8ZpU34GcQArERf03OyZnLh:1HE4cyY4TcyY8WYpNoWa1w8ZpQcQ6AfK
MD5:	3943FA2A647AECEDFD685408B27139EE
SHA1:	0129DD19D28373359530B3B477FE8A9279DABB7D
SHA-256:	18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
SHA-512:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC9D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "crawl_app_unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "crawl_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailable": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prijavite se v Chrome.".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\sr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	743
Entropy (8bit):	4.913927107235852
Encrypted:	false
SSDEEP:	12:1HEJssbdOGGssbdO+WYpU347xBP+dg cucO8ZpU34s1muP03OyZnLAOfTYzDYD:1HEKsb59sbTWYplx4Xud8Zpy1mNOGAOv
MD5:	D485DF17F085B6A37125694F85646FD0
SHA1:	24D51D8642CDC6EFD5D8D7A4430232D8CDE25108
SHA-256:	7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818
SHA-512:	0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... Chrome".....".. },.. "app_name": {.. "message": "..... Chrome".....".. },.. "crawl_app_unavailable": {.. "message": "..... ..".....".. },.. "crawl_connect_to_network": {.. "message": "..... ..".....".. },.. "iap_unavailable": {.. "message": "..... .."..... ..".....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... .. Chrome.".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\sv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	630
Entropy (8bit):	4.52964089437422
Encrypted:	false
SSDEEP:	12:1HEJJKmbGGJKmb+WYpU34OACwz+dgNPGFZO8ZpU34JgpXLSb03OyZnLAOfTYLdID:1HErMkaqMk6WYpTOcb8ZpDgdZOGAO8Y
MD5:	D372B8204EB743E16F45C7CBD3CAAF37
SHA1:	C96C57219D292B01016B37DCF82E7C79AD0DD1E8
SHA-256:	B8BA77E0089B0676545EC16D32468B727812B444F90B33A7A5B748E6C36C4388
SHA-512:	33640529E0D5DCC5CA4BDB0615A2818E8D26C6FCB7B3474C08AC3EB7B9DB40E1F0A79954ED20728CD47A686D2533DCBC76ABCBD917F8530C8DE8BBA68752E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalning via Chrome Web Store".. },.. "app_name": {.. "message": "Betalning via Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Appen .r inte tillg.nglig f.r tillf.llet.".. },.. "crawl_connect_to_network": {.. "message": "Anslut till ett n.tverk.".. },.. "iap_unavailable": {.. "message": "Betalning i appen .r inte tillg.ngligt f.r n.rvarande.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logga in i Chrome.".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\th\messages.json

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

File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	945
Entropy (8bit):	4.801079428724355
Encrypted:	false
SSDEEP:	24:1HEKa1dDa1/WYp6Ufi72SmlG8ZpyactrW2SAOGAOfvSLD:WK2DNYp6U4y3bpyLxwGFW
MD5:	83E2D1E97791A4B2C5C69926EFB629C9
SHA1:	429600425CB0F196DDD717F940E94DBD8BFF2837
SHA-256:	2FECA577F43D97BAEEA464741D585892103585208FD0A935B810A03BDCE83C88
SHA-512:	60A5928DAA8CB4341487F477C56B5A98B83EDE50E5F4F55A802E01FDDAB86F3E795D391953D3D9214552D14D3F58C5A183693C613720FC12FC387D7B8F9B9AB
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... Chrome". },.. "app_name": {.. "message": "..... Chrome". },.. "crawl_app_unavailable": {.. "message": ".....". },.. "crawl_connect_to_network": {.. "message": ".....". },.. "iapi_unavailable": {.. "message": ".....". },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.". },.. "please_sign_in": {.. "message": "..... Chrome".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\tr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	4.710869622361971
Encrypted:	false
SSDEEP:	12:1HEJY8YG9Y8+WYpU34wWT+dgGb0GO8ZpU34wryd7T03OyZnLAOfTYGbPKG:1HE0jWYpyRnG8Zpyr/OGAOfFPn
MD5:	2CEAE0567B6BB1D240BBAD690A98CA3B
SHA1:	5944346FBD4A0797B13223895995CAB58E9ECD23
SHA-256:	A7CB86F30C9C31FE5540282C308BA96ADB4EC16EF98C87129EB88105E5BEF5FC
SHA-512:	108A07C6D03D7178E8D0FFEF5349E0249A898D864964FED8757BD8A08BC1C6D9613F2A6C01AA34A6606127D1C6CE14C229FA02586677DBB060B85E3E845950E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Ma.azas .demeleri".. },.. "app_name": {.. "message": "Chrome Web Ma.azas .demeleri".. },.. "crawl_app_unavailable": {.. "message": "Uygulama .u anda kullan.lamaz".. },.. "crawl_connect_to_network": {.. "message": "L.tfen bir a.a ba.lan.n".. },.. "iapi_unavailable": {.. "message": "Uygulama .i .demeler .u anda kullan.lamaz".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. },.. "please_sign_in": {.. "message": "L.tfen Chrome'da oturum a..n".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\uk\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	720
Entropy (8bit):	4.977397623063544
Encrypted:	false
SSDEEP:	12:1HEJ7wLkSIXZGG7wLkSIXZ+WYpU34zb1Oy2P+dgSV1EjIT08ZpU347qtfP2CTW:1HElwEkK4uwEk8WYpd/dTV1e8Zptq5S
MD5:	AB0B56120E6B38C42CC3612BE948EF50
SHA1:	8B3F520E5713D9F116D68E71DAEED1F6E8D74629
SHA-256:	68ABA284751EB9C856032062EF9B1651E2A1E5CE5FDA0977FFC97D63BA7BED9E
SHA-512:	CD852A58217F739C1CD58567FF432D31A7AD3F68C884ABBA1DA95799BCD1545C6A5D3B06F319681C12B78AD0A709828DE4B22736316F148D21F5DB76A5BCCBF
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... Chrome".. },.. "app_name": {.. "message": "..... Chrome".. },.. "crawl_app_unavailable": {.. "message": ".....". },.. "crawl_connect_to_network": {.. "message": ".....". },.. "iapi_unavailable": {.. "message": ".....". },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. },.. "please_sign_in": {.. "message": "..... Chrome".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\vi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	695
Entropy (8bit):	4.855375139026009

Encrypted:	false
SSDEEP:	12:1HEJMAZrSFZGGMAZrSFZ+WYpU34WFHoz+dgdkizoO8ZpU34NFHoz03OyZnLAOfTU:1HEI4B8WYpAKytFZ8ZpXKMOGAOfd6D
MD5:	7EBB677FEAD8557D3676505225A7249A
SHA1:	F161B4B6001AAEAEAB246FF8987F4D992B48D47BE
SHA-256:	051F96ED874C11C4A13589B5F68964E4F5B03B52DDA223D56524F2CA23760C04
SHA-512:	74FD267CF7CE299FB8E7054605C3F651F057F676FF865082FA24F4916755456768DB0DA62DBC515D829B48AB1F9CFC8AD3E841DCBF1F194D5CB14C5335A192A0
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Thanh to.n tr.n c.a h.ng Chrome tr.c tuy.n".. }.. "app_name": {.. "message": "Thanh to.n tr.n c.a h.ng Chrome tr.c tuy.n".. }.. "crawl_app_unavailable": {.. "message": ".ng d.ng hi.n kh.ng kh. d.ng.".. }.. "crawl_connect_to_network": {.. "message": "Vui l.ng k.t n.i v.i m.ng.".. }.. "iap_unavailable": {.. "message": "Thanh to.n trong .ng d.ng hi.n kh.ng kh. d.ng.".. }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be compl eted.".. }.. "please_sign_in": {.. "message": "Vui l.ng ..ng nh.p v.o Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\zh_CN\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	5.210259193489374
Encrypted:	false
SSDEEP:	12:1HEJ01GG01+WYpU34zeHz+dgfO8ZpU34YKiO03OyZnLAOfTYB6U:1HEplWYplSv8Zp+JOGAOfa6U
MD5:	BB73BF561BB79F89D9BF7C67C5AE5C65
SHA1:	2FADD3A1959B29C44830033A35C637D0311A8C9C
SHA-256:	D804F2A040D21D7511EFD5213D8E1721D64964A1A0DBB48E21622CEEDC9D967E
SHA-512:	627D44CEF1FE5C5ABD598BD47FF5E22B9EFC1CF98DDE3868FA9E5896C134A0C9C055AC34EDDADAE56B6690E51AEA89965D38F770552A85C732CC796795DC68D2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome". }.. "app_name": {.. "message": "Chrome". }.. "crawl_app_unavailable": {.. "message": ".....". }.. "crawl_connect_to_network": {.. "message": ".....". }.. "iap_unavailable": {.. "message": ".....". }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. }.. "please_sign_in": {.. "message": "... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_locales\zh_TW\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	634
Entropy (8bit):	5.386215984611281
Encrypted:	false
SSDEEP:	12:1HEJ2j62GG2j62+WYpU34m7T+dgc8nOO8ZpU34mvIO03OyZnLAOfTYAuH:1HEuSZCWYpsStwP8ZpROGAOfCH
MD5:	5FF50C673CC0C661D615F0CFD0E6DCA0
SHA1:	60DFF98DEAB9C4746B288BDD9C94B3BCAE5EAA85
SHA-256:	C6F8C640F3353A7B9B1432A0C139C1AEEC40133800E6C9B467B63991AD660308
SHA-512:	361D62D91F4931C5F34092C9F2C6A5323D5EEB82A24E7ABE11F7817D8D66341C0ECAD4DCB4B10873920C8D6A3CC9F5704889E178EB2549001A9F62BEDF6C809
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome". }.. "app_name": {.. "message": "Chrome". }.. "crawl_app_unavailae": {.. "message": ".....". }.. "crawl_connect_to_network": {.. "message": ".....". }.. "iap_unavailable": {.. "message": ".....". }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. }.. "please_sign_in": {.. "message": "... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL_metadata\verified_contents.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	7780
Entropy (8bit):	5.791315351651491
Encrypted:	false
SSDEEP:	192:RktDNJ2Uzsl5KcASyoH+CouKP/iNGRo/oRHMIT:AZQflcsU
MD5:	0834821960CB5C6E9D477AEF649CB2E4
SHA1:	7D25F027D7CEE9E94E9CBDEE1F9220C8D20A1588

SHA-256:	52A24FA2FB3BCB18D9D8571AE385C4A830FF98CE4C18384D40A84EA7F6BA7F69
SHA-512:	9AE AFC3ECE295678242D81D71804E370900A6D4C6A618C5A81CACD869B84346FEAC92189E01718A7BB5C8226E9BE88B063D2ECE7CB0C84F17BB1AF3C5B1A31C4
Malicious:	false
Reputation:	low
Preview:	[{"description":"","treehash_per_file":"","signed_content":{"payload":"","eyJjb250ZWZ0X2hhc2hlcyl6W3siYmxvY2tfc2I6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2liwiZmlsZXMiOiIt7InBhdGgiOiJfbG9jYWxlcY9iZy9tZXNzYWdlcy5qc29uliwicm9vdF9oYXNoljoiZHUtdGRPdUNWcmxkY254Q0poRkg2NXpLU05vb1RiUE56bDNHbz dRMGJ3SSJ9LHs icGF0aCI6Ii9sb2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJ6ZGtWafF9XdkxJWl hkc2VzWHBvSHNRMGh1ZGtSM2d1QIMzb2VsTEZLNkVIn0seyJwYXRoljoiX2xvY2FsZXMvY3MvbWVzc2FnZXMu anNvbilsInJvb3RfaGFzaCI6Ik9nUkNlZlVoam9xOU93NHFFaEhvTTQxNzNmElJyYkVpUVdsRXNRSzhscFkifSx7InBhdGgiOiJfbG9jYWxlcY9kYS9tZXNzYWdlcy5qc29uliwicm9vdF9oYXNoljoiN2JVWW1LYkhQUUNRMXBGcmUzTHJySEhwWk9xN1c2Zk5hT0laWmdKUERTTSJ9LHsicGF0aCI6Ii9sb2NhbGVzL2RIL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJOV3FkU3Rfc1NFMm9KT2VuSUZtM0pMRm9iOGtBZ3ZTa3RtZGpCRGJWazdBIn0seyJwYXRoljoiX2xvY2FsZXMvZ3MvWVzc2FnZXMu anNvbilsInJvb3RfaGFzaCI6ImgyaEZ0YUJ0LXJQUeToUm00QkFWM0VEZmhFbnh5MEIGOVhYT3Z0aHhINjAi fSx7InBhdGgiOiJfbG9jYWxlcY9lbi9tZXNzYWdlcy5qc29uliwicm9vdF9oYXNoljoiD0pSZDFmM3NxMERFVJTLHX d

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\craw_background.js	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	544643
Entropy (8bit):	5.385396177420207
Encrypted:	false
SSDEEP:	6144:abyfBNC2FRdjirXqbe5Dq31IVIMqX+wd5/CcMMJcRULt0NjyTOEzZQ+h72W3GB0n:F/tg
MD5:	6EEBED29E6A6301E92A9B8B347807F5F
SHA1:	65DFB69B650560551110B33DCBA50B25E5B876DE
SHA-256:	04CD9494B0ED83924DAD12202630B20D053D9E2819C8E826A386C814CC0A1697
SHA-512:	FEDE6DB31F2AD242E7BC7B52A8859BA7F466A0B920A8DADC32DCF5B2A2742E98B767FF22E0C5BC5C11FEC021240AA9E458486C9039EB4EBE5CF6AF7BE97BF2
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.defineProperty?Object.defineProperty:function(a,b,c){if(a==Array.prototype a==Object.prototype)return a;a[b]=c.value;return a};e.getGlobal=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object")};e.global=e.getGlobal(this);e.IS_SYMBOL_NATIVE="func

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\craw_window.js	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	261316
Entropy (8bit):	5.444466092380538
Encrypted:	false
SSDEEP:	3072:I5vU7I6s2M9dulWFCbmYJ4tnFWdqpMad2vywhlp81QFv9F9nNsZgiDdOFIV/mZmc:I5vqFCb2p8Gx9FNNsZ9Dd/ceR
MD5:	1709B6F00A136241185161AA3DF46A06
SHA1:	33DA7D262FFED1A5C2D85B7390E9DBC830CBE494
SHA-256:	5721A4B3F8E09C869A629EFFD350B51C9D46F0AC136717D4DB6265C0EE6F9AC8
SHA-512:	26835B4C050F53AD2DDB84469DF9A84BBB2786A655AB52DFC20B54BEDCB81D1ECD789198D5B7D8B940242E5CEAC818A177444D02397AE82C203438C4B1D15CB
Malicious:	false
Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var b,k,k {};k.scope={};k.createTemplateTagFirstArg=function(a){return a.raw=a};k.createTemplateTagFirstArgWithRaw=function(a,c){a.raw=c;return a};k.arrayIteratorImpl=function(a){var c=0;return function(){return c<a.length?{done:!1,value:a[c++]},{done:!0}}};k.arrayIterator=function(a){return{next:k.arrayIteratorImpl(a)}};k.makeIterator=function(a){var c="undefined"!==typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return c?c.call(a):k.arrayIterator(a)};.k.arrayFromIterator=function(a){for(var c,d=[];!(c=a.next()).done;)d.push(c.value);return d};k.arrayFromIterable=function(a){return a instanceof Array?a:k.arrayFromIterator(k.makeIterator(a))};k.ASSUME_ES5=!1;k.ASSUME_NO_NATIVE_MAP=!1;k.ASSUME_NO_NATIVE_SET=!1;k.SIMPLE_FROUND_POLYFILL=!1;k.ISOLATE_POLYFILLS=!1;k.FORCE_POLYFILL_PROMISE=!1;k.FORCE_POLYFILL_PROMISE_WHEN_NO_UNHANDLED_REJECTION=!1;,.k.objectCreate=k.ASSUME_ES5 "function"==typeof Object.cre

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\css\craw_window.css	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1741
Entropy (8bit):	4.912380256743454

Encrypted:	false
SSDEEP:	24:LalZ74H+rMwJHwlodHRmxt3jiu1iu1RDpfeWIMI548wJHwDwCapt/VMYXj8Eq27K:Z+rMm71le88S1tWYXmrVZFh
MD5:	67BF9AABE17541852F9DDFF8245096CD
SHA1:	A4AC74DD258E8E0689034FAA1B15A5C7C56DC3BB
SHA-256:	10DFBD2D98950B79EE12F6B8E3885AABE31543048DE56AD4FC0A5E34D0D9D4EC
SHA-512:	298FA132C6F122798FDB9BC6DE8024915147ADC20355B56A92F0ED9ACCE4549BE6E7F42212E07DCA166E31624D4E66E299565845D4BA1C51CA935050641B61F
Malicious:	false
Reputation:	low
Preview:	html, body { . margin: 0;. overflow: hidden;}.webview { . width: 100%;. height: 100%;. min-height: 100%;. position: absolute;}....crawl_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;}....crawl_overlay img { . margin: 16px;}.#loading_overlay { . opacity: 1;}.#offline_overlay { . opacity: 0;. display: none;}.#offline_overlay > img { . -webkit-filter: saturate(0%);}.#offline_overlay > span { . font-family: 'Open Sans', 'Deja Vu Sans', Arial, sans-serif;. font-size: 15px;. line-height: 21px;. color: #8d8d8d;. display: block;}.#loading_splash { . width: 128px;. height: 128px;}.#drag_overlay { . position: absolute;. left: 0;. top: 0;. right: 0;. bottom: 0;. pointer-events: none;. -webkit

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\html\crawl_window.html	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	810
Entropy (8bit):	4.723481385335562
Encrypted:	false
SSDEEP:	12:hYenuEJlig5fRpvV4AEdN2sAAuzg/7RwQuLYpUH9KfRnQBGgZKy3QGgjPSWZDQL:hYeLJKTVNEuLAuzg/twQucpS9bj3
MD5:	34A839BC40DEBC746BBD181D9EF9310C
SHA1:	8B4EAA74D31EED5B0BABA3CA5460201F6B10DA46
SHA-256:	BB8742615E4CD996AE5D0200E443AE6A6F0B473255F03AFFDB8FB4660DE4554D
SHA-512:	EE81E5509CBC2CB2B6C834224688C1E1B1AA9AA3866C52F8EAED040D5C390653C52D8D681E2E2CF62906643962ABAC823D5B622385B983B21E0DCCAFDF281F
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <link href="/css/crawl_window.css" rel="stylesheet">. <script src="/crawl_window.js"></script>. </head>. <body>. <webview></webview>. <div class="crawl_overlay" id="loading_overlay">. . . </div>. <div cl ass="crawl_overlay" id="offline_overlay">. . . . </div>. <div id="drag_overlay"></div>. <div id="top_bar">. <div id="close_button">. . </div>. <div id="maximize_button">. . </div>. </div>. </body>.</html>.

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\flapper.gif	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 30 x 30
Category:	dropped
Size (bytes):	70364
Entropy (8bit):	7.119902236613185
Encrypted:	false
SSDEEP:	768:g5TXOSBAqNIPmA8NcjCWdM0VFMJEwawTeElfWupav5TXg7wV+irIPny9MTVQHydi:g5KSmilPmAHzWiMsDfWug7DmqM6HybkF
MD5:	398ABB308EEBC355DA70BCE907B22E29
SHA1:	CFFB77B8A1724B8F81D98C6D6AD0071D10162252
SHA-256:	2B73533F47A99FEEA9CC405FFAFA9C4C53623F62487AEBFBA415945120B22040
SHA-512:	FC7A56FC8A61A582161874B5ADBAD30A84840190008EDB0B6FBF84F91393CA58E988E3FE446F11A0C3C691C18249B93AEC2904B3D0C4F0857D79034F662385A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....!.NETSCAPE2.0.....9::h0.bT(6.!!&.("g*k..JL1.[...o. .(..B(6.."...Z.CUyh0.....j.C.z8..S.....2.T'...Q..4 g]!\$ueW.Ny Q.lo!AoF#9h>7.0t..%.,,.@.m4..7.!.....9::h0.bT(6.!!&.("g*k..JL1.[...o. .(..B(6.."...Z.CUyh0.....j.C.z8..S.....2.T'...Q..4 g]!\$ueW.NyQ.lo!AoF#9h>7.0t..%.,,.@.m 4..7.!.....'.w=.....\)._6.k.OF...n.#!~"....2b3..I)..eu.Q.`e.....gr.?>.s.I0.....@.~.Tr.[8.+.,;.EE....S.*f....., ..B8/D...;9.q.....ukC...r.I...j.....BGY...o2J....+O4....X4.....cH%7....I....0H! !.....!.....p8.a\$....hh@.4....X,A.O.L..(.....JX.j.....z.X.Q....jB.d....B..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\icon_128.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4364
Entropy (8bit):	7.915848007375225
Encrypted:	false

SSDEEP:	96:YjILDJjTvXUtNvX8dgb9HT6y8nviiyHG5iCRYtiIP:YtNTfUzvX8KM+MGRsIP
MD5:	4DBC9F9E6F5A08D299BAC9E54DF07694
SHA1:	BB38F5DE34B1E0BE1109220BA55271087A4D9EA5
SHA-256:	91C2718DD23B4356D71F88F6146868369033291086DF327534546DFA459BEB0E
SHA-512:	A5F2B1F47502836130D8083F757B7773C1E1CB36B76AD298C29AB2B428C8002D2F15BD839838FC326DAC3681C2F48AB25A3E7631D33726C4B25E8EC14170915
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a.....IDATx..yp.....gF#.: [H.I.I..8...Ÿ.k.....!a7Km...E...Te..T.....J...p....%.(....+...3....eY.e...L.o...5....h4...\\....{?....~.u.`0.....`0.....`Y.....[(.....).4....a i..w38.+....Bf././..]{.....8...3.....3W~OJ.. /...u6V.C..U.0.+...=c..9.X.?.....L.....S@L...m.0..>.C..L TF.p5..f4M.,V...8..a.<...RP..@)E,..E"...h.....!...~....,l..T.....m..._[[{w{{.... {*^.....M.x..h4.h....\R.E....j).7.....h4.A.E....., ..iii.Vj?2...=/B.FK9P..@)=Rj..D".Y...2.B..x.)0...&J..2.....f.O..e.H.....!J)"I..R....B.....QJ;K..L..L".L~mhh.R.@).FFF ~.L&...~.B.....u.....}{.....~.....f..yUU.....^M...6.....j.,w.e.~!\$.C.R.....E(%e9.....k..@...W8.....@.....O..@%~..@.S..P.....Tp...."?ME..c.....S...`S1...7.b.. aNE..k...3.yP.}.Ch.}.....B.....IPE..C.<....T...k.....Z..o_.....g.....P..A=y.J.)h..@.q.-*]AU.4...F.M.....y%Bj+ \~..9.....:..=...r....E]o...F..P.....i...j....

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\icon_16.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	558
Entropy (8bit):	7.505638146035601
Encrypted:	false
SSDEEP:	12:6v/7vyVgSKYsfFzXxXsrPfA+b0YX+5IOUWCQKznuow7:6yVnKYsFzHxsrIq0YXmgQGn6
MD5:	FB9C46EA81AD3E456D90D58697C12C06
SHA1:	5FC450F7D73CCFAC8F0D818CB3392BA4D91B69DE
SHA-256:	016CA659BA080E194FBFC0929602B16506ED60AA6019FAA51410C4FD93B583E8
SHA-512:	ADD810EE9EB7CAEC505B5FD90A1F184CE39D8F8C689DCC240F188FE353B9575489492E07D572A3B1C11A1555CE66AFCa5134903E4C1AA3D54BC7C5ED3E65B50C
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a.....IDAT8...Mk.Q...;... ..F..QW.....F...J?.w..7~.....'Q.Bj... ..QS...M&_w..b&.]`.....p...f?.D\$.y^.....y*...\\..Z..t6..oRj.@&.u..G.qN).t.-V*.>{.N .EpjwFk.60o.J0.'Y..cT..Y.Tb. DF.d..s.Z..E..9.4._C.....%.*.^....4.l...Y..X..R.../...Wj+w0[j.._B.k.\$[\\>.%.....lz .w.ALxo.2;..a..".p..S..&..uXS...<..6.[..zD..._N+w.WbM7y e6X<...'(=r)}.....\$.f..5..P....k..."..8.s.<zgSm@.....).Y.....e..j]....F...l..A\$......T?.....m....8.....N...Z.....V..vd.h'....C.?.....H.:j..C.M.....9.b.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\topbar_floating_button.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.475799237015411
Encrypted:	false
SSDEEP:	3:yionv//thPI3xWrA4RthwkBDsTBZtnAkx/RPJdMv7bScsP4a9zn94FptVp:6v/lhPKM4nDspnAkZJNmgPdlN2TTp
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.}'.> %O...V!s...../...`<..`.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\topbar_floating_button_close.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	252
Entropy (8bit):	6.512071394066515
Encrypted:	false
SSDEEP:	6:6v/lhPKM4nDsp7q1hKVlomsj9rxKNgtmN0VZ+GFYep:6v/7iMXVq1yIxmNgmtKVnYM
MD5:	0599DFD9107C7647F27E69331B0A7D75
SHA1:	3198C0A5F34DB67F91A0035DBC297354CBC95525
SHA-256:	131817CD9311C03DF22D769DD2AD7FA2E6E9558863A89F7E5E1657424031A937
SHA-512:	0076ACB9D6A886BD987876E49495038F9388B292A9EFE5C9093CCA64CA3692E3A5D24E35172C7697F6AAE34B86CA217EE59C003423E46D9499BD27EC7D777A64

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.l.r..m.R..{.....`.f...#x.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\topbar_floating_button_hover.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.423186859407619
Encrypted:	false
SSDEEP:	3:yionv//thPI3xWrA4RthwkBDsTBZtnAkx/9IVtEHxrPLyN+ltNPhv/l2up:6v/lhPKM4nDspnAkZHVtERrPLyglitNPn
MD5:	7CB6B9DC1A30F63B8BD976924B75AD96
SHA1:	0C40B0C496D2F2B5F2021C117EC8610AC03AB469
SHA-256:	721B7AAA9A42A54A349881615A12E3A26983ACA48E173FD2F66E66AA0D725735
SHA-512:	4764937364E355956B242B84010AC56102536D2AACBE4227F0E88E4DE7AB468571957EA6C33012539156E5349AE4F777115615AE3361F60ADDF9CD227424F76A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ..szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...A..0...+B.z.s...*.....\$.<u..[.....h.....C.CA).....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\topbar_floating_button_maximize.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	166
Entropy (8bit):	5.8155898293424775
Encrypted:	false
SSDEEP:	3:yionv//thPI3xWrA4RthwkBDsTBZtttd//HmnFz1P/ZjXIUTqyCic30ltK1p:6v/lhPKM4nDsptF/HOP/ZjXIUeyCo/p
MD5:	232CE72808B60CBE0F4FA788A76523DF
SHA1:	721A9C98C835D2CD734153BBE07833C6637ECD68
SHA-256:	AFA4EA944CBDEC8543242E627EF46D5BFD3766DCAC664E7E50CDEEF2B352740C
SHA-512:	4048EEA5A78DD569521C488C4CE4F7B77AC0454C92EE9107A81A1B3AF91A4EE036039AC1A0A6B8DD26B12E7F1595DB80B7FAA7B6A25D9032BF385528A81A8654
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ..szz.....tEXtSoftware.Adobe ImageReadyq.e<...HIDATx.....0.CQS.....~..."......m.v+Sq....<!...M8m...'....@\$..0....E.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\images\topbar_floating_button_pressed.png	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.46068685940762
Encrypted:	false
SSDEEP:	3:yionv//thPI3xWrA4RthwkBDsTBZtnAkx/9IVtEXIyN+ltN1/lsg1p:6v/lhPKM4nDspnAkZHVtEZglitN1eup
MD5:	E0862317407F2D54C85E12945799413B
SHA1:	FA557F8F761A04C41C9A4BA81994E43C6C275DBB
SHA-256:	5C10CE0589EB115600F77381130B70AE0B7B3752614D86D4C89E857658AA222B
SHA-512:	07CB69327961FD0019BEF8EF7590B5524905AC373A815F73F6D9E0B26840929F919A96CAA977D4B5656704DACD0F352D568FB3997F80EE6BB94C95B58839DBFE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ..szz.....tEXtSoftware.Adobe ImageReadyq.e<...BIDATx...A..0...+B..@wu...*.....\$.<u..[.....h.....M..x(...IEND.B`.

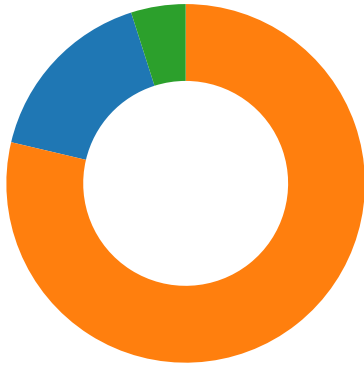
C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\CRX_INSTALL\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	1322
Entropy (8bit):	5.449026004350873
Encrypted:	false
SSDEEP:	24:1HEis7V/C/yox/fiqeUoLFmF1s80FKrGfd0d3NZNZx1Fq7eY7nfj1B:WL7V2opIV1mvs8rxTZRczhB
MD5:	01334FB9D092AF2AA46C4185E405C627
SHA1:	47AD3C0E82362FFE5B881DF8D71D6F79AB7F5796
SHA-256:	F52714812D68C577A445169D11E84DF6751C2D6886BC429643072BB5D61C6C27
SHA-512:	888D96ADB7A847ABE472145258C8C46950EB2FA3BA7D596C2E90A17C8FB06FD0155C56CC8ABA5D076D89368417464BCB2D236F9E40E53241950A01F9F8ED546F
Malicious:	false
Reputation:	low
Preview:	{.. "app": {.. "background": {.. "scripts": ["craw_background.js"].. }.. }.. "default_locale": "en".. "description": "__MSG_APP_DESCRIPTION__".. "display_in_launcher": false,.. "display_in_new_tab_page": false,.. "icons": {.. "128": "images/icon_128.png".. "16": "images/icon_16.png".. }.. "key": "MIGfMA0GCsSgGSib3DQEBABQAA4GNADCBiQKBgQCkFmLqViEyokd1wk57FxJtW2XXpGXzIHBzv9vQI/01UsuP0IV5/lj0wx7zJ/xciBUgDelxobvv9XD+zO1MdjMWuqJFcKuSS4Suqkje6u+pMrTSGOSHq1bmBVh0kpToN8YoJs/P/yrRd7FEtAXTaFTGxQL4C385MeXSjaQfiRiQIDAQAB".. "manifest_version": 2,.. "minimum_chrome_version": "29".. "name": "__MSG_APP_NAME__".. "oauth2": {.. "auto_approve": true,.. "client_id": "203784468217.apps.googleusercontent.com".. "scopes": ["https://www.googleapis.com/auth/sierra", "https://www.googleapis.com/auth/sierrasandbox", "https://www.googleapis.com/auth/chromewebstore", "https://www.googleapis.com/auth/chromewebstore.readonly"].. }..

C:\Users\user\AppData\Local\Temp\scoped_dir1740_2048838617\f86ae616-600c-400d-8146-4898941be92c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRyKNgoldZ8GjJCiUXZSk+QSVh8PxEalRVHmclD9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99FId9RBQYBVcaxInfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFC451EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
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 lp..>k.]1..n.<Fb..f..*Q1.....s..2..[*..6....Pp....obM...1.....b1.....(u^,'z....v.F.W.X4."*eu...b.....\..Fl...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..j..{...z...}y.n.'..').....,b...5.08K%..O.g..D.S.F5o..<(....>...f..X..l..2."l...w....7f]~.c.4.E.....0..0...*H.....0.....)'..b.*\$w\$&.q&.]zF_2...;...?..U...W...L1.2...R...#...W....c1k.\$W...\$.J....+M!.Hz.n'U.I)N. b.l...{.K@]6.LIP/....](A.....l...).H...IQ.y;MG.d..ix..#f.Z\$[...]?...0K...t'i.s...Y..%Ky....0...{!+.-v.;...J....Z...).(6..@?V;.-.2..c....[0Y0...*H.=...*H.=...B.....r...2..+Y.l...k..bR.j5Sl..8.....H"i.-l..`Q {...F0D. .0...!..A..L.+.=...kP.l.1..

Static File Info
 No static file info

Network Behavior
Network Port Distribution
Total Packets: 61 53 (DNS) 443 (HTTPS) 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:10:58.538089991 CEST	49732	80	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.539216042 CEST	49733	80	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.545274019 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.545315981 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:58.545401096 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.545624018 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.545651913 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:58.551842928 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.551892996 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.551980019 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.552206993 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.552223921 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.563539028 CEST	80	49732	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.563661098 CEST	49732	80	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.563977003 CEST	49732	80	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.564176083 CEST	80	49733	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.564269066 CEST	49733	80	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.589231014 CEST	80	49732	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.589277983 CEST	80	49732	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.589365005 CEST	80	49732	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.597846031 CEST	49736	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.597889900 CEST	443	49736	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.597970963 CEST	49736	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.599469900 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.601097107 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.601133108 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.601370096 CEST	49736	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.601398945 CEST	443	49736	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.601967096 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:58.602031946 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.602113962 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.602310896 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.602365971 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:58.604192019 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:58.604300022 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.604373932 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.604417086 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.632172108 CEST	49732	80	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.667814016 CEST	443	49736	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.668286085 CEST	49736	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.668329954 CEST	443	49736	95.168.170.165	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:10:58.669703960 CEST	443	49736	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.669795990 CEST	49736	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.818675995 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.818883896 CEST	49736	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.819021940 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.819041967 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:58.819232941 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.819258928 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:58.819281101 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.819577932 CEST	443	49736	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.828591108 CEST	49736	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.828624010 CEST	443	49736	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.829128027 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.829155922 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.855303049 CEST	443	49736	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.855401039 CEST	49736	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.858648062 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.858757019 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.858794928 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.858825922 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.858902931 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.860023975 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.861000061 CEST	49735	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:10:58.861030102 CEST	443	49735	142.250.186.174	192.168.2.3
Jun 26, 2022 09:10:58.865081072 CEST	49736	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:58.865108967 CEST	443	49736	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:58.867438078 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:58.867542982 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.867573977 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:58.867764950 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:58.867844105 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.869842052 CEST	49734	443	192.168.2.3	142.250.185.109
Jun 26, 2022 09:10:58.869868040 CEST	443	49734	142.250.185.109	192.168.2.3
Jun 26, 2022 09:10:59.107825994 CEST	49740	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:59.107880116 CEST	443	49740	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:59.107959986 CEST	49740	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:59.111529112 CEST	49740	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:59.111560106 CEST	443	49740	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:59.166053057 CEST	443	49740	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:59.167174101 CEST	49740	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:59.167215109 CEST	443	49740	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:59.167886019 CEST	443	49740	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:59.168401003 CEST	49740	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:59.168536901 CEST	49740	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:59.168548107 CEST	443	49740	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:59.168637037 CEST	443	49740	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:59.217395067 CEST	443	49740	95.168.170.165	192.168.2.3
Jun 26, 2022 09:10:59.217808008 CEST	49740	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:59.222327948 CEST	49740	443	192.168.2.3	95.168.170.165
Jun 26, 2022 09:10:59.222358942 CEST	443	49740	95.168.170.165	192.168.2.3
Jun 26, 2022 09:11:04.042510986 CEST	80	49733	95.168.170.165	192.168.2.3
Jun 26, 2022 09:11:04.042661905 CEST	49733	80	192.168.2.3	95.168.170.165
Jun 26, 2022 09:11:04.548065901 CEST	49733	80	192.168.2.3	95.168.170.165
Jun 26, 2022 09:11:04.575550079 CEST	80	49733	95.168.170.165	192.168.2.3
Jun 26, 2022 09:11:07.291904926 CEST	80	49732	95.168.170.165	192.168.2.3
Jun 26, 2022 09:11:07.291975975 CEST	49732	80	192.168.2.3	95.168.170.165
Jun 26, 2022 09:11:08.707607031 CEST	49732	80	192.168.2.3	95.168.170.165
Jun 26, 2022 09:11:08.735383987 CEST	80	49732	95.168.170.165	192.168.2.3

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:10:58.457433939 CEST	56417	53	192.168.2.3	8.8.8.8
Jun 26, 2022 09:10:58.476977110 CEST	53	56417	8.8.8.8	192.168.2.3
Jun 26, 2022 09:10:58.509706020 CEST	57723	53	192.168.2.3	8.8.8.8
Jun 26, 2022 09:10:58.521287918 CEST	58116	53	192.168.2.3	8.8.8.8
Jun 26, 2022 09:10:58.527050972 CEST	53	57723	8.8.8.8	192.168.2.3
Jun 26, 2022 09:10:58.550796032 CEST	53	58116	8.8.8.8	192.168.2.3
Jun 26, 2022 09:11:03.099231005 CEST	53804	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:11:03.127708912 CEST	443	53804	142.250.186.174	192.168.2.3
Jun 26, 2022 09:11:03.128256083 CEST	53804	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:11:03.156296015 CEST	443	53804	142.250.186.174	192.168.2.3
Jun 26, 2022 09:11:03.156353951 CEST	443	53804	142.250.186.174	192.168.2.3
Jun 26, 2022 09:11:03.156392097 CEST	443	53804	142.250.186.174	192.168.2.3
Jun 26, 2022 09:11:03.156430960 CEST	443	53804	142.250.186.174	192.168.2.3
Jun 26, 2022 09:11:03.165472984 CEST	53804	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:11:03.167201042 CEST	53804	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:11:03.188879967 CEST	53804	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:11:03.189280033 CEST	53804	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:11:03.216728926 CEST	443	53804	142.250.186.174	192.168.2.3
Jun 26, 2022 09:11:03.217447996 CEST	53804	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:11:03.224924088 CEST	443	53804	142.250.186.174	192.168.2.3
Jun 26, 2022 09:11:03.225254059 CEST	443	53804	142.250.186.174	192.168.2.3
Jun 26, 2022 09:11:03.225285053 CEST	443	53804	142.250.186.174	192.168.2.3
Jun 26, 2022 09:11:03.225457907 CEST	53804	443	192.168.2.3	142.250.186.174
Jun 26, 2022 09:11:03.251569033 CEST	53804	443	192.168.2.3	142.250.186.174

DNS Queries							
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 26, 2022 09:10:58.457433939 CEST	192.168.2.3	8.8.8.8	0x6066	Standard query (0)	gossip-celeb-fashion.com	A (IP address)	IN (0x0001)
Jun 26, 2022 09:10:58.509706020 CEST	192.168.2.3	8.8.8.8	0xbc98	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jun 26, 2022 09:10:58.521287918 CEST	192.168.2.3	8.8.8.8	0xe67b	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)

DNS Answers									
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:10:58.476977110 CEST	8.8.8.8	192.168.2.3	0x6066	No error (0)	gossip-celeb-fashion.com		95.168.170.165	A (IP address)	IN (0x0001)
Jun 26, 2022 09:10:58.476977110 CEST	8.8.8.8	192.168.2.3	0x6066	No error (0)	gossip-celeb-fashion.com		213.227.145.147	A (IP address)	IN (0x0001)
Jun 26, 2022 09:10:58.476977110 CEST	8.8.8.8	192.168.2.3	0x6066	No error (0)	gossip-celeb-fashion.com		213.227.149.216	A (IP address)	IN (0x0001)
Jun 26, 2022 09:10:58.527050972 CEST	8.8.8.8	192.168.2.3	0xbc98	No error (0)	accounts.google.com		142.250.185.109	A (IP address)	IN (0x0001)
Jun 26, 2022 09:10:58.550796032 CEST	8.8.8.8	192.168.2.3	0xe67b	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jun 26, 2022 09:10:58.550796032 CEST	8.8.8.8	192.168.2.3	0xe67b	No error (0)	clients.l.google.com		142.250.186.174	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- accounts.google.com
- gossip-celeb-fashion.com
- clients2.google.com
- https:

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49734	142.250.185.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49736	95.168.170.165	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49735	142.250.186.174	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49740	95.168.170.165	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49732	95.168.170.165	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jun 26, 2022 09:10:58.563977003 CEST	746	OUT	GET / HTTP/1.1 Host: gossip-celeb-fashion.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-06-26 07:10:58 UTC	0	OUT	GET / HTTP/1.1 Host: gossip-celeb-fashion.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-26 07:10:58 UTC	1	IN	HTTP/1.1 404 Not Found Server: nginx Date: Sun, 26 Jun 2022 07:10:58 GMT Content-Type: text/html Content-Length: 548 Connection: close Vary: Accept-Encoding
2022-06-26 07:10:58 UTC	2	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49735	142.250.186.174	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-26 07:10:58 UTC	1	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-26 07:10:58 UTC	2	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-e1sXYgYQRDXB3ggNWN4ZQ' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Sun, 26 Jun 2022 07:10:58 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5655 X-Daystart: 658 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked

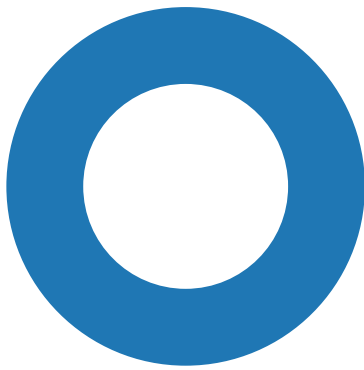
Timestamp	kBytes transferred	Direction	Data
2022-06-26 07:10:58 UTC	3	IN	Data Raw: 33 31 39 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 35 35 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 36 35 38 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 20 73 Data Ascii: 319<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5655" elapsed_seconds="658"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname="" s
2022-06-26 07:10:58 UTC	3	IN	Data Raw: 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 70 20 61 Data Ascii: kegccagldldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><app a
2022-06-26 07:10:58 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49740	95.168.170.165	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-26 07:10:59 UTC	5	OUT	GET /favicon.ico HTTP/1.1 Host: gossip-celeb-fashion.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://gossip-celeb-fashion.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-06-26 07:10:59 UTC	6	IN	HTTP/1.1 404 Not Found Server: nginx Date: Sun, 26 Jun 2022 07:10:59 GMT Content-Type: text/html Content-Length: 548 Connection: close Vary: Accept-Encoding
2022-06-26 07:10:59 UTC	6	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome

Statistics
Behavior

● chrome.exe
● chrome.exe



💡 Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 1740, Parent PID: 5044

General

Target ID:	0
Start time:	09:10:54
Start date:	26/06/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "http://gossip-celeb-fashion.com
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Completion	Count	Source Address	Symbol
-----------	------------	-------	----------------	--------

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

Registry Activities

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF7F62CFC4B	RegSetValueExW

Analysis Process: chrome.exe

PID: 5564, Parent PID: 1740

General

Target ID:	1
Start time:	09:10:56
Start date:	26/06/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,9784695222289147633,16330879895871495791,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1936 /prefetch:8
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Completion	Count	Source Address	Symbol
-----------	------------	-------	----------------	--------

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

Disassembly

No disassembly