

JOeSandbox Cloud BASIC



ID: 651265
Cookbook: browseurl.jbs
Time: 18:12:42
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report https://express.adobe.com/page/QSpEtjTBWEere/	5
Overview	5
General Information	5
Detection	5
Signatures	5
Classification	5
Process Tree	5
Malware Configuration	5
Yara Signatures	5
Sigma Signatures	5
Snort Signatures	6
Joe Sandbox Signatures	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
World Map of Contacted IPs	9
Public IPs	10
Private	10
General Information	10
Warnings	11
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASNs	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	12
C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	12
C:\Users\user\AppData\Local\Google\Chrome\User Data\27a016a7-313a-4fea-a06e-80fca7ef8ede.tmp	12
C:\Users\user\AppData\Local\Google\Chrome\User Data\4927f5c3-f8bb-4c84-8ee0-f02802047416.tmp	12
C:\Users\user\AppData\Local\Google\Chrome\User Data\709d8bb9-c17e-4afc-ac8c-0e3339de77a4.tmp	13
C:\Users\user\AppData\Local\Google\Chrome\User Data\7d5d964b-78f9-4f7f-9e77-a4ee97f78d45.tmp	13
C:\Users\user\AppData\Local\Google\Chrome\User Data\9892867c-905f-4b79-ac8a-f0602d4f01cc.tmp	13
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0a7047a5-3592-41e7-bd99-61fc42019fc1.tmp	14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2886b6ad-ab63-4799-91f8-40407181f0ae.tmp	14
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2ff535d1-fe6f-4d1e-baf3-76c5fff8fb99.tmp	15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3ef79956-b817-40ab-ac60-8c18be43cfc.tmp	15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8507cdbe-4b73-42d4-a942-ff7663b72b13.tmp	15
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8ae8b0bc-7794-4328-ba01-06743ae513fd.tmp	16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index (copy)	16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccgmgiada\1.0.0.6_0\metadata\computed_hashes.json	16
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	17
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcapaombhbimeihdjneigic\def\GPUCache\data_1	19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcapaombhbimeihdjneigic\def\Network Persistent State (copy)	19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcapaombhbimeihdjneigic\def\98b08b0-43d5-47e7-a74f-c8b2f493a9ef.tmp	19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgiada\def\0f25ce2b-a737-407c-8110-84d4234450ba.tmp	20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgiada\def\GPUCache\data_1	20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgiada\def\Network Persistent State (copy)	20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	21

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\82f5442-0663-4b36-b5be-9f40d0972250.tmp	21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6e43385-86df-4424-9082-4eaf1c861a4e.tmp	21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ff721e75-de78-4e39-83d4-ff11f3857379.tmp	22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	23
C:\Users\user\AppData\Local\Google\Chrome\User Data\6d5d7b4-b740-4436-98a3-8b8a825a6353.tmp	23
C:\Users\user\AppData\Local\Google\Chrome\User Data\dcca05ac-97f0-4ad6-9fb2-536ebdbde734.tmp	24
C:\Users\user\AppData\Local\Google\Chrome\User Data\380db3d-e053-4d07-825e-919efa7c09c7.tmp	24
C:\Users\user\AppData\Local\Temp\40212a03-e0ad-48db-b4a3-7035593adebd.tmp	24
C:\Users\user\AppData\Local\Temp\41be5f9c-4016-4134-bef8-2736450dabf5.tmp	25
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\41be5f9c-4016-4134-bef8-2736450dabf5.tmp	25
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\bg\messages.json	25
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\ca\messages.json	26
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\cs\messages.json	26
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\da\messages.json	26
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\de\messages.json	27
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\el\messages.json	27
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\en\messages.json	27
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\en_GB\messages.json	28
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\es\messages.json	28
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\es_419\messages.json	28
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\et\messages.json	29
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\fi\messages.json	29
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\fil\messages.json	29
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\fr\messages.json	30
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\hi\messages.json	30
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\hr\messages.json	30
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\hu\messages.json	30
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\id\messages.json	31
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\it\messages.json	31
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\ja\messages.json	31
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\ko\messages.json	32
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\lt\messages.json	32
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\lv\messages.json	32
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\nb\messages.json	33
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\nl\messages.json	33
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\pl\messages.json	33
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\pt_BR\messages.json	34
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\pt_PT\messages.json	34
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\ro\messages.json	34
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\ru\messages.json	35
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\sk\messages.json	35
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\sl\messages.json	35
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\sr\messages.json	36
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\sv\messages.json	36
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\th\messages.json	36
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\tr\messages.json	37
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\uk\messages.json	37
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\vi\messages.json	37
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\zh_CN\messages.json	37
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\locales\zh_TW\messages.json	38
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\metadata\verified_contents.json	38
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\craw_background.js	38
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\craw_window.js	39
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\css\craw_window.css	39
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\html\craw_window.html	39
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\images\flapper.gif	40
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\images\icon_128.png	40
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\images\icon_16.png	40
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\images\topbar_floating_button.png	41
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\images\topbar_floating_button_close.png	41
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\images\topbar_floating_button_hover.png	41
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\images\topbar_floating_button_maximize.png	42
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\images\topbar_floating_button_pressed.png	42
C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\manifest.json	42
Static File Info	43
Network Behavior	43
Statistics	43
Behavior	43
System Behavior	43
Analysis Process: chrome.exePID: 2492, Parent PID: 868	43
General	43
File Activities	43
Registry Activities	44
Key Value Modified	44
Analysis Process: chrome.exePID: 5716, Parent PID: 2492	44
General	44
File Activities	44
Disassembly	44

Windows Analysis Report

https://express.adobe.com/page/QSpEtjTBWEere/

Overview

General Information

Sample URL:

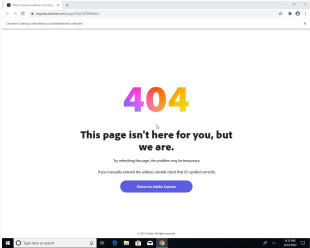
http://
https://express.adobe.com
/page/QSpEtjTBWEere/

Analysis ID:

651265

Infos:





Detection

MALICIOUS

SUSPICIOUS

CLEAN

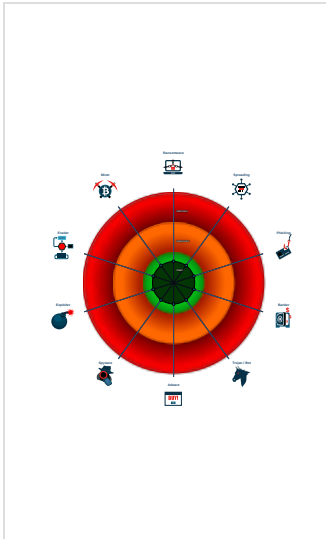
UNKNOWN

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

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 2492 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://express.adobe.com/page/QSpEtjTBWEere/ MD5: C139654B5C1438A95B321BB01AD63EF6)
 - chrome.exe (PID: 5716 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1548,3426159670808259283,2010510569848056573,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /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

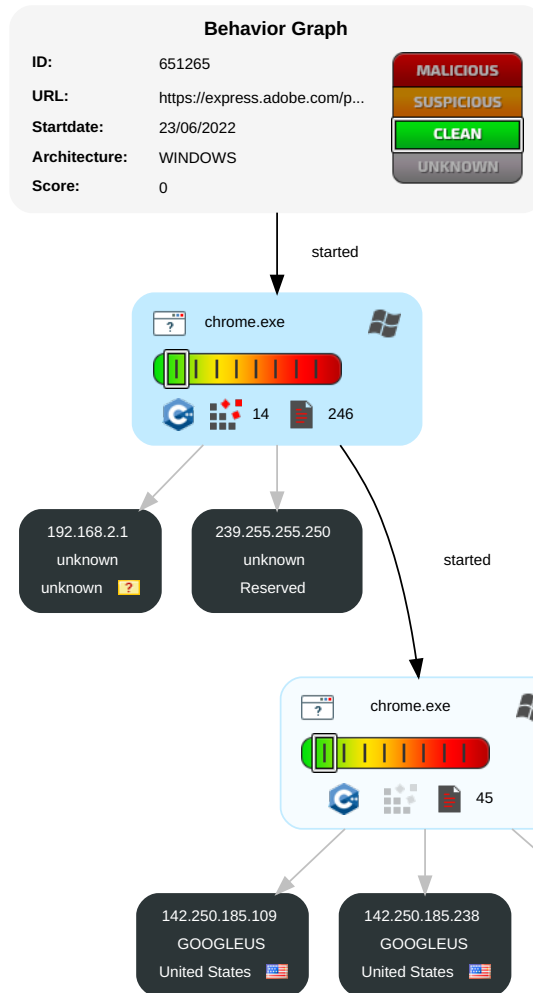
Joe Sandbox Signatures

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	Data Obfuscation	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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

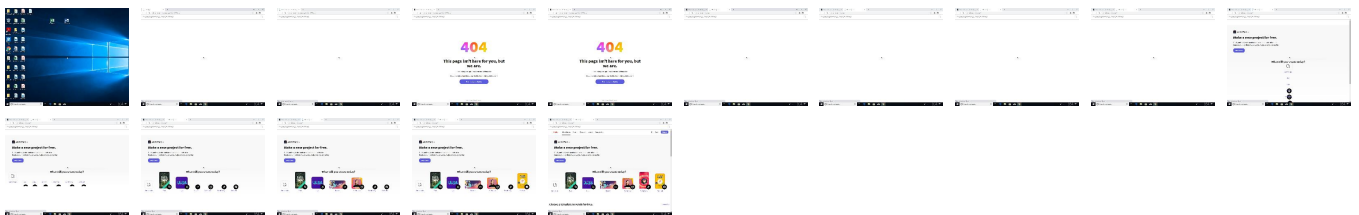
Behavior Graph

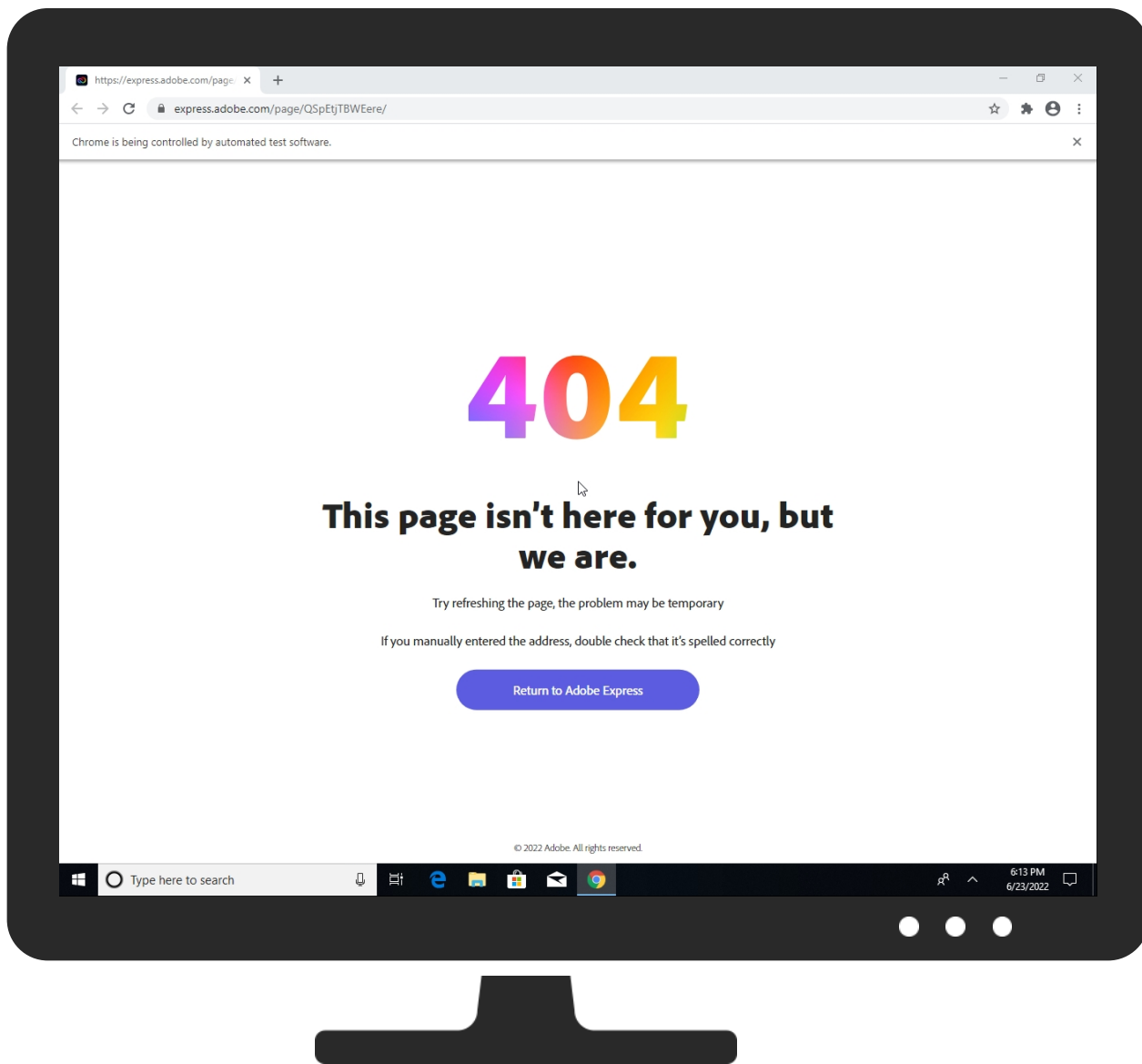


Screenshots

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://https://express.adobe.com/page/QSpEtjTBWEere/	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	

Domains and IPs

Contacted Domains

 No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com	e82f5442-0663-4b36-b5be-9f40d0972250.tmp.1.dr, f6e43385-86df-4424-9082-4eaf1c861a4e.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://dns.google	e82f5442-0663-4b36-b5be-9f40d0972250.tmp.1.dr, 0f25ce2b-a737-407c-8110-84d4234450ba.tmp.1.dr, a98b08b0-43d5-47e7-a74f-c8b2f493a9ef.tmp.1.dr, f6e43385-86df-4424-9082-4eaf1c861a4e.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	e82f5442-0663-4b36-b5be-9f40d0972250.tmp.1.dr, f6e43385-86df-4424-9082-4eaf1c861a4e.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://play.google.com	e82f5442-0663-4b36-b5be-9f40d0972250.tmp.1.dr, f6e43385-86df-4424-9082-4eaf1c861a4e.tmp.1.dr	false		high
http://https://accounts.google.com	e82f5442-0663-4b36-b5be-9f40d0972250.tmp.1.dr, f6e43385-86df-4424-9082-4eaf1c861a4e.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://clients2.googleusercontent.com	e82f5442-0663-4b36-b5be-9f40d0972250.tmp.1.dr, f6e43385-86df-4424-9082-4eaf1c861a4e.tmp.1.dr	false		high
http://https://apis.google.com	e82f5442-0663-4b36-b5be-9f40d0972250.tmp.1.dr, f6e43385-86df-4424-9082-4eaf1c861a4e.tmp.1.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.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://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://accounts.google.com/MergeSession	craw_window.js.0.dr	false		high
http://https://clients2.google.com	e82f5442-0663-4b36-b5be-9f40d0972250.tmp.1.dr, f6e43385-86df-4424-9082-4eaf1c861a4e.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	unknown	United States		15169	GOOGLEUS	false
13.225.239.122	unknown	United States		16509	AMAZON-02US	false
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
15.188.95.229	unknown	United States		16509	AMAZON-02US	false
52.215.98.143	unknown	United States		16509	AMAZON-02US	false
54.194.254.72	unknown	United States		16509	AMAZON-02US	false
13.225.239.31	unknown	United States		16509	AMAZON-02US	false
52.215.108.43	unknown	United States		16509	AMAZON-02US	false
142.250.185.238	unknown	United States		15169	GOOGLEUS	false
104.16.149.64	unknown	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private	
IP	
192.168.2.1	
127.0.0.1	

General Information	
Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651265
Start date and time: 23/06/2022 18:12:42	2022-06-23 18:12:42 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://express.adobe.com/page/QSpEtjTBWEere/
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:	20

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@27/96@0/13
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 • Browse: https://express.adobe.com/

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 142.250.185.142, 173.194.182.71, 173.194.187.73, 173.222.108.216, 173.222.108.232, 142.250.185.163, 80.67.82.195, 173.222.108.192, 80.67.82.194, 80.67.82.200, 23.211.4.169, 192.168.2.3, 23.35.236.237, 23.35.236.137, 142.250.185.67, 142.250.186.42, 173.194.182.70, 20.223.24.244
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.
- VT rate limit hit for: <https://express.adobe.com/page/QSpEtjTBWEere/>

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:	0D6803758FF87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
Malicious:	false
Reputation:	low
Preview:	BDic.....6....".Z..4g....{/...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 XGNDS.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 GM DS.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 GVMDS.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\27a016a7-313a-4fea-a06e-80fca7ef8ede.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):	204266
Entropy (8bit):	6.043012738207363
Encrypted:	false
SSDEEP:	3072:68bfiflHRF/F5TV+1C5V42Mqr0A+roO311FcbXafIb0u1GOJmA3iuR2:6Ayw/FWC/f3wbaqfllUOoSiuR2
MD5:	93EF2845556351356C8CA465736BB933
SHA1:	69381F57C46A083B40C34B2F8AEA3F2FF7A8675B
SHA-256:	C17EBD3C432B10E9DF9C77EDEFF9D335B440B560ED209647CEDF053D08EBAD6E
SHA-512:	8C91D5672540AA3B6DAE2A5BBB223E2DAFB7F6210A2ED158CFA5E966027A89E71CE24CED491CFF33CAD779CF62A32540C9E50A214D489FC6AC6657CD904BCD5B
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": "1.656033228632387e+12", "network": "1.656000829e+12", "ticks": "117620955.0", "uncertainty": "4110552.0" }, "os_crypt": { "encrypt_d_key": "RFBBUeKBAAAAOlyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAIAAAAAABBMAAAAAQAAIAAAABAL2tyan+IsWtxhoUVdUYrYiwg8lJkppNr2ZbBFie9UAAAAA6AAAAA9gAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRY.JjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdflljw4oXIE4R7I0AAAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBuHMXghJbDGB5WCu+JEdxaxLLxaYPp4zeP", "password_manager": { "os_password_blank": true, "os_password_last_changed": "13291230639324767", "plugins": { "metadata": { "adobe-flash-player": { "disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\4927f5c3-f8bb-4c84-8ee0-f02802047416.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7511422233425447
Encrypted:	false
SSDEEP:	384:9LAvDhSgtmNhVeETON7rgvXd3AfR8H14Gsbrmx7TxgFBlwrarmSWky9jzD8ONdbQ:daKFdul4goeHnIR4//CJKzhPdu
MD5:	8EBA9B56A6B9EC0BAC1E78E000D79C3F
SHA1:	10F9FFEAE878CF539AC0F040B768FE31941839A85
SHA-256:	8A8F281A0F188F315908D78D0C5CB7D27A5F63936E69B6466FFAFBC11F365C07
SHA-512:	DDA5CB4B402503A4E3BAD366A42FEFE5FF78B7B78615FB6F9D81482C938387FFBAE62D1B6A298F01A6F9AE9DDBEC80B68FAD0F9550967842EDF549AAAA8597BA

Malicious:	false
Reputation:	low
Preview:	.t.....*...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.Pl...])...%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.D...C:.\P.r.o.g.r.a.m..F.i.l.e.s\..C.o.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\709d8bb9-c17e-4afc-ac8c-0e3339de77a4.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):	212707
Entropy (8bit):	6.071004513572975
Encrypted:	false
SSDEEP:	3072:sla8bfiHHRF/F5TV+1C5V42Mqr0A+roO311FcbXafiB0u1GOJmA3iuR2:eaAyw/FWC/f3wbaqfllUooSiuR2
MD5:	1E471E11885CB3661BB9A8699ACBFF5E
SHA1:	938E29B4074984E8895A796B042FFB40EC60803F
SHA-256:	11D0AA865759F6440139BE18F4EAF5A8EAF1CC00424DC8C35FE5D31FEA413B28
SHA-512:	F19B372240C2B6FCF4CD047C71F9F3C17697F008F466D4EAB86CACE9B09C8D1062626B89B99E57772251649B9CD325319AF104D0F2A57D9CF549796145551B9F
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":1.656033228632387e+12,"network":1.656000829e+12,"ticks":117620955.0,"uncertainty":4110552.0}},"os_crypt":{"encrypt_e_d_key":"RFBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95Wkt94zTZqQ3WydzHLcAAAAAIAAAAAABBMAAAAAQAAIAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbFie9UAAAAA6AAAAAgAAIAAAABDv4gjlLq1dOS7kRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdflljw4oXIE4R7I0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGwCOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYpP4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639324767"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d5d964b-78f9-4f7f-9e77-a4ee97f78d45.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7511791886844374
Encrypted:	false
SSDEEP:	384:NLavDhSgtmNhVeETON7rgvXd3Afr8H14Gsbrmx7TxgFBlwrarmSVy9jzD8ONdbNU:NaKFdulYgoeHnlR4//CJkZhPdY
MD5:	80FF89DA13B8C92E96EAA4695F69667D
SHA1:	C2667479D0B78CB7B03631AB42CC5233B2BE6BCA
SHA-256:	E9B17EF57E3E0ACC39DB75A773EF586F787D98B23BCF5F9588F1596FAB62CA75
SHA-512:	5ACF1F0E3CEDAB09AC0EC625016E00874039347ACEF3EDF7DFDA486FFEE294BB12AE1E976C0429CB0388A3F4BEED18DACE9FBF074D6344368C2182EDE5054626
Malicious:	false
Reputation:	low
Preview:	.q.....*...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.Pl...])...%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.D...C:.\P.r.o.g.r.a.m..F.i.l.e.s\..C.o.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\9892867c-905f-4b79-ac8a-f0602d4f01cc.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):	212707
Entropy (8bit):	6.071005888016764
Encrypted:	false
SSDEEP:	3072:6Yd8bfiHHRF/F5TV+1C5V42Mqr0A+roO311FcbXafiB0u1GOJmA3iuR2:1dAyw/FWC/f3wbaqfllUooSiuR2
MD5:	08F3A0207E6F0E93C8335E0DD7C872D0
SHA1:	E6D232A4BB5797A34353D32BBDFOE64698F13644
SHA-256:	2F99E322A117D0892AFA881BA216E10B60A141199C4EC169F60BA2D4489B98B6

SHA-512:	427DFB17FAB885D3665E3A488D4E788061C4F10198A3DB1FF06F5645286667589306A8402F8695D99DC8D683B33AD7806A0CA41CB4324423C8BF21F35A562AE0
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":1.656033228632387e+12,"network":1.656000829e+12,"ticks":117620955.0,"uncertainty":4110552.0}},"os_crypt":{"encrypt_d_key":"","RFBBUeKBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAIAAAAAABBMAAAAAQAAIAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbFie9UAAAAA6AAAAAgAAIAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRY.JjDXn4W2fxYqQj2xYfYeAnS1vCL4JXAsdflljw4oXlE4R7l0AAAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGwcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"","13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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:+ftlE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89CF9B0734358FF432F2BC83338112DC7B830F9B30F2C
SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6CF
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0a7047a5-3592-41e7-bd99-61fc42019fc1.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):	17529
Entropy (8bit):	5.574591926804809
Encrypted:	false
SSDEEP:	384:08h2tkLlcvXn1kXqKf/pUZNCgVLH2HfDzrU3FZQk4A:bLIOn1kXqKf/pUZNCgVLH2HffrU30k3
MD5:	DB986ABB74C2C5D215EBBB93AA228B9C
SHA1:	305CDE7ADD1CE69EBE4D25100F6083E55EB6AC2D
SHA-256:	B3C48BA57DB965D9B8543DA976A7950D3F1849244328D7EC47713434C65872E5
SHA-512:	17B80DE0A0F300873E57E9EE25BE87221EEA882CB8159E4000F88412B459B8332833AE318B6CEFFB8DF9E1F9E04CD441AD421AE073714392FCB2CD56388A435
Malicious:	false
Reputation:	low
Preview:	{ "download": {"always_open_pdf_externally": true, "directory_upgrade": true, "extensions_to_open": "pdf:doc:docx:docm:docm:xls:xlsx:xlsxm:xslm:ppt:pptx:pptxm:pptm:mhtrft: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": {"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": "13300506826339114", "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\2886b6ad-ab63-4799-91f8-40407181f0ae.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):	5375
Entropy (8bit):	4.992268758915456
Encrypted:	false
SSDEEP:	96:n9Cja6fn1pKcILok0JC9RWL8uk+15bOTQVuw:n9CGm1pc049YPk+f
MD5:	07E3A6DBD6CD50C9B9A0E60D67B38F7F
SHA1:	4AF79B2EEDAD91D17E91EA0857452111A29ADFFB
SHA-256:	F1C28C04C2379CDCF5B281A1D9076D12E88B62A62850C51AAF45203BA3040A62
SHA-512:	7C7CA575AF9C25BC1D8875C62E4555210698DF05F78DF1DC7163577905120AFFFE0E57C5C633FD2B8CE7A7ABB78EFF60CB7A21A7D694AD562B73FDA73C2BF75B

Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf.doc.docx.docxm:docm.xls:xlsx.xlsxm:xslm:ppt:pptx:pptxm:pptm:mhtr: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":"13300506826339114","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\8ae8b0bc-7794-4328-ba01-06743ae513fd.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index (copy)	
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:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8/A7
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\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:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTWGb7V9Hne4qasKxXltnLG48gcLg/Pkl:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9C8BCFD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low

Preview:	{ "file_hashes": { ["block_hashes": ["A+1PYW3V6CJbBuQ7aqrqYhyH3bT8PKyBXp3hN2slpI0=", "WSOpQRkYTHjPSIG9Zrf2a7TNhy43NdcG1Zg5Nv0UbH0=", "jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRvIaY=", "LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6Rl=", "nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=", "wifibc1QfMBN2jrtUtLgScFevuceTpAatmLvul11RJA=", "dHjWISlIdji7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=", "zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTi=", "DpjXcO85FFFY9KJFPkGNfUtdQIOsGwO5jUckiUwY14=", "gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=", "prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CmJYqdhS=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFwN8EzCM=", "EPQ3jzdrLkAHyvf3920B5Y3aAkO1Jdn/UtbAmq6T0=", "+oOc6ca+ChKUpTu+oa2ZRxE+wG3QJmuYWEvYCs40NI=", "3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=", "1A9NNawxuhu95H5eThvf1rewJ4QQWWhhPNxJXO1C/n68=", "E3vWLQxzmj+e5QYbUscLJ5n0ITpw5JBHV1Kph3/KM=", "i3l8ghdTf9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=", "R8B8qYabnMSILPhrtuOhGYrHn3llsMHqBbi70gkljEE=", "rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=", "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:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985D
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):	5.306344309037089
Encrypted:	false
SSDEEP:	6:l8fUWfkvuVq2PWXp+N23iKKdK25+Xqx8chl+IFUtqVA8fUWfkRESgZmwYVA8fUWt:IfSuVva5KkTXfchl3FUt+f+g/gfuSI5M
MD5:	CBFCC4AAF6BAA18213A155FFE4287C07
SHA1:	DF32E806883462C35468AE8853E8B1151E3F3C41
SHA-256:	B29D229877853337FD1A5AE41E60B5BDBC9EE99B35D831795DA9BBD4210EE97E
SHA-512:	E968C6A4713C12F203226B3755840618A14A9927D892706D6D2B7840F3C4228B2CF6C5E062360BC5E0BE4FA521CE75CF0CD4F2AF88DEB9F9D9D23264C3FDEA5
Malicious:	false
Reputation:	low
Preview:	2022/06/23-18:13:57.567 1bd0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2022/06/23-18:13:57.568 1bd0 Recovering log #3.2022/06/23-18:13:57.570 1bd0 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):	5.306344309037089
Encrypted:	false
SSDEEP:	6:l8fUWfkvuVq2PWXp+N23iKKdK25+Xqx8chl+IFUtqVA8fUWfkRESgZmwYVA8fUWt:IfSuVva5KkTXfchl3FUt+f+g/gfuSI5M
MD5:	CBFCC4AAF6BAA18213A155FFE4287C07
SHA1:	DF32E806883462C35468AE8853E8B1151E3F3C41
SHA-256:	B29D229877853337FD1A5AE41E60B5BDBC9EE99B35D831795DA9BBD4210EE97E
SHA-512:	E968C6A4713C12F203226B3755840618A14A9927D892706D6D2B7840F3C4228B2CF6C5E062360BC5E0BE4FA521CE75CF0CD4F2AF88DEB9F9D9D23264C3FDEA5
Malicious:	false
Reputation:	low
Preview:	2022/06/23-18:13:57.567 1bd0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2022/06/23-18:13:57.568 1bd0 Recovering log #3.2022/06/23-18:13:57.570 1bd0 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\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEIIllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Reputation:	low
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky: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\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\a98b08b0-43d5-47e7-a74f-c8b2f493a9ef.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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky: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\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\0f25ce2b-a737-407c-8110-84d4234450ba.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):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/fy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071B1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","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\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEIIllkEthXllkI2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Reputation:	low
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\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):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/fy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071B1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","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\Default\e82f5442-0663-4b36-b5be-9f40d0972250.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):	1815
Entropy (8bit):	4.892602749509893
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDH3qyvz5sLGS2RLsbMbQjds6MHWYhbD:JTnOCXGDHa+zsAMtGLhH
MD5:	13F3BC7AD47FFBDFB93BDE11BAD7DD58
SHA1:	842F5B47E2F129F343F78D2D70696192D91DBC37
SHA-256:	EF9936D9ED2F3F044BEE17878FBBD3EC08F17F272C42DCE9D034C71D0CBC89A0
SHA-512:	EBE81B6C9EF15FD75A5C1124420D7EBD83EB870705C2E14117558208350960430C38FF5E33B9B27F824132BFB2A975147CF7112F372F9B22EE5B0E0F7A8F4E09
Malicious:	false
Reputation:	low
Preview:	{\"net\":{\"http_server_properties\":{\"servers\":{\"isolation\":[],\"server\":\"https://www.gstatic.com\",\"supports_spdy\":true},{\"isolation\":[],\"server\":\"https://www.google.com\",\"s upports_spdy\":true},{\"isolation\":[],\"server\":\"https://ssl.gstatic.com\",\"supports_spdy\":true},{\"isolation\":[],\"server\":\"https://fonts.gstatic.com\",\"supports_spdy\":true},{\"isolation\": [],\"server\":\"https://apis.google.com\",\"supports_spdy\":true},{\"isolation\":[],\"server\":\"https://play.google.com\",\"supports_spdy\":true},{\"isolation\":[],\"server\":\"https://ogs.google.c om\",\"supports_spdy\":true},{\"isolation\":[],\"server\":\"https://www.googleapis.com\",\"supports_spdy\":true},{\"isolation\":[],\"server\":\"https://clients2.googleusercontent.com\",\"s upports_spdy\":true},{\"isolation\":[],\"server\":\"https://dns.google\",\"supports_spdy\":true},{\"alternative_service\":{\"advertised_versions\":[50],\"expiration\":\"1330309882887778 6\",\"port\":443,\"protocol_str\":\"quic\"}},\"isolation\":[],\"server\":\"https://redirector.gvt1.com\"},{\"alternative_service\":{\"advertised_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f6e43385-86df-4424-9082-4eaf1c861a4e.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+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLSNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH

MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC48472F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
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\ff721e75-de78-4e39-83d4-ff1f3857379.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):	19792
Entropy (8bit):	5.564355516859378
Encrypted:	false
SSDEEP:	384:08h2tRLlcvXn1kXqKf/pUZNCgVLH2HfDzrUAHGDFLmk4kp:sLIOn1kXqKf/pUZNCgVLH2HffrUEGD4G
MD5:	EDFBD675BCC9D3AAB9CE24FE606C7DA4
SHA1:	587C9F355803CCEDD91624C7A7E9242988DC0D47
SHA-256:	C46801CC7DEFF96B0614C84FEA603BBE55765030E7C19E9C92A7F78DE8002C75
SHA-512:	DF479B373F1FA807225AF69A81D984008EB26427C0D1F749065E0C3D3446EFD98D871D855970613550B7DAA1227D62B717607F24D85E66E65B40D962756C2080
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":{"pdf.doc:docx:docm:xls:xlsx:xlsm:xlsm:ppt:pptx:pptxm:pptm:htm t: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":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"active_permissions":{"api":{"management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"},"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{"},"content_settings":[],"creation_flags":1,"events":{"},"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[]},"incognito_preferences":{"},"install_time":"13300506826339114","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\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:tbdlmQxZaHIGiOR6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEBF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
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:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
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):	204266
Entropy (8bit):	6.043012738207363
Encrypted:	false
SSDEEP:	3072:68bfiflHRF/F5TV+1C5V42Mqr0A+roO31l1FcbXafIB0u1GOJmA3iuR2:6Ayw/FWC/f3wbaqfllUOoSiuR2
MD5:	93EF2845556351356C8CA465736BB933
SHA1:	69381F57C46A083B40C34B2F8AEA3F2FF7A8675B
SHA-256:	C17EBD3C432B10E9DF9C77EDEF9D335B440B560ED209647CEDF053D08EBAD6E
SHA-512:	8C91D5672540AA3B6DAE2A5BBB223E2DAFB7F6210A2ED158CFA5E966027A89E71CE24CED491CFF33CAD779CF62A32540C9E50A214D489FC6AC6657CD904BD C5B
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":1.656033228632387e+12,"network":1.656000829e+12,"ticks":117620955.0,"uncertainty":4110552.0}}, "os_crypt":{"encrypt_e d_key":"RFBBUeKBAAAAOlyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydZHLcAAAAAIAAAAAABmAAAAAQAAAAABAL2tyan+IsWtxhoUVdUYrY iwg8lJkppNr2ZbFie9UAAAAA6AAAAAaAIAAAABDv4gjLq1dOS7lKRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfllw4oXIE4R7I0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGwCOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639324767"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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):	95428
Entropy (8bit):	3.7511422233425447
Encrypted:	false
SSDEEP:	384:9LAvDhSgtmNhVeETON7rgvXd3AfR8H14Gsbrmx7TxgFBlwrarmSWky9jzD8ONdbQ:daKFdul4goeHnlR4//CJkzhPdu
MD5:	8EBA9B56A6B9EC0BAC1E78E000D79C3F
SHA1:	10F9FFEAE878CF539AC0F040B768FE31941839A85
SHA-256:	8A8F281A0F188F315908D78D0C5CB7D27A5F63936E69B6466FFAFBC11F365C07
SHA-512:	DDA5CB4B402503A4E3BAD366A42FEFE5FF78B7B78615FB6F9D81482C938387FFBAE62D1B6A298F01A6F9AE9DDBEC80B68FAD0F9550967842EDF549AAAA8597 BA
Malicious:	false
Reputation:	low
Preview:	.t.....*...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.D...C::\P.r.o.g.r.a.m..F.i.l.e.s.\C.o .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\6665d7b4-b740-4436-98a3-8b8a825a6353.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.750594427226366
Encrypted:	false
SSDEEP:	384:jLAvDhSgJNiTON7rgvXd3AfR8H14Gsbrmx7TxgFBlwrarmSVy9jzD8ONdbNy17ak:kKFdulYgoeHnlR4//CJkzhPdK
MD5:	457B815E9969D3C04FB2B610807447FE
SHA1:	3458A62F1AB9BEB5A400E53965D1D5016889752E
SHA-256:	1FD5C7F607541D396216C8A4322541434BDF23B6EBCAA8BCD9960418ECD63AE
SHA-512:	DE4D505AE2828E3A44D6330D16742688967EDC673A380DBAD4245AB54B4C4FB76BA8845C27FA967B8629F49B47E9A40FCF78302831BA7773F0F8FA5C4CC6486

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!...D)...%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.D...C::\P.r.o.g.r.a.m..F.i.l.e.s\l.C.o.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\dcca05ac-97f0-4ad6-9fb2-536ebdbde734.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):	212707
Entropy (8bit):	6.071006787167728
Encrypted:	false
SSDEEP:	3072:6d38bfiffHRF/F5TV+1C5V42Mqr0A+roO3l1fCbXaflB0u1GOJmA3iuR2:Q3Ayw/FWC/f3wbaqfllUOoSiuR2
MD5:	4829A86DD7321976DB17A346067BCBD8
SHA1:	E8034B0C26BF1578D792A1A3FAB891EED2042A86
SHA-256:	5C252E4B555BACB752A47A780A3DCC18A2DBF2FCCED424F3EF95C2A6DE350C96
SHA-512:	73E6E2246BD94FB245BB1C60232A7B47A28D086B8AADFFFC3012555FE62F4B94F1ADF620D782062F0E7B5E69FE8363C8367F1A5A865893F5560F5CFB5C4B5BECF
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":1.656033228632387e+12,"network":1.656000829e+12,"ticks":117620955.0,"uncertainty":4110552.0},"os_crypt":{"encrypt_d_key":"RFBbUEkBAAAAOlyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLCAAAAAIAAAAAABBMAAAAAQAAIAAABAL2tyan+IsWtxhoUVdUYrYiwg8lJkppNr2ZbFie9UAAAAA6AAAAAaAAIAAAABDv4gjLq1dOS7lKRG21YVXojnHhsRhnNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdflljw4oXlE4R7l0AAAABlT36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBuHMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\e380db3d-e053-4d07-825e-919efa7c09c7.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):	212707
Entropy (8bit):	6.071005029825148
Encrypted:	false
SSDEEP:	3072:ssA8bfiffHRF/F5TV+1C5V42Mqr0A+roO3l1fCbXaflB0u1GOJmA3iuR2:PAAyw/FWC/f3wbaqfllUOoSiuR2
MD5:	BB1E9FD87275F2C01BEF78478C16FC27
SHA1:	B5E99F00947BCDAEA6D1990C648E174C4E77A2C4
SHA-256:	B9F1A4F091366E160AA0E7BF56A73CE1296C05FCD8A24E65A69821410353256E
SHA-512:	9138DFF2DFA48FCA145B4F1C556E7794C40AA9B31EA40F7DB489B4C90F0BD9D0717DE24B62AC4CBAE8355ED186B78DDA3890BAC61E966D8DF77E4EEDD664A56
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":1.656033228632387e+12,"network":1.656000829e+12,"ticks":117620955.0,"uncertainty":4110552.0},"os_crypt":{"encrypt_d_key":"RFBbUEkBAAAAOlyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLCAAAAAIAAAAAABBMAAAAAQAAIAAABAL2tyan+IsWtxhoUVdUYrYiwg8lJkppNr2ZbFie9UAAAAA6AAAAAaAAIAAAABDv4gjLq1dOS7lKRG21YVXojnHhsRhnNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdflljw4oXlE4R7l0AAAABlT36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBuHMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639324767"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\40212a03-e0ad-48db-b4a3-7035593adebd.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECB7FFCDBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\41be5f9c-4016-4134-bef8-2736450dabf5.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+QSVh85PxEalRVHmclD9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99FId9RBQYBVcaxInfl
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
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.....\..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..){..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....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.!1..

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\41be5f9c-4016-4134-bef8-2736450dabf5.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+QSVh85PxEalRVHmclD9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99FId9RBQYBVcaxInfl
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
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.....\..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..){..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....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.!1..

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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": "..... .. Chrome".. },.. "crawl_connect_to_network": {.. "message": "..... .. Chrome".. },.. "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_dir2492_211076532\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+dgYGfFoO8ZpU34+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": "Inicieu la sessi. a Chrome.".. },.. }

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BF5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488CB
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": "Pipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.In. 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_dir2492_211076532\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:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxICZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6IL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA04CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "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": "Betalng 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_dir2492_211076532\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:1HEzWWYp3Beww8Zp7k4OGAOfQj
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_dir2492_211076532\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:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... Chrome Web Store".. },.. "app_name": {.. "message": "..... Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "..... Chrome Web Store".. },.. "crawl_connect_to_network": {.. "message": "..... Chrome Web Store".. },.. "iap_unavailable": {.. "message": "..... Chrome Web Store".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "..... Chrome".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEFEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
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_dir2492_211076532\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+WYPuU34OuFpR+dgGfZO8ZpU34aEGFpR03OyZnLAOfTYdD: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_dir2492_211076532\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:	12:1HEJHlbgGHIb+WYPuU34ubdDH+dgxbFxTO8ZpU34lPbdIvO03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNI5OGAOfD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "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_dir2492_211076532\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:	12:1HEJHlbgGHIb+WYPuU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LIOGAOfD
MD5:	6B2583D8D1C147E36A69A88009CBEBEC7
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 tr ansaction could not be completed.".. }... "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..
----------	---

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqWYpTeObk8ZpT/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_unavail able": {.. "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_dir2492_211076532\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+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BE/ D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. }... "app_name": {.. "message": "Chrome Web Storen maksut".. }... "crawl_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. }... "crawl_connect_to_network": {.. "message": "Muodosta verkkoysteys".. }... "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. }... "please_sign_in": {.. "message": "Kirjaudu sis.n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAQfvQ
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEE7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF5 2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. }... "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. }... "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_dir2492_211076532\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:	3F9D44EA8807069A32ACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paielements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paielements 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_dir2492_211076532\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": "..... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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:	12:1HEJGiimxbmZGGGiimxbmZ+WYpU34OBOEuhpIO+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".. },.. "crawl_app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "crawl_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no 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_dir2492_211076532\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:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgiJ08ZpU34Huo9O03OyZnLAOfTYBIAym:1HEVrk5WYpQzTug/8ZpwoXOGAOfYAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "crawl_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el".. },.. "crawl_connect_to_network": {.. "message": "K.rj.k, csatlako zzon 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_dir2492_211076532\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..".. },.. "crawl_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_dir2492_211076532\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".. },.. "crawl_app_unavailable": {.. "message": "App al momento non disponibile..".. },.. "crawl_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_dir2492_211076532\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:	12:1HEJ07uUGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
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_dir2492_211076532\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". }.. "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_dir2492_211076532\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:1HELqHtkKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BD4EAE3EA5
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_dir2492_211076532\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:	1F67FF6EF6E90C0CE3AAAF56ED543AEFD381574D

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.rl.k. Chrome.".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCF5
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_dir2492_211076532\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:	12:1HEJJQGbGGJQGkb+WYPu34OQKJT+dgixUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXi8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A7
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_dir2492_211076532\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+dgQUgO8ZpU34bdbfilu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOfiC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C1A3943A6373C2
SHA-512:	A71F7C7BFBFBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADF81271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B77

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 com pleted.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+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_dir2492_211076532\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:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F24
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "crawl_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_dir2492_211076532\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+WYpU344Hlx2Z+dgrVPIZO8ZpU34qT7hI3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB783BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. }.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. }.. "craw_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 completed..".. }.. "please_sign_in": {.. "message": "Conectear.-te la Chrome..".. }..}..
----------	--

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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/TO8ZpU347NWjT03On:1HEIOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F632
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_dir2492_211076532\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:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE08"AAB62F1C88CD2A40CC44E59D
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 completed..".. }.. "please_sign_in": {.. "message": "Prihl.ste sa do prehlada.a Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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+dgca1ZO8ZpU34GcQArERff03OyZnLh: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".. }.. "craw_app_unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. }.. "craw_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_dir2492_211076532\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+dgucucO8ZpU34s1muP03OyZnLAOfTYzDYD:1HEKsb59sbTWYplx4Xud8Zpy1mNOGAOv
MD5:	D485DF17F085B6A37125694F85646FD0
SHA1:	24D51D8642CDC6EFD5D8D7A4430232D8CDE25108
SHA-256:	7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818
SHA-512:	0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E
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_dir2492_211076532\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:	12:1HEJJMkbGGJmkb+WYpU34OACwz+dgNPGFZO8ZpU34JgpXLSb03OyZnLAOfTYLdID:1HErMkaqMk6WYpTOcb8ZpDgdZOGAOf8Y
MD5:	D372B8204EB743E16F45C7CBD3CAAF37
SHA1:	C96C57219D292B01016B37DCF82E7C79AD0DD1E8
SHA-256:	B8BA77E0089B0676545EC16D32468B727812B444F90B33A7A5B748E6C36C4388
SHA-512:	33640529E0D5DCC5CA4BDB0615A2818E8D26C6FCB7B3474C08AC3EB67B9DB40E1F0A79954ED20728CD47A686D2533DCBC76ABCBD917F8530C8DE8BBA68752E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Bet��ln��g via Chrome Web Store".. }.. "app_name": {.. "message": "Bet��ln��g via Chrome Web Store".. }.. "craw_app_unavailable": {.. "message": "Appen .r inte tillg.nglig f.r tillf.llet.".. }.. "craw_connect_to_network": {.. "message": "Anslut till ett n.tverk.".. }.. "iap_unavailable": {.. "message": "Bet��ln��g 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_dir2492_211076532\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/WYpU6FI72SmIG8ZpyactrW2SAOGAOfvSLD:WK2DNYp6U4y3bpyLxwGFW
MD5:	83E2D1E97791A4B2C5C69926EFB629C9
SHA1:	429600425CB0F196DDDD717F940E94DBD8BFF2837
SHA-256:	2FECA577F43D97BAEEA464741D585892103585208FD0A935B810A03BDCE83C88
SHA-512:	60A5928DAA8CB4341487F477C56B5A98B83EDE50E5F4F55A802E01FDDAB86F3E795D391953D3D9214552D14D3F58C5A183693C613720FC12FC387D7B8F9B9AB
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_dir2492_211076532\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:	12:1HEJ9Y8GG9Y8+WYpU34wWT+dgGb0GO8ZpU34wryd7T03OyZnLAOfTYGbPKG:1HE0jWYpyRnG8Zpyr/OGAOfFPn
MD5:	2CEAE0567B6BB1D240BBAD690A98CA3B
SHA1:	5944346FBD4A0797B13223895995CAB58E9ECD23
SHA-256:	A7CB86F30C9C31FE5540282C308BA96ADB4EC16EF98C87129EB88105E5BEF5FC
SHA-512:	108A07C6D03D7178E8D0FFE5349E0249A898D864964FED8757BD8A08BC1C6D9613F2A6C01AA34A6606127D1C6CE14C229FA02586677DBB060B85E3E845950E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Ma.azas .demeleri".. }.. "app_name": {.. "message": "Chrome Web Ma.azas .demeleri".. }.. "craw_app_unavailable": {.. "message": "Uygulama .u anda kullan.lam.yor.." }.. "craw_connect_to_network": {.. "message": "L.tfen bir a.a ba.lan.n.." }.. "iap_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_dir2492_211076532\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+dgSV1EjIT08ZpU347qtP2CTW:1HElwEkK4uwEkK8WYpd/dTV1e8Zptq5S
MD5:	AB0B56120E6B38C42CC3612BE948EF50
SHA1:	8B3F520E5713D9F116D68E71DAEED1F6E8D74629
SHA-256:	68ABA284751EB9C856032062EF9B1651E2A1E5CE5FDA0977FFC97D63BA7BED9E
SHA-512:	CD852A58217F739C1CD58567FF432D31A7AD3F68C884ABBA1DA95799BCD1545C6A5D3B06F319681C12B78AD0A709828DE4B22736316F148D21F5DB76A5BCCBF
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_dir2492_211076532\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+dgdklzoO8ZpU34NFHoz03OyZnLAOfTU:1HEI4B8WYpAKytFZ8ZpXKMOGAOfd6D
MD5:	7EBB677FEAD8557D3676505225A7249A
SHA1:	F161B4B6001AAEAB246FF8987F4D992B48D47BE
SHA-256:	051F96ED874C11C4A13589B5F68964E4F5B03B52DDA223D56524F2CA23760C04
SHA-512:	74FD267CF7E299FB8E7054605C3F651F057F676FF865082FA24F4916755456768DB0DA62DBC515D829B48AB1F9CFC8AD3E841DCBF1F194D5CB14C5335A192A0
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".. }.. "craw_app_unavailable": {.. "message": ".ng d.ng hi.n kh.ng kh. d.ng.." }.. "craw_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 completed.." }.. "please_sign_in": {.. "message": "Vui l.ng .ng nh.p v.o Chrome.." }..}

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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_dir2492_211076532\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_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_dir2492_211076532\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:AZQficsU
MD5:	0834821960CB5C6E9DA774AEF649CB2E4
SHA1:	7D25F027D7CEE9E94E9CBDEE1F9220C8D20A1588
SHA-256:	52A24FA2FB3BCB18D9D8571AE385C4A830FF98CE4C18384D40A84EA7F6BA7F69
SHA-512:	9AEAF3CECE295678242D81D71804E370900A6D4C6A618C5A81CACD869B84346FEAC92189E01718A7BB5C8226E9BE88B063D2ECE7CB0C84F17BB1AF3C5B1A31C4
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyl6W3siYmxvY2tfc2l6ZSI6NDNA5NiwiZGlnZXN0Ijoic2hhMjU2liwiZmlsZXMiOiIt7lnBhdGgiOiJfbG9jYXlcy9iZy9tZXNzYWdlcy5qc29uliwicm9vdF9oYXNoljoiZHUtdGRPdUNWcmxkY254Q0poRkg2NXpLU05vb1RiUE56bDNHbzdRMGJ3SSJ9LHsicGF0aCI6Ij9sb2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJ6ZGtWaF9XdkxJWlhkck5xWHBvSHNRMGh1ZGtSM2d1QIMzb2VsTEZLNkVIn0seyJwYXRoljoiX2xvY2FsZXMvY3MvbWVzc2FnZXMuYWVzL2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJOV3FkU3Rfc1NFMm9KT2VuSUZlM0pMRm9iOGtBZ3ZTa3RtZGpCRGJWazdBln0seyJwYXRoljoiX2xvY2FsZXMvZWVzc2FnZXMuYWVzL2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJ6ZGtWaF9XdkxJWlhkck5xWHBvSHNRMGh1ZGtSM2d1QIMzb2VsTEZLNkVIn0seyJwYXRoljoiX2xvYXlcy9lbi9tZXNzYWdlcy5qc29uliwicm9vdF9oYXNoljoidOpSZDFmM3NxmERFVTJHXLXd

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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:abyfBNC2FRdjRXqbe5Dq31IVIMqX+wd5/CcMMJcRULt0NjyTOEzZQ+h72W3GB0n:Ft/g
MD5:	6EEBED29E6A6301E92A9B8B347807F5F
SHA1:	65DFB69B650560551110B33DCBA50B25E5B876DE
SHA-256:	04CD9494B0ED83924DAD12202630B20D053D9E2819C8E826A386C814CC0A1697
SHA-512:	FEDE6DB31F2AD242E7BC7B52A8859BA7F466A0B920A8DADCB32DCFB5B2A2742E98B767FF22E0C5BC5C11FEC021240AA9E458486C9039EB4EBE5CF6AF7BE97BF2
Malicious:	false
Reputation:	low
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var d,e=el[{};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_dir2492_211076532\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:	26835B4C050F53AD2DDB84469DF9A84BBB2786A655AB52DFC20B54BEDCB81D1ECD789198D5B7D8B940242E5CEAC818A177444D402397AE82C203438C4B1D15CB
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_dir2492_211076532\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;}.craw_overlay { position: absolute;.. left: 0; top: 0; right: 0; bottom: 0;.. background-color: white;.. -webkit-transition: opacity 250ms linear;.. display: -webkit-flex;.. -webkit-flex-direction: column;.. -webkit-flex: 1 0%;.. -webkit-align-items: center;.. -webkit-justify-content: center;.. -webkit-app-region: drag;}.craw_overlay img { margin: 16px;}.#loading_overlay { opacity: 1;}.#offline_overlay { opacity: 0; display: none;}.#offline_overlay > img { -webkit-filter: saturate(0%);}.#offline_overlay > span { font-family: 'Open Sans', 'Deja Vu Sans', Arial, sans-serif; font-size: 15px; line-height: 21px; color: #8d8d8d; display: block;}.#loading_splash { width: 128px; height: 128px;}.#drag_overlay { position: absolute;.. left: 0; top: 0; right: 0; bottom: 0; pointer-events: none;.. -webkit

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\CRX_INSTALL\html\craw_window.html	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

Size (bytes):	558
Entropy (8bit):	7.505638146035601
Encrypted:	false
SSDEEP:	12:6v/7vyVgSKYsfFzXxXsrPfA+b0YX+5IOUWCQKZnuow7:6yVnKYsfZhXsrlq0YXmgQGn6
MD5:	FB9C46EA81AD3E456D90D58697C12C06
SHA1:	5FC450F7D73CCFAC8F0D818CB3392BA4D91B69DE
SHA-256:	016CA659BA080E194FBFC0929602B16506ED60AA6019FAA51410C4FD93B583E8
SHA-512:	ADD810EE9EB7CAEC505B5FD90A1F184CE39D8F8C689DCC240F188FE353B9575489492E07D572A3B1C11A1555CE66AFC5134903E4C1AA3D54BC7C5ED3E65B50C
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.Ep]wFk.60o.J0.`Y..cT..Y.Tb. DF.d..s.Z..E..9.4._C_...%.*.^...4.l...Y..X..R.../...Wj+w0[.]_B.k.\${\.>.%.....lz .w.ALxo.2;...a...".p..S..&..uXS...<..6..[.zD..._N+w.WbM7ye6X<...'(.=f).....\$f..5..P...k..."..8.s.<zgSm@.....).Y.....e..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_dir2492_211076532\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/RPJdMV7bScsP4a9zln94FptVp: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.j'> %O...V!s...../...`<.`.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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/lhPKM4nDsp7q1hKVlomsj9rxKNgtmNOVZ+GFYep:6v/7iMXVq1ylxemNgtmKVnYM
MD5:	0599DFD9107C7647F27E69331B0A7D75
SHA1:	3198C0A5F34DB67F91A0035DBC297354CBC95525
SHA-256:	131817CD9311C03DF22D769DD2AD7FA2E6E9558863A89F7E5E1657424031A937
SHA-512:	0076ACB9D6A886BD987876E49495038F9388B292A9EFE5C9093CCA64CA3692E3A5D24E35172C7697F6AAE34B86CA217EE59C003423E46D9499BD27EC7D77A64
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ..szz.....tEXtSoftware.Adobe ImageReadyq.e<...IDATx..... ..Pp.X....H...b@...].^LC_.E.BP+.....X.P.....q..~.p/. ..s.....%D^..\$......@!...<...)? .4{k.G3...4.[cH..0..l.8..lr..m.R..{.....`.f...#..x.....IEND.B`.

C:\Users\user\AppData\Local\Temp\scoped_dir2492_211076532\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/9lVtEHxrPLyN+ltNPhv/l2up:6v/lhPKM4nDspnAkZHVtERrPLygltnPn
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_dir2492_211076532\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//thPI3xWrA4RthwkBDsTBZttdd//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_dir2492_211076532\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/9IVtEXlyN+ltN1/lsg1p:6v/lhPKM4nDspnAkZHVtEZgltN1eup
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_dir2492_211076532\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:	24:1HEis7ViC/yox/fiqeUoLFmF1s80FKrGfd0d3NZNZx1Fq7eY7nfj1B:WL7V2opiV1mvs8rxTZRczhB
MD5:	01334FB9D092AF2AA46C4185E405C627
SHA1:	47AD3C0E82362FFE5B881DF8D71D6F79AB7F5796
SHA-256:	F52714812D68C577A445169D11E84DF6751C2D6886BC429643072BB5D61C6C27
SHA-512:	888D96ADB7A847ABE472145258C8C46950EB2FA3BA7D596C2E90A17C8FB06FD0155C56CC8ABA5D076D89368417464BCB2D236F9E40E53241950A01F9F8ED54CF
Malicious:	false
Reputation:	low
Preview:	{.. "app": {.. "background": {.. "scripts": ["crawl_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": "MIGfMA0GCsSgSib3DQEBAQUAA4GNADCBiQKBgQCkKfMnLqViEyokd1wk57FxJtW2XXpGXzIHBzv9vQI/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"].. }..

Static File Info

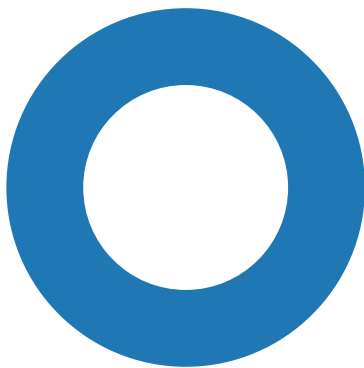
🚫 No static file info

Network Behavior

🚫 No network behavior found

Statistics

Behavior



● chrome.exe
● chrome.exe

💡 Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 2492, Parent PID: 868

General

Target ID:	0
Start time:	18:13:44
Start date:	23/06/2022
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 "https://express.adobe.com/page/QSpEijTBWEere/
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: 5716, Parent PID: 2492
General		
Target ID:	1	
Start time:	18:13:46	
Start date:	23/06/2022	
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=1548,3426159670808259283,2010510569848056573,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /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	