ID: 635131
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 15:17:20
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

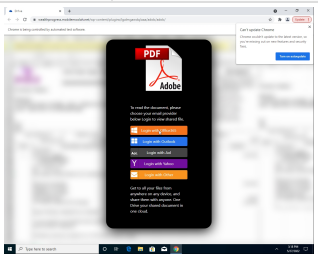
Windows Analysis Report

https://dik.si/OB6x6

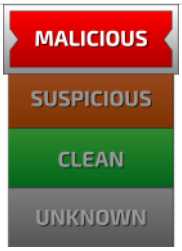
Overview

General Information

Sample URL:	https://dik.si/OB6x6
Analysis ID:	635131



Detection



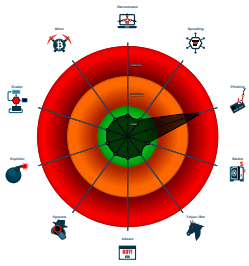
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish7
- Multi AV Scanner detection for dom…
- Yara detected HtmlPhish10
- Multi AV Scanner detection for subm…
- HTML body contains low number of …
- Suspicious form URL found
- No HTML title found
- Form action URLs do not match ma…

Classification



Process Tree

- **System is start**
- chrome.exe (PID: 6556 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation --single-argument https://dik.si/OB6x6 MD5: 74859601FB4BEEA84B40D874CCB56CAB)
  - chrome.exe (PID: 3468 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1752,1225860649479586440,12493433813693861157,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2120 /prefetch:8 MD5: 74859601FB4BEEA84B40D874CCB56CAB)
- **cleanup**

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
72168.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
72168.0.pages.csv	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Phishing

Yara detected HtmlPhish7

Yara detected HtmlPhish10

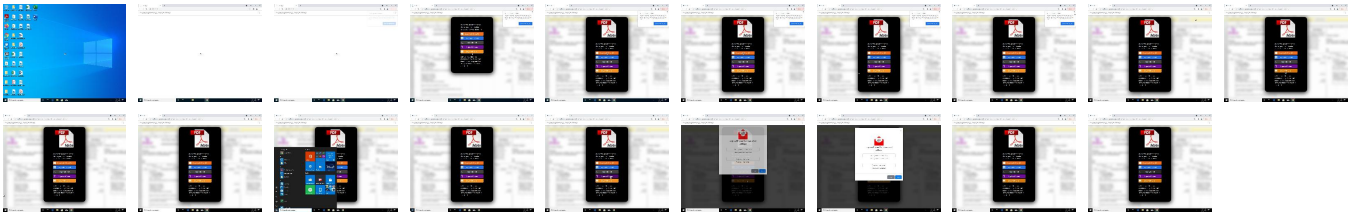
Mitre Att&ck Matrix

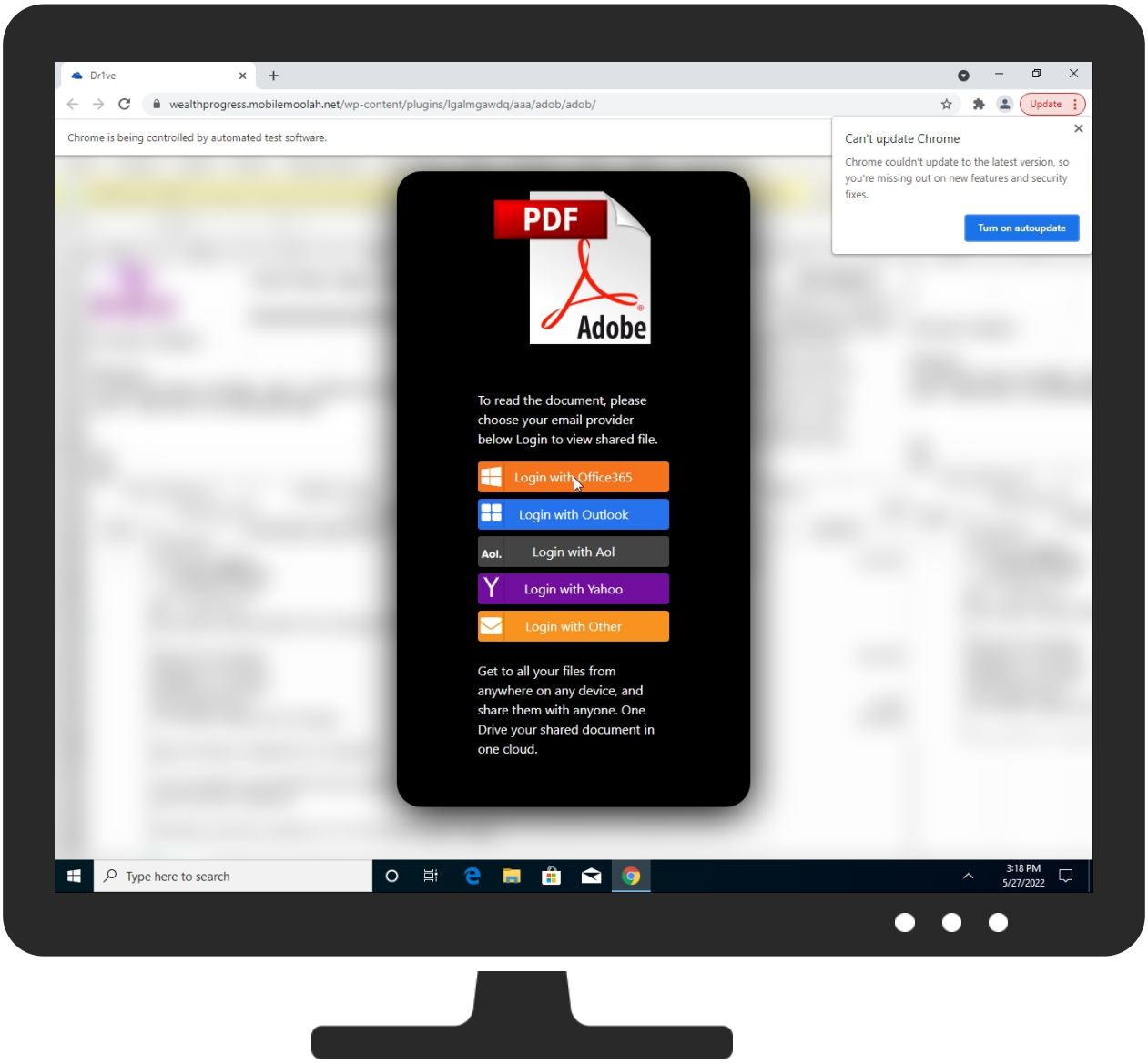
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading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

Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
https://dik.si/OB6x6	9%	Virustotal		Browse
https://dik.si/OB6x6	100%	Avira URL Cloud	phishing	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
wealthprogress.mobilemoolah.net	4%	Virustotal		Browse
dik.si	5%	Virustotal		Browse
lipis.github.io	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
https://wealthprogress.mobilemoolah.net/wp-content/plugins/lgalmgawdq/aaa/adob/adob/	0%	Virustotal		Browse

Domains and IPs

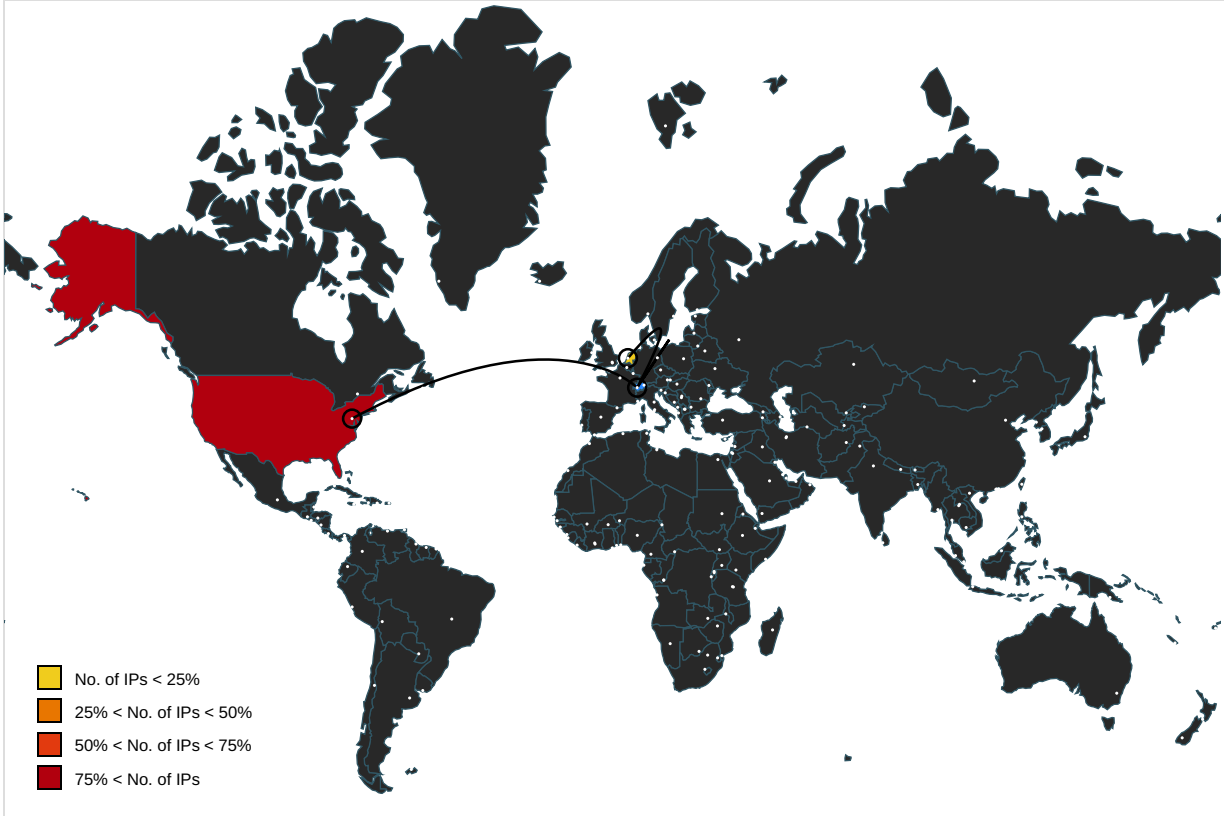
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealthprogress.mobilemoolah.net	64.227.108.223	true	false	• 4%, Virustotal, Browse	unknown
stackpath.bootstrapcdn.com	104.18.11.207	true	false		high
dik.si	188.114.96.3	true	true	• 5%, Virustotal, Browse	unknown
lipis.github.io	185.199.108.153	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	142.250.184.237	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
clients.l.google.com	172.217.23.110	true	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://wealthprogress.mobilemoolah.net/wp-content/plugins/lgalmgawdq/aaa/adob/adob/	true	• 0%, Virustotal, Browse	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.125.108.199	unknown	United States		15169	GOOGLEUS	false
142.250.185.234	unknown	United States		15169	GOOGLEUS	false
142.250.185.110	unknown	United States		15169	GOOGLEUS	false
142.250.185.227	unknown	United States		15169	GOOGLEUS	false
172.217.23.110	clients.l.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.11.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.181.227	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
64.227.108.223	wealthprogress.mobilemolah.net	United States		14061	DIGITALOCEAN-ASNUS	false
188.114.96.3	dik.si	European Union		13335	CLOUDFLARENETUS	true
69.16.175.10	unknown	United States		20446	HIGHWINDS3US	false
142.250.184.237	accounts.google.com	United States		15169	GOOGLEUS	false
185.199.108.153	lipis.github.io	Netherlands		54113	FASTLYUS	false
142.250.186.42	unknown	United States		15169	GOOGLEUS	false
104.17.25.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
142.250.184.234	unknown	United States		15169	GOOGLEUS	false
142.250.186.99	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635131
Start date and time: 27/05/202215:17:20	2022-05-27 15:17:20 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://dik.si/OB6x6
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.phis.win@27/80@10/211
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): CompPkgSrv.exe
- Excluded IPs from analysis (whitelisted): 142.250.185.227, 142.250.185.110, 74.125.108.199, 69.16.175.10, 69.16.175.42, 142.250.185.234, 142.250.184.234
- Excluded domains from analysis (whitelisted): login.live.com, slscr.update.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Created / dropped Files

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\0619541d-efde-4b97-89ac-87858b26a841.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96852
Entropy (8bit):	3.756665696445929
Encrypted:	false
SSDEEP:	
MD5:	63E8F27DCC6773B05C2D2FEB1EBCBB85
SHA1:	4E4E7A1A7BE5B53047ACBB7DD1F47958F97557C6
SHA-256:	8D48BB71F19C9097122E97BB1190D2BCB136B29F856DB7F794FCD0D69CB70F75
SHA-512:	872EBD6656667FC79CE95075F490AAFB312CFA09D36D60F48496187A9536BCF2D83E3BA759788DB1EAF4A35C3252C083F70BE7516EAC790AE573E4C384A27DD0
Malicious:	false
Reputation:	low
Preview:	Pz.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....puA...c.:.\.p.r.o.g.r.a.m. .f.i.l.e.s. .(.x.8.6.).\.m.i.c.r.o.s.o.f.t. .o.n.e.d.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.....f.i.l.e.s.y.n.c.s.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e."...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....2.1...0.8.3...0.4.2.5...0.0.0.3.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...n]8. ...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.7.-.Z.i.p.\.7.-.z.i.p...d.l.l.....n\....%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.7.-.z.i.p.\.....7.-.z.i.p...d.l.l.....7.-.Z.i.p.....7.-.Z.i.p. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....1.9...0.0.....n]8.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\25c5704a-c4c4-45e5-bad7-da092eccf1c6.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):	105157
Entropy (8bit):	6.034886974499159
Encrypted:	false
SSDEEP:	
MD5:	21F611838444D5AC217A484205BB81B3
SHA1:	20C37D309252CDA567DF00E5F1BB51E52DEEE481
SHA-256:	EF0CCBC4BA47C543B446D2B7E298F30EE0A10171A6B181DDEC4FFDCD8065BFCA
SHA-512:	907901FC7C09BCCE287E6EE59BB7D112408CB27A0E60BE110F0441E1C83370D3B60CE30D34960616C024565DACD35DCD8ED54CEFD5D847C74EC53F70D1E8739
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653689881782276e+12,"network":1.653657483e+12,"ticks":171695368.0,"uncertainty":2993445.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"policy":{"last_statistics_update":"13298163479427840"},"profile":{"info_cache":{"Default":{"active_time":1653689880.650481,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\4f00d8ec-401a-4099-ac30-3d87fe0c9e6a.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97592
Entropy (8bit):	3.7566114370705646
Encrypted:	false
SSDEEP:	
MD5:	103E4CD8462909AC83B4A290DBCF8CA5
SHA1:	B320B177C746E38097E0D36B2B59A02FC0F4B3B7
SHA-256:	5E95697F73F4BE72307270CB816A17CD64DE4A36B4F4B9B6F80D511CE55917D7
SHA-512:	B49C32A99B992A2F41D56ECC5D31B03FD727C12D290629B881E423ED98DF26D865830D12460F9D8917AB0EBF33F53E0604B9ABB07C2E88ECCA7A0724EEC35E7
Malicious:	false
Reputation:	low
Preview:	4}.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....puA...c.:.\.p.r.o.g.r.a.m. .f.i.l.e.s. .(.x.8.6.).\.m.i.c.r.o.s.o.f.t. .o.n.e.d.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.....f.i.l.e.s.y.n.c.s.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e."...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....2.1...0.8.3...0.4.2.5...0.0.0.3.....T...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e.\.2.1...0.8.3...0.4.2.5...0.0.0.3.\.a.m.d.6.4.\.F.i.l.e.S.y.n.c.S.h.e.l.l.6.4...d.l.l.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...n]8. ...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.7.-.Z.i.p.\.7.-.z.i.p...d.l.l.....n\....%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.7.-.z.i.p.\.....7.-.z.i.p...d.l.l.....7.-.Z.i.p.....7.-.Z.i.p. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n.....1.9...0.0.....n]8.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\64269ed6-12ae-4006-864a-8e675020f08d.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):	109644
Entropy (8bit):	6.064856016604446
Encrypted:	false
SSDEEP:	
MD5:	6AA7F56BE8E4ED1AEC7FD209AB1332B0
SHA1:	C484C9F7B68FBF4CF785A5E4265B16D381A5AE80
SHA-256:	08613058C294BC8C1ED9B0530AA705BD4D53ED5D781A7BD2833D8F3B300BC1CB
SHA-512:	41EF7C13E5A75A583F59154D323BAF7C229D8A58D124A771EBD72C7A0DBC3CE3D468FC0AC4828B04C99F05756B502787D1A8C946E4A3E871BF1E67A976E674E3
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653689881782276e+12,"network":1.653657483e+12,"ticks":171695368.0,"uncertainty":2993445.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187718326"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

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

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\0d47c0b4-99d5-45d8-922b-159a9522a808.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\1096a981-e73d-4c14-8a47-cae7cb5d6ffe.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):	18396
Entropy (8bit):	5.555448074171695
Encrypted:	false
SSDEEP:	
MD5:	13CFF5C8A78AA0AA0086727BF29B88E8
SHA1:	F7263D222B5909E4EDA09ED53B80FAFBD1E54C76
SHA-256:	D4873DE9ECACACE937BA4B277DC89D7A8213ADA4ACC373F76C4A8F8A151DC2AA
SHA-512:	0D478D552DBCB22DB332C6C4448A00204B5955A1828159AA2CB5CB52ED4A46C99817A6AD45055A6FB077D8557B6CA1000F0664C48FF353B36DE675DE03ABE0 9
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mh t:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"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,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13298163479751140","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome. google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons": {"128":"webstore_i

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\172a1c50-8599-425d-bdd4-d45b04ff3809.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3488
Entropy (8bit):	4.941651499654654
Encrypted:	false
SSDEEP:	
MD5:	C6A4D257F0C34DAEB0FF5F1633C834B0
SHA1:	587CB8FE720AAE84EBFA76BEC6CF03BFE4B7E46F
SHA-256:	B62490EF860AD814987E6133935A02F57FC2E3CF367A06EACFBDF28F89662E98
SHA-512:	728C1E61201960A89C8B839028948BE0E0D6D96FA62D585F8CDE33FB49ADAC45000BE179ADEAB35B6C9B530BFEDD9092BE30FD8E6FC3ECE87ACFC84B605E7 876
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298163480826991","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_remov ed":true},"browser":{"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_righ t":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"this_week_number":2734},"default_apps_install_state":2,"domain_diversity":{"last_rep orting_timestamp":"13298163480825521"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"prod uct_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"a16ce157-d5bf-4e36-921b-2c0a44f683db"}},"intl":{"selected_lang uages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"CAEAC91795718286E5A 01B5AA0F032D5","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\1d10d499-946d-4ce6-8a41-4e0a2b5dcf6b.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	15765
Entropy (8bit):	5.574026388129096
Encrypted:	false
SSDEEP:	
MD5:	F0502DDEE17CF9CC0B14D250E847CD32
SHA1:	060DD171EC6F40046D51276DE384865028271240
SHA-256:	74F585E5E6FB01CF8F4B39D5905BCD126DF948AC6D77281A394C86CD35E55DC7
SHA-512:	B539D01FFD5EE41867BF194FA8E36A3F66C4E0FBEB4C3AD51A61B6AA23888A15E3C875FAAFA41A6AC4ACD2F401CB0BC072FAE8E081F87B188E912F7FEF563 257
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mh t:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"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,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13298163479751140","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome. google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons": {"128":"webstore_i

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\34fa52f1-05c0-416a-8395-acd446f995c7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3343
Entropy (8bit):	4.945222848960228
Encrypted:	false
SSDEEP:	
MD5:	CAB8BEABE7E66A4015C98A3C77B3698B
SHA1:	C960AAAEA7014E105290C7D0F09BFCA837C8E8CC
SHA-256:	75431010BFE77818B8BEF4B0C4B328C00668DC6B13C09AAB769EBF58BDA4EDF7
SHA-512:	0D1E94E84294AEA4BF400FF9D0654748BFFEB92D3A1643A6A13B541ADB1BC13EA2F649560A27C8CC3D8AEF9DA5D6B668C7E3BE696091CE882A475B91A9A4CAC8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230891381309","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230891381310","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39697},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230887958662","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230887958664","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":52163},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3-29"],"expiration":"13270230886326794","port":443,"protocol_str":"quic"},{"advertised_alpns":["h3-Q050"],"expiration":"13270230886326795","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\5cff33d4-9fbd-4675-9b11-de0641751f64.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	181072
Entropy (8bit):	5.774426487043815
Encrypted:	false
SSDEEP:	
MD5:	1B40AC9ABB964672109D49ABFCFE2717
SHA1:	966E224F2887075825D42D2E7E0063BFAA81A99C
SHA-256:	503149B1B47F8296DEDB800251DBD9AF614856F0D7E6AB1C03DBC90EBCE53674
SHA-512:	00B50E49CAFD8246102BB460C7B96C20B50A2DDCB48A64C40D65901B517A2698DB9C5AA5EC7F143314DDB8D74624377F12A95C7F4D9FCE206473E8BBF12638B
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .2v...M..(..... ....]..X\.).H...>..Z.....\..._...V...F...A...A.....^..Wb...f.)...l...v.M...B...@..Wc...[.....z...`...J.....9...E...k...R.D.....G...A....;...E...h..XKd..KW.....D...>...=..X....GQ.JW..;M..8K..@H..=;.....JV.YKV.IT.BS.Y.....(..... .....[..TZ.5.B...@..T.....X...]...`..\...K...D...A...;.....3...\...e...V...h.).d.G.<...F...@...3...^..Td...X.....e....v.....:...E...=..T`...d...h.B.....?...;...O...B...A...b.!.g...Ru.....9...8...P...C...C...l..U].M.5@.....6...C...@..T....EW..LX..=K..Ob..Me..5R..AX..;V..++.....BL..KW..KW..DO..BL..EN..AJ..;1.....HT.UIV.FT.BQ.U.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\7d890a49-9aa9-45f9-bba6-f733dca8abec.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):	4379
Entropy (8bit):	5.02202945231993
Encrypted:	false
SSDEEP:	
MD5:	1A666F1184C6D4FB77A1DA15B9E51F7C
SHA1:	53AA28A42399E9B7B29275058A5F23926AF95071
SHA-256:	3A3844A32ABA4ADB0E2965FB6E6D5E9BAA4C5908AB1A557E72996117E91B6AA8
SHA-512:	B93B7DC48DC6C6EE85E3130859FFEE1BF7BBFA2B4EF5C0260E47091B011D13CF0747D470A4CC537924E03A8C64C964B6BEA77EE0EF764E0CD798A42424549F4F
Malicious:	false
Reputation:	low

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298163480826991","alternate_error_pages":{"backup":true},"autocomplete":{"retention_policy_last_version":92},"autofill":{"orphan_rows_removed":true},"browser":{"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"this_week_number":2734,"this_week_services_downstream_foreground_kb":{"115188287":51,"21145003":243,"35565745":2,"5151071":2,"88863520":1}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298163480825521"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1653689882.7186,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm":{"product_category_for_subt

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\8cdfc90c-3ed5-419d-86b2-7d4b33ace0b1.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3488
Entropy (8bit):	4.9419145797338375
Encrypted:	false
SSDEEP:	
MD5:	66754F90CA0F5614EDA3D7C492AA2608
SHA1:	59185F6BD3EC3802CB881EB406E0854A0DC2ABA0
SHA-256:	43B7F7797D22B52A97639A25378CA440CFE7FC3315EE0AD8B15359DCF7E700C7
SHA-512:	D643F3BA195791B589CEC682809CA91CD3DC89E9BCEC2FD2C83122ECCF9E3A2F8660AA221EA437918BB4D5FB28E5E19640E6B3476B57E2D9BA9C5339F8B19E05
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298163480826991","alternate_error_pages":{"backup":true},"autofill":{"orphan_rows_removed":true},"browser":{"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"this_week_number":2734},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298163480825521"},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gcm":{"product_category_for_subtypes":"com.chrome.windows"},"google":{"services":{"signin_scoped_device_id":"a16ce157-d5bf-4e36-921b-2c0a44f683db"}},"intl":{"selected_languages":"en-US,en"},"invalidation":{"per_sender_topics_to_handler":{"1013309121859":{},"8181035976":{}}},"media":{"device_id_salt":"CAEAC91795718286E5A01B5AA0F032D5","engagement":{"schema_version":4}},

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11336
Entropy (8bit):	6.0707244876366575
Encrypted:	false
SSDEEP:	
MD5:	2E2110A99AD3AE9721A458C95C64C868
SHA1:	72AE17599EDC0B2DC61C41D946E3E296864F2CBA
SHA-256:	BB46BA705D5F6F43F66B07EA5DA4CC7CC0BF8FE635CCC4EBBA30A5D4A54158DE
SHA-512:	29D95D043F3E529DD33F73B3207A9167D479D9FC404209497B53229CF68AA634CB8A1FE3FD08512FD7F48AFB567144DB873FBBDAD8171D42968B97357F06BC1
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["8D+nOE33nrpuAnTVcJlgMPWVo79reBkp3Z22WTJi5B8="],"block_size":4096,"path":"_locales/nb/messages.json"},{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	181072
Entropy (8bit):	5.774426487043815
Encrypted:	false
SSDEEP:	
MD5:	1B40AC9ABB964672109D49ABFCFE2717
SHA1:	966E224F2887075825D42D2E7E0063BFAA81A99C

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

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	865
Entropy (8bit):	5.446082759099936
Encrypted:	false
SSDEEP:	
MD5:	05CD0CBAF4C0D701E284A82E9C77E07D
SHA1:	06D6D98A4AE7210DF999D53659C45EC048EC2416
SHA-256:	FC0A5897F57B0710F0B5A61F2A3FF412E015F6D47EAB89109265C72F9AE57735
SHA-512:	A3AF23AC1EDA4FBA97431EE91F7E975A6FFFF6EF768A79A35BAA7F11A033AF406B2F3EC9D2A53848F7446A88DC29472C1070489F158BADA195F475DC30314C02
Malicious:	false
Reputation:	low
Preview:	....."i....dik..https..ob6x6..si..aaa..adob..content..lgalmgawdq..mobilemoolah..net..plugins..wealthprogress..wp*.....aaa.....adob.....content.....dik.....https.....lgalmgawdq.....mobilemoolah.....net.....ob6x6.....plugins.....si.....wealthprogress.....wp..2.....6.....a.....b.....c.....d.....e.....g.....h.....i.....k..l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....w.....x...:x..... ..B.....8..... .....*.https://dik.si/OB6x62.:.....}..... .....*Thttps://wealthprogress.mobilemoolah.net/wp-content/plugins/lgalmgawdq/aaa/adob/adob/2.:.....J. .....$(+3;FJO

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

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

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4379
Entropy (8bit):	5.02202945231993
Encrypted:	false
SSDEEP:	
MD5:	1A666F1184C6D4FB77A1DA15B9E51F7C
SHA1:	53AA28A42399E9B7B29275058A5F23926AF95071

SHA-256:	3A3844A32ABA4ADB0E2965FB6E6D5E9BAA4C5908AB1A557E72996117E91B6AA8
SHA-512:	B93B7DC48DC6C6EE85E3130859FFEE1BF7BBFA2B4EF5C0260E47091B011D13CF0747D470A4CC537924E03A8C64C964B6BEA77EE0EF764E0CD798A42424549F4F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298163480826991","alternate_error_pages":{"backup":true},"autocomplete":{"retention_policy_last_version":92},"autofill":{"orphan_rows_removed":true},"browser":{"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"this_week_number":2734,"this_week_services_downstream_foreground_kb":{"115188287":51,"21145003":243,"35565745":2,"5151071":2,"88863520":1}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298163480825521"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1653689882.7186,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a.r\",[]]"},"gcm":{"product_category_for_subt

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16305
Entropy (8bit):	5.568150230320413
Encrypted:	false
SSDEEP:	
MD5:	4E4B9AD744E9D67195644F9F6D9F1816
SHA1:	62B07680161A95DD2F187634E91312B23B6AC050
SHA-256:	EFF0B7FB69050941E2E2DFE79E2A081FA4D18F89F233D1022811861202410367
SHA-512:	A0582784B0F201CA73BE585EB6933D25CCD84D467D5A6987F127B8F63684736D6B594B54A4B95E72667E499702A03F2334EF003633120AC60F4205D407C82595
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13298163479751140","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\ce1b6615-639b-40d0-89a2-f28631b5608e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16305
Entropy (8bit):	5.568150230320413
Encrypted:	false
SSDEEP:	
MD5:	4E4B9AD744E9D67195644F9F6D9F1816
SHA1:	62B07680161A95DD2F187634E91312B23B6AC050
SHA-256:	EFF0B7FB69050941E2E2DFE79E2A081FA4D18F89F233D1022811861202410367
SHA-512:	A0582784B0F201CA73BE585EB6933D25CCD84D467D5A6987F127B8F63684736D6B594B54A4B95E72667E499702A03F2334EF003633120AC60F4205D407C82595
Malicious:	false
Reputation:	low
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13298163479751140","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000006.dbtmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	

MD5:	AEFD77F47FB84FAE5EA194496B44C67A
SHA1:	DCFBB6A5B8D05662C4858664F81693BB7F803B82
SHA-256:	4166BF17B2DA789B0D0CC5C74203041D98005F5D4EF88C27E8281E00148CD611
SHA-512:	B733D502138821948267A8B27401D7C0751E590E1298FDA1428E663CCD02F55D0D2446FF4BC265BDCDC61F952D13C01524A5341BC86AFC3C2CDE1D8589B2E1
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000006.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Default\fcda211c-ffd3-45d2-a084-fc61f74add84.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):	4490
Entropy (8bit):	5.036726961842481
Encrypted:	false
SSDEEP:	
MD5:	ACC8034618E6F7C96E7FD3109102B1F8
SHA1:	B2BF3E5B5974A6AE7587771CF95E175CCD7096F7
SHA-256:	3D9C5D9EA0E571E13F0F491ECCC07CA24C8A22C22A856980805552B90B49AC03
SHA-512:	2F5AD966A49562EF4F4BD0F9E8EB3BBAE6E6DF207E1C577F1522E4B59FD75233F1F9D1F8C384116113B66920FDA11CD167F5E0109388D8DE3A8754215D4C884
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298163480826991","alternate_error_pages":{"backup":true},"autocomplete":{"retention_policy_last_version":92},"autofill":{"orphan_rows_removed":true},"browser":{"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"this_week_number":2734,"this_week_services_downstream_foreground_kb":{"115188287":51,"21145003":243,"35565745":2,"49601082":3,"5151071":2,"54845618":25,"82509217":10187,"88863520":1}},"default_apps_install_state":2,"domain_diversity":{"last_reporting_timestamp":"13298163480825521"},"download":{"directory_upgrade":true},"extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"last_chrome_version":"92.0.4515.107"},"gaia_cookie":{"changed_time":1653689882.7186,"hash":"2jmj7l5rSw0yVb/vlWAYkK/YBwk=","last_list_accounts_data":"[\"gaia.l.a

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Last Version

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.873140679513133
Encrypted:	false
SSDEEP:	
MD5:	3A0E5D4F452CF99191634D0FFAB744A0
SHA1:	F115BBB898EEFF640D8D19AD44A86C3FCDFFC0AD
SHA-256:	B9D528D3AE283039F4700C7E4E790744C58A26353A91B536DD91CBA4F648A35F
SHA-512:	87BF9DB30598EC454A02A4A32E5458E83870524D4AA497CB167C8A92B7521204B7B75E2BE18D61F9FBE51CA7DE8E35782AA65E6F6F11E4A4926A9B6C85D6528A
Malicious:	false

Reputation:	low
Preview:	92.0.4515.107

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	105157
Entropy (8bit):	6.034886974499159
Encrypted:	false
SSDEEP:	
MD5:	21F611838444D5AC217A484205BB81B3
SHA1:	20C37D309252CDA567DF00E5F1BB51E52DEEE481
SHA-256:	EF0CCBC4BA47C543B446D2B7E298F30EE0A10171A6B181DDEC4FFDCD8065BFCA
SHA-512:	907901FC7C09BCCE287E6EE59BB7D112408CB27A0E60BE110F0441E1C83370D3B60CE30D34960616C024565DACD35DCD8ED54CEFD5D847C74EC53F70D1E8739
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653689881782276e+12,"network":1.653657483e+12,"ticks":171695368.0,"uncertainty":2993445.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2IIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYeIlmLnfOlbhRQ"},"policy":{"last_statistics_update":"13298163479427840"},"profile":{"info_cache":{"Default":{"active_time":1653689880.650481,"avatar_icon":"chrom

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\CertCsdDownloadAllowlist.store_new

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	75
Entropy (8bit):	5.665289857076014
Encrypted:	false
SSDEEP:	
MD5:	69BA418A3AAA7E798AC9D2529D38450D
SHA1:	3CED151CA242772D33B65823C464983D25290971
SHA-256:	6A8B167A771891BE2FD100E5B9012A19C53CF2C78F2150BC1E1AA05A94EF5E24
SHA-512:	C85BC237929B44DCD3F5C35E6A0B59202CA4918ABCA2B94D7429BA77D772698B912412D726F66958F918B65FA03324183F8BC012D65E965B2B223E81B458EB5E
Malicious:	false
Reputation:	low
Preview:	.....A .:.....".0010.....B". ..B.....o.$'.A.d..L....xR.U

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\ChromeExtMalware.store_new

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1230942
Entropy (8bit):	4.0012345855525515
Encrypted:	false
SSDEEP:	
MD5:	0B403BC243C1962288CBCD6283D19BE2
SHA1:	B7811FD529BC482B690347A6B346BAD529E3D5D6
SHA-256:	9FB910F8C545F2EB7A44EF6D8F65DDF1BB1756C5376AF8A8065E7AFAEBC44B40
SHA-512:	411CBD7A89451F59141C227990A2D5E9E174D670A0D7B0B4C73AC68C7377101656B5519A7BBCFAAE4914DD988625C00493397D02722F81AE891B3AED6EA1DBEA
Malicious:	false
Reputation:	low

Preview:	.....K .*..K.....K. ...Kaaaadbolalgmogecpogmlebfkpigmpdjaaaaiognmpgbjoffachmpnnppfnokcbeaaaakngccdmgikgidoadpaopippmdfihaaadcbdjencpiphepfhhdebfocp bfddcaaaggnhhcicpemabkcpekihlocinhaalaaahfampijhmeembhjbebjebkeoedjjfaaaiinppadbheljngocoegdcncpaejiiaaakpbbojhipcodjiknnbjkafgjolnjnaaalhkjlldhojjcmm iaoopcglbdlfjcpaaamfohdgeiomgdngemljnheihdmgkecaaamnkbkbppehfhhkmiodoniifhfpkkaaaanfaliloicindpienfhcnpndcibpcgaaankgpdiealiomopmnjblmeimiejfdaaabajgb pmnmnmhdfmjmnbkbjpibhmefdaabchfpoaokbenfoikepjpdidacbiekfaabchjflcbccncldaekpjpcienceijonaabcnnmihfbpfblmeflmggaccdjlpfppaabefojcgchjbojmkeidhaceaaojj jodaabgniekficofjmfoejkgpncpaimldcmaablllpaogiigffnofgfhaecokpnhflghaaboihdfgkjdneohdofabaponaaibbdeaabpdmlmkpedpigeignclfmodjhpllljaacakdiakmgiollmahg dginnioeonmfbaacdffaeghaialcklmicpdlpnikjholcaacfcnecbpnccnonpbdgpbljaghhclaaaacgihcbcjhegjcfgkobdigjngohmjmfaacgmmndomhckgeglaphhdeegmonpbfjaacgncgin kjobaaiokjcmbjgjclgbgfaaacjmcdmclhpdpjagjcmclecpgjodlmgaackamlchlgmalkmcphbhhcjebbpnfdfaacoogimce

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\ChromeUrlClientIncident.store (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	717
Entropy (8bit):	7.722474810251154
Encrypted:	false
SSDEEP:	
MD5:	37780C7EE0D6A1144E43A63A5ED49A21
SHA1:	79FFFF451BCF7AFDCE2F097C652040BE96D5826A
SHA-256:	B853EF13A189F3C0D3EE863EEA03B5D9EC88BE70A1F3BEF0414058971A2601B7
SHA-512:	16A261856890DE359E68C54D060C3A04D1180DCDC18A73C5FD29B2672089C58A88A88C2A282242C6FE1367AB9D8251EB2A60395870ED2863B3C3A906CD564CF
Malicious:	false
Reputation:	low
Preview:	..... .*.....3))...o._.....m.../J.....;.Pv....<.xW...i>!4.<!.(".M.#*.C#ZCW$..k&.n.*`..+.....r70..+0>.12...7.0.8i..:e=q:m.c=\|..>f..?...C...F.O.H...H.4.ILWal.)!KB3.O3..P.{.Sc..S. ..W.+W..WYTV.ZC.IZ...[...[.sY\.fN\.++_3{._.)a_...`9..`{..a80.b...c.m>d39Adh..g.t,h.-\iI..k..o_..pe>Ns...u.2.v.=.yoU.z.b.z...z..$}.4...w.....,...1'..iV.....AO.z.6..{..[....9...;..e.....b.K. v[I.../..eM...m.....l.&...=.;....@S.....w..D.v...X..|.....9....Yk.....n.A...a..<..;.c..r;.9..."....o..q.....-...0,..&.Y.....W..3...Ft.sP...N.0Nh..b}..(.K$...Dr..9X.....>.Q.....8.. ..}u.h.W.y[P..~[.1.5...Y.....PO.....N.:.....".0010.....=...B". VE.1.r.;7...h.z(.6l)..#....,u.|

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\ChromeUrlClientIncident.store_new

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	717
Entropy (8bit):	7.722474810251154
Encrypted:	false
SSDEEP:	
MD5:	37780C7EE0D6A1144E43A63A5ED49A21
SHA1:	79FFFF451BCF7AFDCE2F097C652040BE96D5826A
SHA-256:	B853EF13A189F3C0D3EE863EEA03B5D9EC88BE70A1F3BEF0414058971A2601B7
SHA-512:	16A261856890DE359E68C54D060C3A04D1180DCDC18A73C5FD29B2672089C58A88A88C2A282242C6FE1367AB9D8251EB2A60395870ED2863B3C3A906CD564CF
Malicious:	false
Reputation:	low
Preview:	..... .*.....3))...o._.....m.../J.....;.Pv....<.xW...i>!4.<!.(".M.#*.C#ZCW$..k&.n.*`..+.....r70..+0>.12...7.0.8i..:e=q:m.c=\|..>f..?...C...F.O.H...H.4.ILWal.)!KB3.O3..P.{.Sc..S. ..W.+W..WYTV.ZC.IZ...[...[.sY\.fN\.++_3{._.)a_...`9..`{..a80.b...c.m>d39Adh..g.t,h.-\iI..k..o_..pe>Ns...u.2.v.=.yoU.z.b.z...z..$}.4...w.....,...1'..iV.....AO.z.6..{..[....9...;..e.....b.K. v[I.../..eM...m.....l.&...=.;....@S.....w..D.v...X..|.....9....Yk.....n.A...a..<..;.c..r;.9..."....o..q.....-...0,..&.Y.....W..3...Ft.sP...N.0Nh..b}..(.K$...Dr..9X.....>.Q.....8.. ..}u.h.W.y[P..~[.1.5...Y.....PO.....N.:.....".0010.....=...B". VE.1.r.;7...h.z(.6l)..#....,u.|

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\IpMalware.store_new

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	5.930473992176578
Encrypted:	false
SSDEEP:	
MD5:	8BE60835ACBD61B21BE993962E7CCB3F
SHA1:	4FE69E7D62317F1B718E1B02A8E016EA7C384EE3
SHA-256:	7CBA8B2699D54AFDBBDEC5299D51684D04C4FE4E4645866FF988C12BB2DDBA6F
SHA-512:	1F64E7054843BE448AF93C330239BB314ED107BA6EABC0E84484A178E051A7A0BECEADF241CE1ACA690940D17715ED535779CE0551DE9C94064E5543CFE0005 1
Malicious:	false
Reputation:	low
Preview:	.....` .*.....<.4N..E..:....."..0010...../B". .p.....\H...J#..).o.....(`....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlBilling.store (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48886
Entropy (8bit):	**7.996560207501968**
Encrypted:	**true**
SSDEEP:	
MD5:	5B99783DEFBFBEBF0B8BC48561BA9719
SHA1:	117AF9E2AC91B9372D0537F705E11870CE520393
SHA-256:	D8CB2358A14D429A4ACD4BECB02E0AD427CC64F5EA3E77CC64F86E2B0193D86E
SHA-512:	35903B9F8147B350DE09474A24B98373C57341CC8FC0C552FD578F05CA79F7F115663133732B3B4D01BDCC43661C69595D19211F3027777B86DC389BB689657D
Malicious:	false
Reputation:	low
Preview:	..... .*.....O.....v..X....J.....)..%...(....`X./...Bur.D$b.J:..O..P..S...Y...[XG._%Z.a]..eP..h.,.sY..zP1...3...8.....2...^...}.....E...%....c..P....&.....]&..~....._..P... L'.....<.....PA.#%e.,.I.1...8...H.0.M...Y1..\.m.`...e...g...mS..sY..y....c>.....3...../.....gp.....6.....&*..+=..(.....?V..T.....t.....@.....c[..r.....1L...U...E. ...$...%/^.&^..(...)x..:|..:,..:,...=...AA..E=..J...O...O.R.Q...R&b.X.r.a...e...m...t...t.E.v..~x.....(...Vc..i6...|.....t.....q.....p..s....9.....ow.....u.#...%.*.1...3i..7...9.r .<d,.<...>w].Aj..O.;.X...\k..r6..rw..|.`..t....2.....~..9.....rE.....,..I.....q...8..@@..6...I....!..h...:.....%L.....wA.03R.8m..>...E.,.H]..L?..TYq.V...]..._.9.`y..d.\.h.S.i...{.;.}.. ...o.....[.....F.....9.....p...]....6..~...P:..n...N....J..M.....8....<..5F....W.....[V..~.....a...B...#.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlBilling.store_new

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48886
Entropy (8bit):	**7.996560207501968**
Encrypted:	**true**
SSDEEP:	
MD5:	5B99783DEFBFBEBF0B8BC48561BA9719
SHA1:	117AF9E2AC91B9372D0537F705E11870CE520393
SHA-256:	D8CB2358A14D429A4ACD4BECB02E0AD427CC64F5EA3E77CC64F86E2B0193D86E
SHA-512:	35903B9F8147B350DE09474A24B98373C57341CC8FC0C552FD578F05CA79F7F115663133732B3B4D01BDCC43661C69595D19211F3027777B86DC389BB689657D
Malicious:	false
Reputation:	low
Preview:	..... .*.....O.....v..X....J.....)..%...(....`X./...Bur.D$b.J:..O..P..S...Y...[XG._%Z.a]..eP..h.,.sY..zP1...3...8.....2...^...}.....E...%....c..P....&.....]&..~....._..P... L'.....<.....PA.#%e.,.I.1...8...H.0.M...Y1..\.m.`...e...g...mS..sY..y....c>.....3...../.....gp.....6.....&*..+=..(.....?V..T.....t.....@.....c[..r.....1L...U...E. ...$...%/^.&^..(...)x..:|..:,..:,...=...AA..E=..J...O...O.R.Q...R&b.X.r.a...e...m...t...t.E.v..~x.....(...Vc..i6...|.....t.....q.....p..s....9.....ow.....u.#...%.*.1...3i..7...9.r .<d,.<...>w].Aj..O.;.X...\k..r6..rw..|.`..t....2.....~..9.....rE.....,..I.....q...8..@@..6...I....!..h...:.....%L.....wA.03R.8m..>...E.,.H]..L?..TYq.V...]..._.9.`y..d.\.h.S.i...{.;.}.. ...o.....[.....F.....9.....p...]....6..~...P:..n...N....J..M.....8....<..5F....W.....[V..~.....a...B...#.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlCsdAllowlist.store (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5115
Entropy (8bit):	7.963573947110426
Encrypted:	false
SSDEEP:	
MD5:	AF9C6A34368E7C2916C23D5E6A406E93
SHA1:	969433E292832A1AB86CB7CFBC7D7C0EBFBB2181
SHA-256:	0CBD52E1E61702E65676DA2C07EC317A2C82D3504E9610DB89C101049EA1B433
SHA-512:	FDF257CD47462C618FE49652DFE4BE3426D35FF4225B4E228B922693135C28B467267A311EE88C2C11CB2BBAAF8D70233A96C3C1DA9D8A31E42A91C96536E31D
Malicious:	false
Reputation:	low
Preview:	........' .*.....V&...vo.....O.....2p....!..^Q... ..6.....$...5..O.\.e....b..+.d.3...n.....s.....o.....|...b..4...p.X.....-7..8....J.."m.-7..b.>..Y....m...n.u.P..0`.....t#...E.....)..2m.....U.....1.!..O .Z...a.a../.....I...<.....1H...vm..~....+.....*.....>.\.....9....].` ...%..Q..)....:.m.....}..}....)..q.../...K...N...5...Y..."...vi..... ...;..f.....B..>W..r..,i.....x>..m...r.. G++.X.N.....W..#.a.4S..A.r..W..... ..X M.. ..!.D[!f..!..!.Z.!..!..."-.#"...#.b.#m.9#...$R..$...%2..%7s_%`..%z..&..'...'...'..'.W.(Z.(_z.(z.m(.+.(...(...(..I(.!.(..(...)..e)vV.*...*(U v+qS.+.1j,>.n,K.,.o0,. .,..,...-+W.-..}-.-.ml-.....=..LC..a.h.../..0..0*.0kV.0t.!0ul.0...1.w.1...1.9z1...2F.Y2..3..r3d..3u.B3.b.3...3...3...3.r.3...4ois4..84..4..5[M.5izF5.5.5..85..95.q? 5...6.V.7@KG8..y84.r8N<.8x..8..88.9.8...9.!.97..9DM.9E.V9j..9.[;_M.;..J<.q.<.3.<..=.m(=`'.=..>...>...?=.?Q.2?S..?p..?u.?.Md?.'.@...@...@...A-!.AM..Aj

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlCsdAllowlist.store_new

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5115
Entropy (8bit):	7.963573947110426
Encrypted:	false
SSDEEP:	
MD5:	AF9C6A34368E7C2916C23D5E6A406E93
SHA1:	969433E292832A1AB86CB7CFBC7D7C0EBFBB2181
SHA-256:	0CBD52E1E61702E65676DA2C07EC317A2C82D3504E9610DB89C101049EA1B433
SHA-512:	FDF257CD47462C618FE49652DFE4BE3426D35FF4225B4E228B922693135C28B467267A311EE88C2C11CB2BBAAF8D70233A96C3C1DA9D8A31E42A91C96536E31D
Malicious:	false
Reputation:	low
Preview:	........' .*.....V&...vo.....O.....2p....!..^Q... ..6.....$...5..O.\.e....b..+.d.3...n.....s.....o.....\|...b..4...p.X.....-7..8....J.."m.-7..b.>..Y....m...n.u.P..0`.....t#...E.....).. .2m.....U.....1.!..O .Z...a.a../.....I...<.....1H...vm..~....+.....*.....>.\.....9....].` ...%..Q..)....:.m.....}..}....)..q.../...K...N...5...Y..".'...vi..... ..;..f.....B..>W..r..,j.....x>..m...r.. G++.X.N.....W..#.a.4S..A.r..W..... ..X M.. ..!.D[!f..!..!.Z.!..!..."-.#"...#.b.#m.9#...$R..$...%2..%7s_%`..%z..&..'...'...'...'.W.(Z.(_z.(z.m(.+.(...(..(...(..l(.!.(..(...)..e)vV.*...*(U v+qS.+.1j,>.n,K.,.o0,. .,.,...-+W.-..}-.-.ml-.....=..LC..a.h.../..0..0*.0kV.0t.!0ul.0...1.w.1...1.9z1...2F.Y2..3..r3d..3u.B3.b.3...3..3...3.r.3...4ois4..84..4..5[M.5izF5.5.5..85..95.q? 5...6.V.7@KG8..y84.r8N<.8x..8..88.9.8...9.!.97..9DM.9E.V9j..9.[;_M.;..J<.q.<.3.<..=.m(=`'.=..>...>...?=.?Q.2?S..?p..?u.?.Md?.'.@...@...@...A-!.AM..Aj

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlCsdDownloadAllowlist.store (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	34141
Entropy (8bit):	**7.994763115034726**
Encrypted:	**true**
SSDEEP:	
MD5:	29DBFC0C369F8CD2973533008CFA1F11
SHA1:	893833F685E5BC722B80244BBCA1124ADC8125B8
SHA-256:	DBBD200AA0AC84FF7C56684D0203B0901A78C4A7DC39E88D0565728BBEFCBF91
SHA-512:	81BCA75DBE85DAEB9C381A3FDE15680A4770462758597F8BAC55DEA39A945E44FDA99DB48EC317F18451C5B19DCC4975B630F31C38B3BB60AE47F3C2341D84F5
Malicious:	false
Reputation:	low
Preview:	..... .*..... ....Nt.*HO5..*... ..UM..7<.....~.'.....V.W..;B.....ST....Fv.^}@/3w1@..U...wWG.(.....V....(' .J...w....&1.D.....n.&|.J=.....=...`H.l..G..... ..R..P.wS6.....\.D. <.....2..zH.dL...i.W..2.....%...2p..j<q.....I..M..H*.O_.i...p....B..)..m..Oty}...`.f.l.4.^...%i..d.lZ.$<R.W...J.....j.....a..g ,G".1...~.>.x.....7....J..@!t=..b..Q....;..l%8\|.n.....2z.%..;..3 J.;..S...VV..[.....%,....Yw...{`X..,_.....,..V}v%G....D.B...)O....m_.....J...`.6..._B]..;....?.$@v....9.fd.ee.O.O.e..L..5[..?....?..y.%..g....~8.B..p!.$.U..Af..F...mu...(....D..!0].A ..l59,....aa...T...Ql{(....R.<....u...b.cQ.iJ].....mh.u@..G..D.|FLz./d=...U.K.p.}.9.U|Ib...(n.y._..9.d....OC.....b..C.A|.8...\,..s....L.`f.....e....g....C^2.....:...V.../J....c..fPB&.t.....Xd..`+..'.. ..z_.[.....,....b.z9.[.....O&.1%.7r..=}.*....c.5.....!.m....h}.h.u.l).....tY..F....o|.....K.....S....C4al?.B1..c.....t....<H./...0.n...

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlCsdDownloadAllowlist.store_new

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	34141
Entropy (8bit):	**7.994763115034726**
Encrypted:	**true**
SSDEEP:	
MD5:	29DBFC0C369F8CD2973533008CFA1F11
SHA1:	893833F685E5BC722B80244BBCA1124ADC8125B8
SHA-256:	DBBD200AA0AC84FF7C56684D0203B0901A78C4A7DC39E88D0565728BBEFCBF91
SHA-512:	81BCA75DBE85DAEB9C381A3FDE15680A4770462758597F8BAC55DEA39A945E44FDA99DB48EC317F18451C5B19DCC4975B630F31C38B3BB60AE47F3C2341D84F5
Malicious:	false
Reputation:	low
Preview:	..... .*..... ....Nt.*HO5..*... ..UM..7<.....~.'.....V.W..;B.....ST....Fv.^}@/3w1@..U...wWG.(.....V....(' .J...w....&1.D.....n.&|.J=.....=...`H.l..G..... ..R..P.wS6.....\.D. <.....2..zH.dL...i.W..2.....%...2p..j<q.....I..M..H*.O_.i...p....B..)..m..Oty}...`.f.l.4.^...%i..d.lZ.$<R.W...J.....j.....a..g ,G".1...~.>.x.....7....J..@!t=..b..Q....;..l%8\|.n.....2z.%..;..3 J.;..S...VV..[.....%,....Yw...{`X..,_.....,..V}v%G....D.B...)O....m_.....J...`.6..._B]..;....?.$@v....9.fd.ee.O.O.e..L..5[..?....?..y.%..g....~8.B..p!.$.U..Af..F...mu...(....D..!0].A ..l59,....aa...T...Ql{(....R.<....u...b.cQ.iJ].....mh.u@..G..D.|FLz./d=...U.K.p.}.9.U|Ib...(n.y._..9.d....OC.....b..C.A|.8...\,..s....L.`f.....e....g....C^2.....:...V.../J....c..fPB&.t.....Xd..`+..'.. ..z_.[.....,....b.z9.[.....O&.1%.7r..=}.*....c.5.....!.m....h}.h.u.l).....tY..F....o|.....K.....S....C4al?.B1..c.....t....<H./...0.n...

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlMalBin.store_new

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1071499
Entropy (8bit):	**7.9998577894876**
Encrypted:	**true**
SSDEEP:	
MD5:	813830870D211EA5F0D0F2C435E989DB
SHA1:	3DB6EA9778E8D4DEB7ED952994193B96CFE781C4
SHA-256:	9336507C53C2E5BE7EF1EB2252EB2312665070E9E604484723324AF67B3F4CD5
SHA-512:	81975A51598BAE98A46B42D3C983C114AB73B6C5060875152A4FE7C8F5BD9BABC93E3D8DBCB9FC3EE5C909331B0222A690851DEA113C02F5418C950519814C0F
Malicious:	false
Reputation:	low
Preview:	.....A .*..A.....A.....A..-I..M*.....k....Z.....d.....h...}x...C...T.....Q;.....a....~.....a.....@...G...^J.....Y..+{../.....@V..A.....,..|..*...IH..... #.../.....d...s....#.....@...V....v.....8...u.....R..eX..h....=...7.....).....Q..M+.....S#..S...i,.....]..a}..e...h.....N..E.....x...r.....2...M.....%...&~..\.....] .....&.....1:..S...T...@..... ... .!.}.!.@.!.9.!N..!...!.L."..."*.."H."s.."x)."...#.7.#...#...$ ..$5..$JK.$.V.$...%y..%{..%|..%..%...&lf.&{..&...&.L.'...'.+.(P..(...(.4.(.q.)...).^.)C ..*.R.*...+B..+qr.,Zt.,d.,.....7..-...72..H...../0t./x../|./.../.../.../...0.P.0]..0~..0...0.m.1j..1...2.H.2"..26..2M..2...2.g.3C..3.,3...3...4.4.4..5.\.5...5#..5...5w..5...5...6...6}..6...6.P.6. .7.y.7...7D..7S..8.&.8.t.8.G.8r_.8.H.8...8..8.c.8..9>*.9...:!..:p":.:..:...;H..;...;...;.;j.<...<.7.="..=,..=F..=FL.=G..=V..=

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlMalware.store_new

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	375059
Entropy (8bit):	**7.999534580185113**
Encrypted:	**true**
SSDEEP:	
MD5:	AE40C4946495034F4EF2C7129C21648D
SHA1:	BDB314C13FFB7A0EB9221C37C642DCA61C682F8C
SHA-256:	A30DE08D5F76ACECD64C145A91D8200435DA38D2B17F9D72405E60FF07799EE3
SHA-512:	1D8E256165FE886EC73E5A414498C2CB93B6CB806EC4D50A07E8092A7EE7CFF93523E84EA5BAE8289987508C2CB9731759BE1F819E97571C368ADD21837E3C45
Malicious:	false
Reputation:	low
Preview:	..... .*.....~.....8.....\...P.....a.....2...8...<....V.....p.....d%.....5...q^..b...s....)..TM..w...../....Q.....$....:..../.....-....n.....@..... ....a.....!.^."...#N..$9Z.$A..%1$.%?I.%._.&9..'...'OH.'...(d..)E..)Sf.*.Z.+...+..0...1:Y.2...2.[.3C..3..4...70n.8.y.9L..9.H.:...:.I.;...<.V.=.).>/A.>. .>...>.1.@p8.A.{.A...A...B5<. C'..Dbf.D...EF..F.3.G.{.G.k.HD..HS..H...I...J...Kx..K...L...N...P...Ph..Q@V.Q..R.'.R.n.S.6.T:..V.U.W...W.R.X...Y...Y.Q.Z...Z...Z...Z...Z...[...[.a.\...\.w.]..^R..^Y).^...^.3._B.._. ..c...c...c...d3..e.C.ffS.g.&.i...i..i..j...j9%.j.%.I...m.9.p[..qz..sw].s.n.t...t*..t+..u..u..vG..vG..w.^.z...{.8.{.Y.{...|.m.|D..}6..}QB.~Ph.~.!..r(.....P.....I.....7...jh..A....(...$..'..... . .....y.....?t...,.....c..N}..nU.....q.....,.....0.....g..v.....6...K(..ZQ...X.....).....F...TA..E8.....3...V...gt.../..Sr.....&.....7...xa..

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlUws.store_new

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	135915
Entropy (8bit):	**7.998561599785015**
Encrypted:	**true**
SSDEEP:	
MD5:	DB60D7D52510E6D6BBBCA5F1366189DC
SHA1:	89BEEC4A66C3D50B0B4BFEC2C40D257364FAABD9
SHA-256:	5464271315A0AA7B4BDBCAE51AA3F6C31EE736C96F70A107674E0C17281B3FC7
SHA-512:	D68E091ABDA8BFDB2300E7D08D9B4B9B384A33B0ED2C14F027EE0424DDEA3420B8ED0B368B3D88A0B567D8C403121A39761D08EDFDCE745B9ADE20C527A7C5BF
Malicious:	false
Reputation:	low
Preview:	..... .*.....E....x...G..5+.....q...o...T..3&.....j..... 2..O....X.....y.....#..$\..%S6.)...)...-....h\./...3...4...5...8...8...?x..GDw.L[n.O...O...PAN.P...P...Q...U. [.U8..U[c.W...W...ZP..Z...\.3.\...].;.^..._..g...i.O.j...k.#.o5a.qQ..qS..si%.s...w.r.y.y.}.....Q.....0.....R....7.....P..+5..Y.....I...H...%.....i..$g.....Z.....>.....;7... ..D8..7K..MJ....*.....i.....F..W6...!..6.....(....P..[J.....Q...dW.._+.....3z.....*...x...g.....$...0K.._.....?..en.$.\.%3F.%;..*...../.I.5...:w..:. ..;...;.6.@.K.A.?.EN&.F...G(..H8..K...M.h.M...N?..S...T...[...\...]...c...dm..e.d.f...g.^.j.!.k>..l...o.W.q.7.s0B.t D.u8..v.W.w...x(D.ymk.y.1.|.?.~V<..0.....Y6..f.....+... s...|k.....4.....b|...b...@.....?..C....C.....|..4.....8...~.....'.....,.....G....;..v.....

C:\Users\alfredo\AppData\Local\Google\Chrome\User Data\c94138de-6848-4f43-b71b-e76ac760e80c.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):	105269
Entropy (8bit):	6.035782118314814
Encrypted:	false
SSDEEP:	
MD5:	FF6FC78476ECB78274EAEE97AA3B7C8F
SHA1:	BE7340FFB6F0F20DF4850516E79D47AC064C7EAB
SHA-256:	A0292FF08DDDC95FBF8864CAA5C8F01AA7B54164D5CCB214531AAAAA2C71893B
SHA-512:	C22679C957CDA0408AF02423757D755A773FB8D6246F706AC0FEEA61D1D1BD94FEA3ECCCC609F9392C90679F4DAA7F5E2B31B2EE4EBE09DDCFE6AD5B17937 17D
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"91.0.4472.77"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653689881782276e+12,"network":1.653657483e+12,"ticks":171695368.0,"uncertainty":2993445.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABBQ7WxpM2gT7fMNkY5iRxkAAAAAAIAAAAAABBmAAAAAQAAIAAAALDWDwoLRYqp0NkiPsTxUN2QcOPsitaJrdacpo+ULE2PAAAAAA6AAAAAAgAAIAAAAOIeKQBWbQSCqXv1OSNS2lIZGHfAdJRwvbkapN4/FWvwMAAAAPz8I/w07KQb4Ut8ObsBGVgFwbuU88R362cCGZpNEtOEILJDMaKWOA4Y9ejBRTt5kEAAAADq8RkIezfgqGPgEaEMkhoGd9qhyBeyucXcRUPEI7mgYIxaDt8C5FJrjkEhV5EOUcUmR2SCzqYelImLnfOlbhRQ"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13288110187718326"},"policy":{"last_statistics_update":"132981634794278

C:\Users\alfredo\AppData\Local\Temp\272f4f39-0e9b-4c7e-b99d-40cb357b043d.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326(88
Malicious:	false
Reputation:	low
Preview:	Cr24.............0.."0...*.H............0..........\7c.<........Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.......[...L|....3>/....u.:T.7...(.yM...?V.<?........1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.......b1.......(.u^.'z......v.F.W.X4."-*eu...b.........\..F!...b...l5....zJ.q.......L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.......N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.......0..0...*.H...........0.......).'..b.*$w\$.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.................I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.............r...2..+Y.I...k..bR.j5Sl..8.......H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\alfredo\AppData\Local\Temp\6556_1793275814\SortingLshClusters

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33872
Entropy (8bit):	2.0569169245781995
Encrypted:	false
SSDEEP:	
MD5:	0F63C5027C2425412AFDE4B88D9BDDE8
SHA1:	98457E193D6DD71525AEB3F48CD13B6455C35B9F
SHA-256:	C8232B6128DC4759DB73245BD110589BA2D910DB20FB6367AFB6E6D9E4C1F54B
SHA-512:	9C98F0F257456B542EF0177F513F07440165468DB4B01342A009210554079186FC03E61E0BF92ABED35A51B6578A263197A9061F699EF960CDEE85553D0BCDEE
Malicious:	false
Reputation:	low
Preview:	#"b####""#########c####""#$#######""""#""#""############""#""################$$$$$$$$$$$$#######$$$$$$$$$$$$########$##$########""#$##$$######""#$##########""#""#$$#####$##$$$$$$$$$$$$$$$##$$$$$$$$$$$$$$$cc#ccc"b"b$######ccbbccc"aa"b######""#####""#""##########""#""#"!!""$#####""#$##$##$$$$#c##$##$$$$$$$####$$$$$$$##$$$$######""#$##$##cc"b#""#"a!#$##$""#####""#""#$##$####""#""#"!!#$####""#$##$$$$$$$$$##$$$$$$$$$$$$$$##$$$$#c##############c######$##$##"""""""""""#"""###########""#""#$##########$$$$$d$$$$$$$$#######$$$$$$$##$$$$c"b##bb##########c###c#""#$##$##"""""""#""#""#########""###"b#""#####$######$$$$$$$##$$$$$$####$$##$$$$##$$$$$$cccc##""bb$######ccbbcccbb"b$##########""#""""#######""#""#"!!""$####""#$######$$$$d##$##$$$$$##$##$$$$$##$$$$$$####c#""#######""#cc"b#"b#"!!""$####""#####""#"!!#######""###""#""#!!!!#$####""#$##$##$$$$$$$$$$$$$$$$$$$$$$$$$$$$$#c######$$$###c######$$$########""###$##$######""#$$$##$$$$$$$$$$$##$$$$$$$$$$$$$$$$$$$$$##$$##$$$$####$$$$$$##$####$$$$$$$$

C:\Users\alfredo\AppData\Local\Temp\6556_1793275814\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	122
Entropy (8bit):	4.549343645753808
Encrypted:	false
SSDEEP:	
MD5:	441350F2F2F1F5726A84E989F3F9BF91
SHA1:	C9530224671F181AE8ED47DBA82741B8AD920EA9
SHA-256:	3640148F4EADB7D60185671799C27A8C530295076AF9179705EAA6D4C544D627
SHA-512:	5AC785E7F3A35035B4958B2EF33534AB6E0448CDC5A5A881911123545930DAAFF6759AB2AB663327525A496E306CC1C98FD5F0EE079E2C6D92C47FD0CFAB51D E
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "Federated Learning of Cohorts",. "floc_component_format": 3,. "version": "1.0.6".}

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1293
Entropy (8bit):	4.132566655778463
Encrypted:	false
SSDEEP:	
MD5:	D7A97183BCBD5FB677AA84D464F0C564
SHA1:	CDBB279B864E2C0A51E0892B8714131802586506
SHA-256:	76EFAD74EB8256B942727C42261147EB9CCA48DA284DB3CDCE5DC6A3B4346F02
SHA-512:	36F0310DD06319E4A51F77E4C3D64F6276891CE6410FE2571324BB71F2FBCDA368EAC4267FF8268086BE6912E41787D0F70771755E3D49E3E8C26648EAC6EFC9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u041f\u043e\u043d\u0430\u0441\u0442\u043e\u044f\u0449\u0435\u043c \u043d\u044f\u043c\u0430 \u0434\u043e\u0441\u0442\u04 42\u044a\u043f \u0434\u043e \u043f\u0440\u0438\u043b\u043e\u0436\u0435\u043d\u0438\u0435\u0442\u043e.","craw_connect_to_network":{"message":"\u041c\u 043e\u043b\u044f, \u0441\u0432\u044a\u0440\u0436\u0435\u0442\u0435 \u0441\u0435 \u0441\u0435 \u043c\u0440\u0435\u0436\u043e.","app_name":{"message":"\u041f \u043b\u0430\u0449\u0430\u043d\u0438\u044f \u0432 \u0443\u0435\u0431\u0433\u0430\u0437\u0438\u043d\u0430 \u043d\u0430 Chrome"},"app_descr iption":{"message":"\u041f\u043b\u0430\u0449\u0430\u043d\u0438\u044f \u0432 \u0443\u0435\u0431\u0433\u0430\u0437\u0438\u043d\u0430 \u043d \u0430 Chrome"},"iap_unavailable":{"message":"\u041f\u043e\u043d\u0430\u0441\u0442\u043e\u044f\u0449\u0435\u043c \u043d\u044f\u043c\u0430 \u0434\u043e \u0441\u0442\u044a\u043f \u0434\u043e \u0432\u0433\u0440\u0430\u0434\u0435\u043d\u0430\u0442\u0430 \

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	556
Entropy (8bit):	4.768628082639434
Encrypted:	false
SSDEEP:	
MD5:	58BA5F65ED971591D1F9D81848EE31D0
SHA1:	BDA3C8B74653334FC8F060CAFBCEA58DF0113AB7
SHA-256:	CDD91587F5AF2C865776B36A5E9A07B10D21B9D911DE0B814B7A1E94B14AE885
SHA-512:	BA2A6BAA3011A54E6B07E29DFD133009D66B6CFFF525DEC0024BDE55A9BED463AD130307EE64BFB4A983A11FFD6B44BD53ED38EB144083A2CBEFA8D85C4D 5D41
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Ara mateix aquesta aplicaci\u00f3 no est\u00e0 disponible."},"craw_connect_to_network":{"message":"Connecteu-vos a una xarxa ."},"app_name":{"message":"Sistema de pagaments de Chrome Web Store"},"app_description":{"message":"Sistema de pagaments de Chrome Web Store"},"iap_un available":{"message":"La funci\u00f3 Pagaments a l'aplicaci\u00f3 no est\u00e0 disponible actualment."},"please_sign_in":{"message":"Inicieu la sessi\u00f3 a C hrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\cs\messages.json

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

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	505
Entropy (8bit):	4.795529861403324
Encrypted:	false
SSDEEP:	
MD5:	31264DDBF251A95DE82D0A67FA47DB3A
SHA1:	3A48DC7AF26A153594C7849E1D92AAC31296459B
SHA-256:	EDB51898A6C73D0090D6916B7B72EBAC71E964EABB5BA7CD68E21966024F0D23
SHA-512:	B97D61BD71E3F0A91FF1048D2ACAD4BC092CCAF157B7A96029B6AB5AF1812B01814E3153CD894307CB13DC132523EAC22B19CADA6B97F4B81B0D1132562317 B5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Appen er ikke tilg\u00e6ngelig i \u00f8jeblikket."},"craw_connect_to_network":{"message":"Opret forbindelse til et netv\u00e6rk."},"app_name":{"message":"Betalinger i Chrome Webshop"},"app_description":{"message":"Betalinger i Chrome Webshop"},"iap_unavailable":{"message":"Betaling i appen er ikke tilg\u00e6ngelig i \u00f8jeblikket."},"please_sign_in":{"message":"Log ind p\u00e5 Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	516
Entropy (8bit):	4.809852395188501
Encrypted:	false
SSDEEP:	
MD5:	7639B300B40DDAF95318D2177D3265F9
SHA1:	BF9EFDF073231CB3FCFCA5CCCA25B079ECFC45BD
SHA-256:	356A9D4ADFEC484DA824E7A72059B724B1686FC90082F4A4B667630436D593B0
SHA-512:	70593318C6626B5D25729E8D8109D5611B95283266621BE60ADD7E60C0DD5BC43848E956C767251B7B3CCDF5A0929922DE38F90CC8632CCD0C1CCFC7D6DEFE 9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Die App ist momentan nicht verf\u00fcgbar."},"craw_connect_to_network":{"message":"Bitte stellen Sie eine Verbindung zu einem Netzwerk her."},"app_name":{"message":"Chrome Web Store-Zahlungen"},"app_description":{"message":"Chrome Web Store-Zahlungen"},"iap_unavailable":{"message":"In-App-Zahlungen sind momentan nicht m\u00f6glich."},"please_sign_in":{"message":"Bitte melden Sie sich in Chrome an."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\el\messages.json

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

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\en\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\es\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	510
Entropy (8bit):	4.719977015734499

Encrypted:	false
SSDEEP:	
MD5:	1FD5DAF46C4D7C4F571C263EC37B943B
SHA1:	A57EE5EF6861F88005C2230EA3D633A1B4CA105A
SHA-256:	BCC2CF06F66E9E3BB4B7887D0EE0AE4A72A6C49F4B2A578A7733B78208984417
SHA-512:	79C3104F1DC51B17B062803209029C8165DBD391FBE0B69BB406D7B4F92FE1898CAC30E20C2E5CFB65D643B978095626C68EAA0CFCA064354D52D52D16BF21A 9
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Esta aplicaci\u00f3n no est\u00e1 disponible en este momento."},"craw_connect_to_network":{"message":"Con\u00e9ctate a una r ed."},"app_name":{"message":"Sistema de pagos de Chrome Web Store"},"app_description":{"message":"Sistema de pagos de Chrome Web Store"},"iap_unavailable": {"message":"En este momento, Pagos En-Apps no est\u00e1 disponible."},"please_sign_in":{"message":"Accede a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	460
Entropy (8bit):	4.679279844668757
Encrypted:	false
SSDEEP:	
MD5:	0293A7BAE6EEE62C4067A80E262D6A2D
SHA1:	E76B07BD49FFBBFB6841B7335CBE7A9620714402
SHA-256:	D06F20D4D68D1DBB89EF7D8E405D9499CB2EB2560217CD5B4A51AB1DD50CAB44
SHA-512:	8BF97DA4038A9C4426A285D5FEF0953F4E7E6D0667091A39DE4D4C5B4C35FC7B6A804425DBB4B82356A93950738E4F0937DE1AD777AE75AAC9BFB97D63F771B 0
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Rakendus pole praegu saadaval."},"craw_connect_to_network":{"message":"Looge \u00fchendus v\u00f5rguga."},"app_name": {"message":"Chrome'i veebipoe maksed"},"app_description":{"message":"Chrome'i veebipoe maksed"},"iap_unavailable":{"message":"Rakendusesisesed maksed ei ole praegu saadaval."},"please_sign_in":{"message":"Logige Chrome'i sisse."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\fi\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	515
Entropy (8bit):	4.699741311937528
Encrypted:	false
SSDEEP:	
MD5:	658DAD2AF2DC3AC1567D84E8B95F68B0

SHA1:	EE1121215960EC5ED5F7B6BDB8E4680731EBF83D
SHA-256:	978BA6D814CF290016833BBAC22DC7C05C2C575B1D6429B9BB14F8C2156BCF29
SHA-512:	F2FB93245D80E2CB2CA1BB2B0654FE92AD9041A558850D78AF4031CB83D2AD3BF5ABCFE6BC32160D028CA3914FA69A64784858A34FA56389C08D52B316346A0 5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Kasalukuyang hindi available ang app."},"craw_connect_to_network":{"message":"Mangyaring kumonekta sa isang network."},"app_ name":{"message":"Mga Pagbabayad sa Chrome Web Store"},"app_description":{"message":"Mga Pagbabayad sa Chrome Web Store"},"iap_unavailable":{"message" :"Kasalukuyang hindi available ang Mga Pagbabayad na In-App."},"please_sign_in":{"message":"Mangyaring mag-sign in sa Chrome."},"jwt_retrieve_failed":{"message" :"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\fr\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\hi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1055
Entropy (8bit):	4.454461505283053
Encrypted:	false
SSDEEP:	
MD5:	B739E3B798D3EEB8AFB3E368455A8E97
SHA1:	56E206DD0AC7EB7B179911BE3F7DD78059CBD4F3
SHA-256:	BA7A53A1398168719F2ACD58CC5FE06AB0B769ECA896D70E7208B18085B42FFA
SHA-512:	181A3B1275D1D17BD48EAA77805981A96E22589A38990214AF3ED029C4A37C2F05ECF747D8FCF816C2AAED6EF82403757F234D67C360A3A6E5DB6C3F59CA1A0 C
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u0910\u092a\u094d\u0932\u093f\u0915\u0947\u0936\u0928 \u0907\u0938 \u0938\u092e\u092f \u0909\u092a\u0932\u092c\u094 d\u0927 \u0928\u0939\u0940\u0902 \u0939\u0948."},"craw_connect_to_network":{"message":"\u0915\u0943\u092a\u092f\u093e \u0928\u0947\u091f\u0935\u0930 \u094d\u0915 \u0938\u0947 \u0915\u0928\u0947\u0915\u094d\u091f \u0915\u0930\u0947\u0902."},"app_name":{"message":"Chrome \u0935\u0947\u092c \u0938\u094 d\u091f\u094b\u0930 \u092d\u0941\u0917\u0924\u093e\u0928"},"app_description":{"message":"Chrome \u0935\u0947\u092c \u0938\u094d\u091f\u094b\u0930 \u0 92d\u0941\u0917\u0924\u093e\u0928"},"iap_unavailable":{"message":"\u0907\u0928-\u0910\u092a \u092d\u0941\u0917\u0924\u093e\u0928 \u0905\u092d\u0940\u0940 \u 0909\u092a\u0932\u092c\u094d\u0927 \u0928\u0939\u0940\u0902 \u0939\u0948."},"please_sign_in":{"message":"\u0915\u0943\u092a\u092f\u093e Chrome \u092e\ u0947\u0902 \u0938\u093e\u0907\u0928 \u0907\u0928 \u0915\u0930\u0947\u0902."},"jwt_retrieve_failed":

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	503
Entropy (8bit):	4.819520019697578
Encrypted:	false
SSDEEP:	
MD5:	9CF848209FF50DBF68F5292B3421831C

SHA1:	D29880B7B15102469123D8747BF645706CE8595B
SHA-256:	EA1744C3CFBAA684A31A00067E8493ED114EFF3E878C797C9C55A7B122D855CD
SHA-512:	B784AEE4926F850F30072ABDA85E2E2E3966285F14BDF647BD2A41C5C06CAB04BC962584830E4E913896010396EAD02D90528235B9D9EDA1BDEFBFBB5333EDF5
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"Aplikacija trenuta\u010dno nije dostupna."},"craw_connect_to_network":{"message":"Pove\u017eite se s mre\u017eom."},"app_name":{"message":"Pla\u0107anja u web-trgovini Chrome"},"app_description":{"message":"Pla\u0107anja u web-trgovini Chrome"},"iap_unavailable":{"message":"Pla\u0107anje u aplikaciji trenuta\u010dno nije dostupno."},"please_sign_in":{"message":"Prijavite se na Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\hu\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\id\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\it\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	464
Entropy (8bit):	4.701550173628233
Encrypted:	false
SSDEEP:	
MD5:	BB9C32BA62DDA02F9471C64B5F9CF916
SHA1:	9825037D5D9185C58456CDD887C77B10A41D8C84
SHA-256:	43A0B113D3773BA78F82BB9E42DDC46F6892D0FBBB351F94A7C105E4A146E9C1
SHA-512:	4D3DB91A6251F2DD9CBF97D29805A7AC23F49988966E9B686D486B4A8CEBEA33F5502E3891D5231674061127C282C745FB87FDA7467A6172851BF6925506C8CA
Malicious:	false

Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"App al momento non disponibile."},"craw_connect_to_network":{"message":"Collegati a una rete."},"app_name":{"message":"Pagamenti Chrome Web Store"},"app_description":{"message":"Pagamenti Chrome Web Store"},"iap_unavailable":{"message":"La funzione Pagamenti In-App non \u00e8 al momento disponibile."},"please_sign_in":{"message":"Accedi a Chrome."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	806
Entropy (8bit):	4.671841695172103
Encrypted:	false
SSDEEP:	
MD5:	96C8CBD161D3CE9CB1A46CB2CD0C6583
SHA1:	78BBFCF035B5B620E353C8E520653ADD3F4E7DB8
SHA-256:	81D8F1D9F72B3139BC5D9845BCF82990308FB6175D07514D8238B1E6D5D02E8A
SHA-512:	692468B7B44D961D8248BBC30CC11DE9F3F7E89D01A609E6CB71CAF653D8212C15DFA834C5FB6E8261FD21A25E9616861C0A3FC01DB27CBBE79C3FDE2C654 DD
Malicious:	false
Reputation:	low
Preview:	{"craw_app_unavailable":{"message":"\u30a2\u30d7\u30ea\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u305b\u3093\u3002"},"craw_connect_to_network":{"message":"\u30cd\u30c3\u30c8\u30ef\u30fc\u30af\u306b\u63a5\u7d9a\u3057\u3066\u304f\u3060\u3055\u3044\u3002"},"app_name":{"message":"Chrome \u30a6\u30a7\u30d6\u30b9\u30c8\u30a2\u6c7a\u6e08"},"app_description":{"message":"Chrome \u30a6\u30a7\u30d6\u30b9\u30c8\u30a2\u6c7a\u6e08"},"iap_unavailable":{"message":"\u30a2\u30d7\u30ea\u5185\u30da\u30a4\u30e1\u30f3\u30c8\u306f\u73fe\u5728\u3054\u5229\u7528\u3044\u305f\u3060\u3051\u307e\u305b\u3093\u3002"},"please_sign_in":{"message":"Chrome \u306b\u30ed\u30b0\u30a4\u30f3\u3057\u3066\u304f\u3060\u3055\u3044\u3002"},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\ko\messages.json

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

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	576
Entropy (8bit):	4.846810495221701
Encrypted:	false
SSDEEP:	
MD5:	41F2D63952202E528DBBB683B480F99C
SHA1:	9DD998542DBE6609299D4A5A25364A32FA7D7865
SHA-256:	FF7C083CD1E6134DD8263C634336EB852274BAD1BFAD18762814C42BC65309D8
SHA-512:	7BD2E2D4264C6BD62DF2584F3C1D3A910C5C5A28F4532F1E8F0C2235E93714EDD6074EA24960D4DEB4F9125DA81CA813F06330EFF66FA8DF1552D1DAC68644 E
Malicious:	false
Reputation:	low

Preview:	{"craw_app_unavailable":{"message":"Programa \u0161iuo metu negalima."},"craw_connect_to_network":{"message":"Prisijunkite prie tinklo."},"app_name":{"message":"\u201eChrome\u201c internetin\u0117s parduotuv\u0117s mok\u0117jimo sistema"},"app_description":{"message":"\u201eChrome\u201c internetin\u0117s pard uotuv\u0117s mok\u0117jimo sistema"},"iap_unavailable":{"message":"Mok\u0117jimai programoje \u0161iuo metu negalimi."},"please_sign_in":{"message":"Prisijunkite prie \u201eChrome\u201c."},"jwt_retrieve_failed":{"message":"The transaction could not be completed."}}.

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "cr aw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be c ompleted.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F6 32
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ....-..... Chrome".. },.. "app_name": {.. "message": "..... ....-..... Chrome".. },.. "craw_app_u navailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "..... . .....".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... . Chrome.".. }.. }..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59 D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplik.cia moment.lne nie je dostupn..".. },.. "craw_connect_to_network": {.. "message": "Pripojte sa k sieti.".. },.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be com pleted.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
MD5:	3943FA2A647AECEDFD685408B27139EE
SHA1:	0129DD19D28373359530B3B477FE8A9279DABB7D
SHA-256:	18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
SHA-512:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC(9D
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_unavailabl e": {.. "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\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
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\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
MD5:	D372B8204EB743E16F45C7CBD3CAAF37
SHA1:	C96C57219D292B01016B37DCF82E7C79AD0DD1E8
SHA-256:	B8BA77E0089B0676545EC16D32468B727812B444F90B33A7A5B748E6C36C4388
SHA-512:	33640529E0D5DCC5CA4BDB0615A2818E8D26C6FCB7B3474C08AC3EB67B9DB40E1F0A79954ED20728CD47A686D2533DCBC76ABCBDB917F8530C8DE8BBA687 52E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalning via Chrome Web Store".. },.. "app_name": {.. "message": "Betalning 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_unavai lable": {.. "message": "Betalning i appen .r inte tillg.ngligt f.r n.rvarande.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logga in i Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
MD5:	83E2D1E97791A4B2C5C69926EFB629C9
SHA1:	429600425CB0F196DDD717F940E94DBD8BFF2837
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\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
MD5:	2CEAE0567B6BB1D240BBAD690A98CA3B
SHA1:	5944346FBD4A0797B13223895995CAB58E9ECD23
SHA-256:	A7CB86F30C9C31FE5540282C308BA96ADB4EC16EF98C87129EB88105E5BEF5FC
SHA-512:	108A07C6D03D7178E8D0FFEF5349E0249A898D864964FED8757BD8A08BC1C6D9613F2A6C01AA34A6606127D1C6CE14C229FA02586677DBB060B85E3E845950E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "app_name": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "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\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
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\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
MD5:	7EBB677FEAD8557D3676505225A7249A
SHA1:	F161B4B6001AEAEAB246FF8987F4D992B48D47BE
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 compl eted.".. },.. "please_sign_in": {.. "message": "Vui l.ng ..ng nh.p v.o Chrome.".. }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	
MD5:	BB73BF561BB79F89D9BF7C67C5AE5C65
SHA1:	2FADD3A1959B29C44830033A35C637D0311A8C9C
SHA-256:	D804F2A040D21D7511EFD5213D8E1721D64964A1A0DBB48E21622CEEDC9D967E
SHA-512:	627D44CEF1FE5C5ABD598BD47FF5E22B9EFC1CF98DDE3868FA9E5896C134A0C9C055AC34EDDADAE56B6690E51AEA89965D38F770552A85C732CC796795DC6 8D2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ....."... },.. "app_name": {.. "message": "Chrome ....."... },.. "craw_app_unavailable": {.. "message": "..... ."... },.. "craw_connect_to_network": {.. "message": "....."... },.. "iap_unavailable": {.. "message": "....."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "... Chrome."... }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\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:	modified
Size (bytes):	634
Entropy (8bit):	5.386215984611281
Encrypted:	false
SSDEEP:	
MD5:	5FF50C673CC0C661D615F0CFD0E6DCA0
SHA1:	60DFF98DEAB9C4746B288BDD9C94B3BCAE5EAA85
SHA-256:	C6F8C640F3353A7B9B1432A0C139C1AEEC40133800E6C9B467B63991AD660308
SHA-512:	361D62D91F4931C5F34092C9F2C6A5323D5EEB82A24E7ABE11F7817D8D66341C0ECAD4DCB4B10873920C8D6A3CC9F5704889E178EB2549001A9F62BEDF6C80 9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ....."... },.. "app_name": {.. "message": "Chrome ....."... },.. "craw_app_unavailable": {.. "message": ".. ....."... },.. "craw_connect_to_network": {.. "message": "....."... },.. "iap_unavailable": {.. "message": "....."... },.. "jwt_retrieve_failed": {.. "message ": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "... Chrome."... }..}..

C:\Users\alfredo\AppData\Local\Temp\scoped_dir6556_981249767\CRX_INSTALL\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1098
Entropy (8bit):	4.919185521409901
Encrypted:	false
SSDEEP:	
MD5:	6CA25F3EF585B63F01BCDF8635120704
SHA1:	00C063811E31EA5F9A00F175A71EA25E7821F621
SHA-256:	49D9DE983F7436BA786E6E04A5A20C10F41687AE06B266B1B6553F696719563D

SHA-512:	566BFD9BADBD8951EE52E5911EB68B51E86286989096D32DE6E32A2523761B0E0AFCA251EF3BEA36B5D51FB8354A5FCA567772A02C3F3B9D8DFE529609FA043 0
Malicious:	false
Reputation:	low
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "name": "__MSG_APP_NAME__",. "description": "__MSG_APP_DESCRIPTION__",. "manifest_versio n": 2,. "version": "1.0.0.6",. "minimum_chrome_version": "29",. "default_locale": "en",. "app": {. "background": {. "scripts": [. "craw_background.js".]. }. },. "permissions": [. "identity",. "webview",. "https://www.google.com/",. "https://www.googleapis.com/*",. "https://payments.google.com/payments/v4/js/integr ator.js",. "https://sandbox.google.com/payments/v4/js/integrator.js".],. "oauth2": {. "auto_approve": true,. "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.read only".],. "client_id": "203784468217.apps.googleusercontent.com". },. "icons": {. "16": "images/icon_16.png",. "128

C:\Users\alfredo\AppData\Roaming\Microsoft\Spelling\en-US\default.dic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	low
Preview:	..

Static File Info

No static file info