ID: 632519
Cookbook: browseurl.jbs
Time: 18:35:21
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

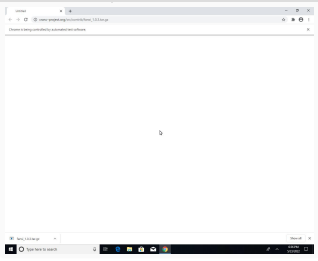
Windows Analysis Report

https://cran.r-project.org/src/contrib/fansi_1.0.3.tar.gz

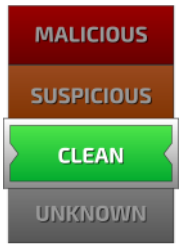
Overview

General Information

Sample URL:	http://https://cran.r-project.org/src/contrib/fansi_1.0.3.tar.gz
Analysis ID:	632519
Infos:	



Detection

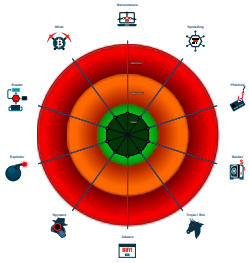


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 1560 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://cran.r-project.org/src/contrib/fansi_1.0.3.tar.gz MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2464 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1568,6762221054703538292,1348112329409344656,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6584 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=quarantine.mojom.Quarantine --field-trial-handle=1568,6762221054703538292,1348112329409344656,131072 --lang=en-GB --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=4772 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

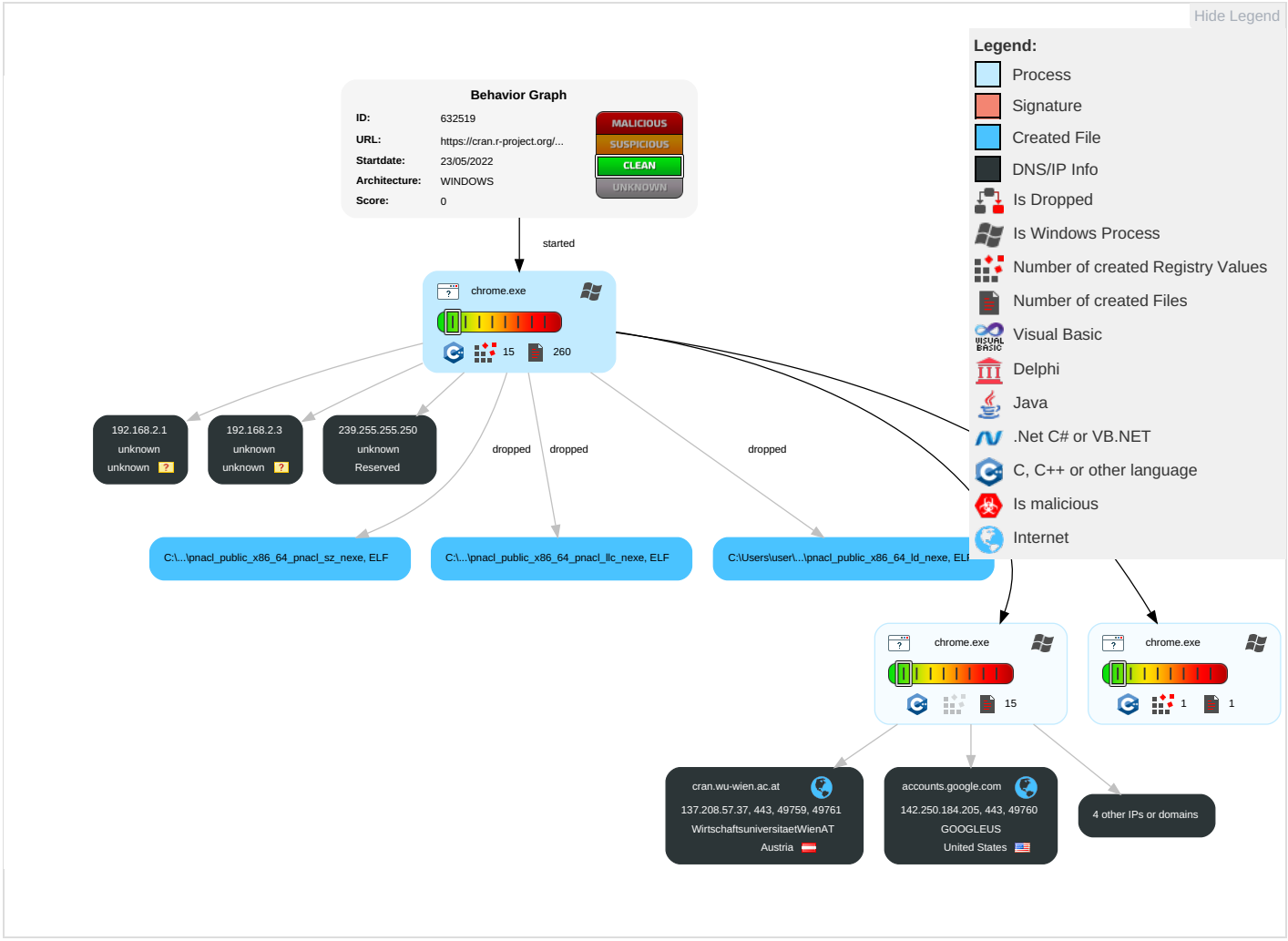
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

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

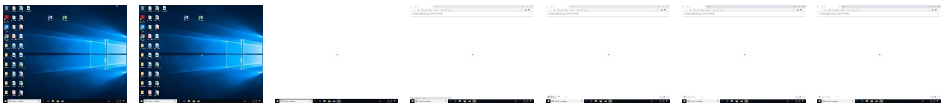
Behavior Graph

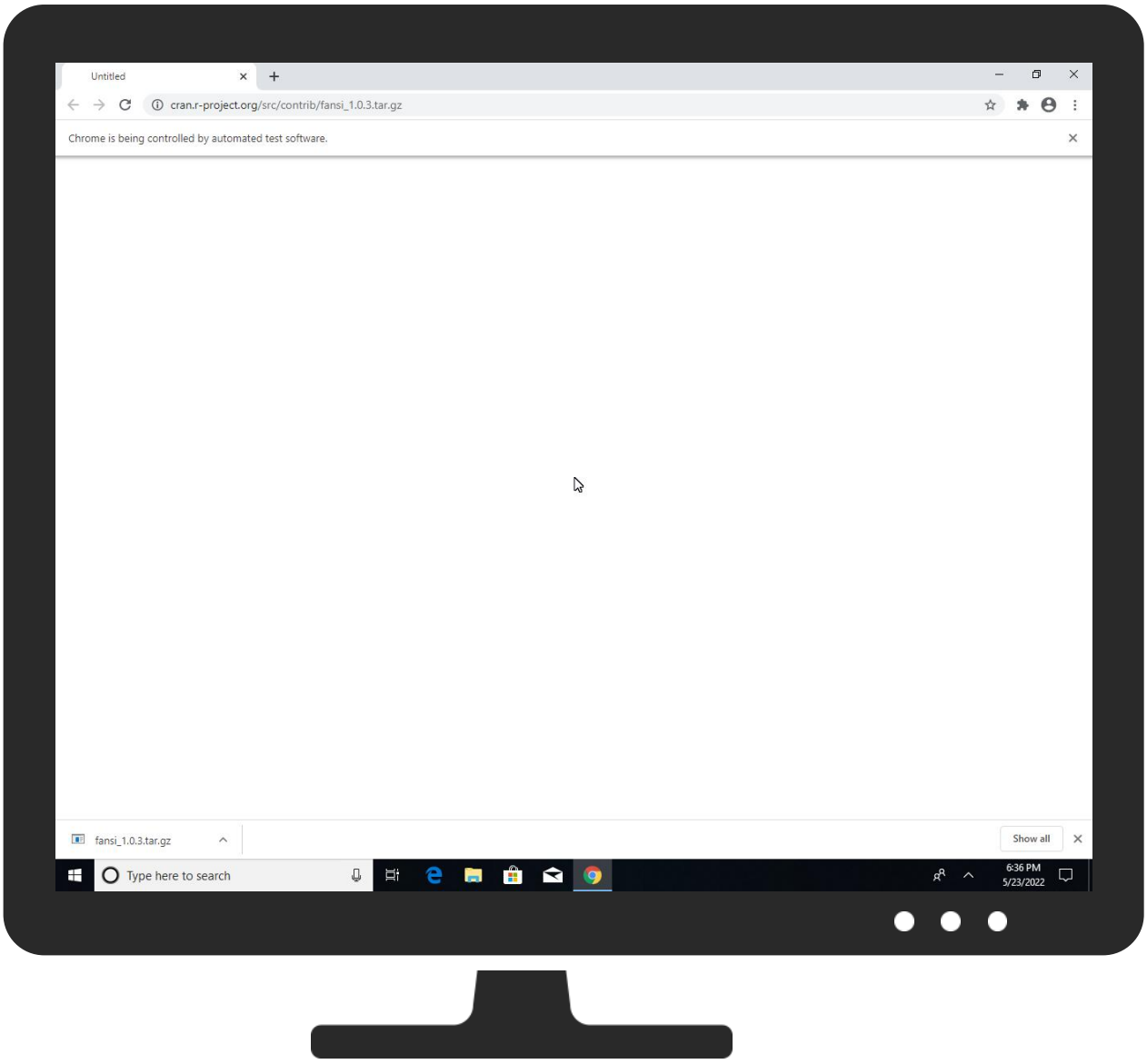


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://cran.r-project.org/src/contrib/fansi_1.0.3.tar.gz	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.184.205	true	false		high
cran.wu-wien.ac.at	137.208.57.37	true	false		unknown
clients.l.google.com	142.250.185.110	true	false		high
cran.r-project.org	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

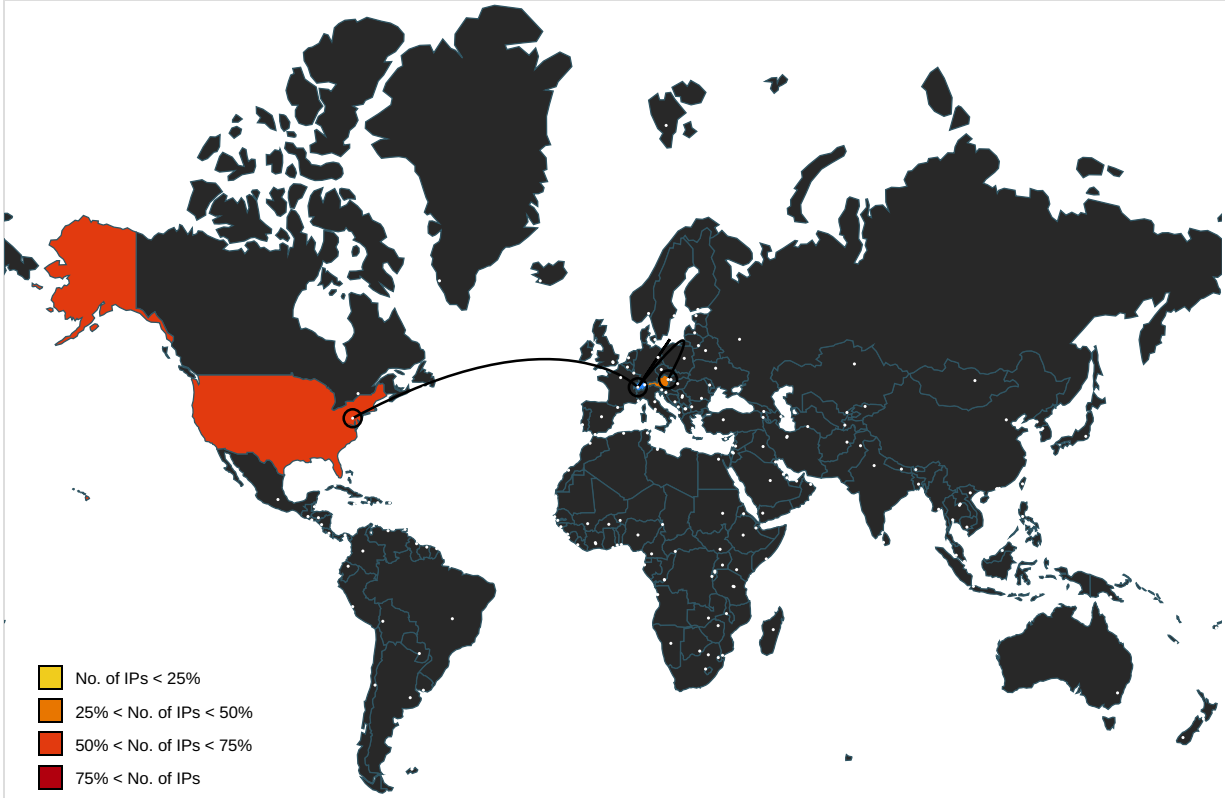
Name	Malicious	Antivirus Detection	Reputation
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://cran.r-project.org/src/contrib/fansi_1.0.3.tar.gz	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	0d2f02c8-0c06-4405-b380-d7f6ea347023.tmp.3.dr, 12053942-9224-461d-9b3e-710dd3138a04.tmp.3.dr, 7b0bada7-4e37-41b9-b758-ce559423173a.tmp.3.dr, 8135de14-17be-421c-bd30-6b80022c300e.tmp.3.dr	false	• URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_background.js.1.dr, craw_window.js.1.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.1.dr	false		high
http://https://ogs.google.com	0d2f02c8-0c06-4405-b380-d7f6ea347023.tmp.3.dr, 12053942-9224-461d-9b3e-710dd3138a04.tmp.3.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.1.dr	false		high
http://https://play.google.com	0d2f02c8-0c06-4405-b380-d7f6ea347023.tmp.3.dr, 12053942-9224-461d-9b3e-710dd3138a04.tmp.3.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	manifest.json.1.dr, craw_window.js.1.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_libcrt_platform_a.1.dr, pnacl_public_x86_64_pnacl_llc_nexe.1.dr	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	manifest.json.1.dr, craw_window.js.1.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.1.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.1.dr	false		high
http://llvm.org/):	pnacl_public_x86_64_pnacl_sz_nexe.1.dr, pnacl_public_x86_64_pnacl_llc_nexe.1.dr	false		high
http://https://www.google.com	0d2f02c8-0c06-4405-b380-d7f6ea347023.tmp.3.dr, 12053942-9224-461d-9b3e-710dd3138a04.tmp.3.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://code.google.com/p/nativeclient/issues/entry%s:	pnacl_public_x86_64_ld_nexe.1.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry	pnacl_public_x86_64_ld_nexe.1.dr	false		high
http://https://accounts.google.com	0d2f02c8-0c06-4405-b380-d7f6ea347023.tmp.3.dr, 12053942-9224-461d-9b3e-710dd3138a04.tmp.3.dr	false		high
http://https://clients2.googleusercontent.com	0d2f02c8-0c06-4405-b380-d7f6ea347023.tmp.3.dr, 12053942-9224-461d-9b3e-710dd3138a04.tmp.3.dr	false		high
http://https://apis.google.com	0d2f02c8-0c06-4405-b380-d7f6ea347023.tmp.3.dr, 12053942-9224-461d-9b3e-710dd3138a04.tmp.3.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.1.dr	false		high
http://https://www.google.com/	manifest.json.1.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_background.js.1.dr, craw_window.js.1.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-clang.git	pnacl_public_x86_64_libcrt_platform_a.1.dr, pnacl_public_x86_64_pnacl_llc_nexe.1.dr	false		high
http://https://clients2.google.com	0d2f02c8-0c06-4405-b380-d7f6ea347023.tmp.3.dr, 12053942-9224-461d-9b3e-710dd3138a04.tmp.3.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json0.1.dr, manifest.json.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
137.208.57.37	cran.wu-wien.ac.at	Austria		1776	WirtschaftsuniversitaetWien AT	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.110	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.184.205	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632519
Start date and time: 23/05/202218:35:21	2022-05-23 18:35:21 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://cran.r-project.org/src/contrib/fansi_1.0.3.tar.gz
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@29/116@3/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 184.30.21.144, 142.250.186.131, 34.104.35.123, 142.250.185.131, 142.250.185.99, 40.125.122.176, 20.54.89.106, 20.223.24.244, 52.242.101.226
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, arc.msn.com, e12564.dspb.akamaiedge.net, edgedl.me.gvt1.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, store-images.s-microsoft.com, update.googleapis.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\05016b1a-1031-4ccc-8833-8ae4572cd0b7.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):	205694
Entropy (8bit):	6.073237294124867
Encrypted:	false
SSDEEP:	6144:vteX5kVfXhSm/TCXnqn3A9IaqfIlUOoSiuRZ:vtUkhxSa+qK3oW
MD5:	3A17FFB46CADA0658A6F999A1DC1FAC6
SHA1:	758E69D2500CCD5457EBE33075B5DA08E673EAFE
SHA-256:	15BC92C94B3781146F2D482C082DA133E55334BB787FB41AC7DD40457C529C8A
SHA-512:	CD059A6D0BAF569CAD637D317D9CBE290156B51A059C1ECC64AC713756118CEC5B98F1EF2220FBEE8F5E7951EE658A774074928966029B221FFA6491D2B41A39
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653323796630281e+12,"network":1.653323798e+12,"ticks":120608476.0,"uncertainty":3921729.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\693b3bcc-88a0-4eb0-82c4-b39e6f54c4d1.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):	205694
Entropy (8bit):	6.073237294124867
Encrypted:	false
SSDEEP:	6144:vteX5kVfXhSm/TCXnqn3A9IaqfIlUOoSiuRZ:vtUkhxSa+qK3oW
MD5:	3A17FFB46CADA0658A6F999A1DC1FAC6
SHA1:	758E69D2500CCD5457EBE33075B5DA08E673EAFE
SHA-256:	15BC92C94B3781146F2D482C082DA133E55334BB787FB41AC7DD40457C529C8A
SHA-512:	CD059A6D0BAF569CAD637D317D9CBE290156B51A059C1ECC64AC713756118CEC5B98F1EF2220FBEE8F5E7951EE658A774074928966029B221FFA6491D2B41A39
Malicious:	false
Reputation:	low

Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653323796630281e+12,"network":1.653323798e+12,"ticks":120608476.0,"uncertainty":3921729.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\79d6731f-c655-473a-b5ea-b58b661f0616.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	197353
Entropy (8bit):	6.045317130343995
Encrypted:	false
SSDEEP:	6144:MeX5kVfXhSm/TCXnqn3A9IaqfIlUOoSiuRZ:MUkhxSa+qK3oW
MD5:	93070C26E5C2164B4E555FE48AA74A1A
SHA1:	79309ED5F7969B7B2083D3FB88A09642B5E3948A
SHA-256:	CEC2D3C206B5CBC49135D4765B202FC92558F8523267D14AAF3377EF15D4CBCE
SHA-512:	51D15CCD86DC89A57F8B6EBE579B3A93AFB70ACD4AAEB6DFE9733663F5FCC5889F33BC62ABC3A7151F824DE82D711180AC418EC2280F54E778ABAB423581DFEF
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653323796630281e+12,"network":1.653323798e+12,"ticks":120608476.0,"uncertainty":3921729.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129218414"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\94b317a5-48d2-48c3-a84b-651e7842e1dd.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	99604
Entropy (8bit):	3.7512594556210432
Encrypted:	false
SSDEEP:	384:6vvSaSs3posLeVNSrnvGO3Ve0JH4j9GCRQrblyOXxYZ2V4IlbrDimfEr4yWelOgz:52ZxSxFNQefEIcBnS2OKcOGxZ
MD5:	44F95C5B48DE8AE6C4C54170938F94D8
SHA1:	8BB934E5B77EBF0599753C8FB0668CDC4628B67C
SHA-256:	EC3D7CF7E48F1645DC883524C2A37FD91E0FEEC84929D185AFBF646194FBC48D
SHA-512:	9F2616E019A10D48126C5065AB245217D962868BD319F391963CE766FA11EB2A9E85FE19DF26FCF5C05F020AB4C56F020469A8ECFC5D48BD22CAAF0350B1061
Malicious:	false
Reputation:	low
Preview:	.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\9d47748c-f74a-411f-b563-7ce51831773c.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):	205694
Entropy (8bit):	6.073236534051064
Encrypted:	false
SSDEEP:	6144:0teX5kVfXhSm/TCXnqn3A9IaqfIlUOoSiuRZ:0tUkhxSa+qK3oW
MD5:	25ACC6AEFF1024ABBCA67EDE2F00B3DB
SHA1:	123E76766F416769B9901F187317FDB2A1793EBE
SHA-256:	E20A91D5EA9B893B3990AE6F550E2762589FABC6715EAED5AF40516FD201B873
SHA-512:	EB5E8621EFC8681E3097233F2F41E4692E4E59201BCECBD19772E41342F12271AD4E7AC847381763B01E8A12D83A43F6797CB82A17B89858F626A38E231FE23E

Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653323796630281e+12,"network":1.653323798e+12,"ticks":120608476.0,"uncertainty":3921729.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129218414"},"plugins":{"metadata":{"adobe-flash-player":{"d

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRLn:+taRLn
MD5:	7AE9008C2AA5ED3E5ED52743E082F5BF
SHA1:	CD90099842F51474494BFC490433578A89C1B539
SHA-256:	94E7D9BF431A0E3F0FD02F0FBA7321F43DD8B523E3D32092AFC474D3FD5ABF62
SHA-512:	596E66D10186ADAD552F4CF7E74CD438AD19AF4C30950D2D6EB80E9F9430CA475D12BB79423EC8D15EAF37ABE0AD1DCCAE459C356A00055A82155C24A35C614
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000001.dbtmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000002.dbtmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Xv:1qIF/
MD5:	206702161F94C5CD39FADD03F4014D98
SHA1:	BD8BFC144FB5326D21BD1531523D9FB50E1B600A
SHA-256:	1005A525006F148C86EFCBFB36C6EAC091B311532448010F70F7DE9A68007167
SHA-512:	0AF09F26941B11991C750D1A2B525C39A8970900E98CBA96FD1B55DBF93FEE79E18B8AAB258F48B4F7BDA40D059629BC7770D84371235CDB1352A4F17F80E14
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000002.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0d2f02c8-0c06-4405-b380-d7f6ea347023.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	1518
Entropy (8bit):	4.811210421839074
Encrypted:	false
SSDEEP:	24:Y26aL3M33ayFGRaXa63aDaaraqavatZa+RdsdsdR/RdsdRdMH6bmQYhbG7n/iy:Y2nzM3qyvK6qDHGXCtwWsQRLsVMH6DYm
MD5:	93D4742B778B57E16F36BFC5AB1D0C37
SHA1:	735350CA83B78C79931EF07E2CF7876A0EBBBE95
SHA-256:	693605B295BCA50FBBE6BFB6209BB5ADEA9D6595376C3D0712E02EDFA8BA8623
SHA-512:	F4560C9B290DCA9928D2E898F31699268CD57195DA7E822A0FBA25C6A5F31BFE2088BC786765BD69D260426AB929B62994C21BCBC15FBEC4FAA57A8DDFEB6E 43
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\12053942-9224-461d-9b3e-710dd3138a04.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1 C
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2905a3be-ef35-4b87-a0c2-01491d160eab.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):	4926
Entropy (8bit):	4.940942805272787
Encrypted:	false
SSDEEP:	48:YcMkKSChkliTqb7qAliqTlYGlQKHoTw0pLArf4MqM8C1Nfct/9BhUJo3KhmeSnpl:nELh+1pIKIg5k0JCKL87bOTlVuHn
MD5:	C058F527641E28C00F4643E17C9D9AEC
SHA1:	5BE29F823B5A4316536A139AC2BECEC740A3D9E7
SHA-256:	4E132A163198297705CA591384844A4C69D2DC78342C8CAB62EED44AFE9AD6E8
SHA-512:	B3F685B90DAEDDA9A488A07BC8A17A79829BF8ADFD0144108576B97AFC0825FADB9235BEC7E08722FFD1E6ED410A2889D92D5D3D1C586A39390DCCFEF6A0A 769
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13297797395101631","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"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":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3ee29310-2853-4b2a-b0d5-b59e7d16dca8.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):	19796
Entropy (8bit):	5.564609551682092
Encrypted:	false
SSDEEP:	384:aDrrdt1LLlwaF/XD0Z1kXqKf/pUZNCgVLH2HfDrtrUtHG+RwTTOcL4r:ULlHoZ1kXqKf/pUZNCgVLH2HflrURGQ5
MD5:	9490CA6AE6BBCA34A988D262E527D849
SHA1:	9303A2EF5CD6E71F33E1076B6D7A3874C1153EC4
SHA-256:	8D1AECD45FEE289EB6D4382D3A9F85A0E26EF8933C5815BBF634BEF7FAB32B47
SHA-512:	F928DB51548544DA197B15C491E9CFC662D86F21EC8ACDD779F2325B75F137CED4AEE6858D71C5EC7595765FB4971E051B3E0A1E2CF6628C05F4D9B2373AA7 1
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":"13297797394227631","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome. google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons": {"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5f7b48c3-2426-4680-9b9a-ca9b71f7e2ff.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):	19795
Entropy (8bit):	5.564671099960879
Encrypted:	false
SSDEEP:	384:aDrrdt1LLlwaF/XD0Z1kXqKf/pUZNCgVLH2HfDrtrUtHG3RwTTOFkL48:ULlHoZ1kXqKf/pUZNCgVLH2HflrURGhY
MD5:	D7CA648C20409A8070263B0EFF5590AF
SHA1:	7A7CD371480A1893228C51ABF30A459EB7D2AA25
SHA-256:	012426EC967134B0E7147DDFD4F8C03F4527C5DB283FDD3BF3334D279C057A63
SHA-512:	1A8DA8832BE0D589323674AEE5F210BB360283036BC43E619EE37E81EF363A118376DC8248A30B63D303DD4BF21EF2C94720325302DD4AC225067DCE9E3F03A
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":"13297797394227631","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome. google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons": {"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7e3c0874-5ff1-4157-b1a3-fa9190674698.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17529
Entropy (8bit):	5.574823789484404
Encrypted:	false
SSDEEP:	384:aDrrdt4LLlwaF/XD0Z1kXqKf/pUZNCgVLH2HfDrtrUjRLTOcL4B:/LlHoZ1kXqKf/pUZNCgVLH2HflrUNtL+
MD5:	D6EC43DB4FA3A47B53D657445E1644AF
SHA1:	92281030894576811FC666387DA837838C95BD5C
SHA-256:	6D9289ED34B43BEAC760CCA53913C936C4754BECECC5A05C6530E3FC2201D064
SHA-512:	06DEA53218A836A500266E985F7E301EFCCB039674A8C42BFE2D1A64AB4AAB91B1188156E654D1429C5737977292ED74926C985B5FA3CD0D43DD87A162D5181
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":"13297797394227631","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\CURRENT (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Xv:1qIF/
MD5:	206702161F94C5CD39FADD03F4014D98
SHA1:	BD8BFC144FB5326D21BD1531523D9FB50E1B600A
SHA-256:	1005A525006F148C86EFCBFB36C6EAC091B311532448010F70F7DE9A68007167
SHA-512:	0AF09F26941B11991C750D1A2B525C39A8970900E98CBA96FD1B55DBF93FEE79E18B8AAB258F48B4F7BDA40D059629BC7770D84371235CDB1352A4F17F80E14
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000002.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985D
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.277658011777669
Encrypted:	false
SSDEEP:	6:AXOWHecK+q2Pwkn23iKKdK25+Xqx8chI+IFUtqVfXOWHeCd0ZmwYVfXOWHehUVkP:AX5+SvYf5KkTXfchI3FUtiX5+CO/IX50
MD5:	B58BD02B01885326A89A092CCFF5E220
SHA1:	2C5262C9AE0A98A388C1EC5054C3281F8F5D6FD8
SHA-256:	38353134E5B8AA7A320E9773B2519A6E47DE6D3F75C3725C691FFF83894DA7EA
SHA-512:	8546BBFF2C5F1B8751F124B9643E56493F035D8ADDAA6D3101834F42112E08468DE4E5A713B513E578A45A960A49F00E4851B03E90C071308F30A05DB64A63D6
Malicious:	false
Reputation:	low
Preview:	2022/05/23-18:36:44.891 8e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/23-18:36:44.893 8e8 Recovering log #3.2022/05/23-18:36:44.894 8e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.277658011777669
Encrypted:	false
SSDEEP:	6:AXOWHecK+q2Pwkn23iKKdK25+Xqx8chI+IFUtqVfXOWHeCd0ZmwYVfXOWHehUVkP:AX5+SvYf5KkTXfchI3FUtiX5+CO/IX50
MD5:	B58BD02B01885326A89A092CCFF5E220
SHA1:	2C5262C9AE0A98A388C1EC5054C3281F8F5D6FD8
SHA-256:	38353134E5B8AA7A320E9773B2519A6E47DE6D3F75C3725C691FFF83894DA7EA
SHA-512:	8546BBFF2C5F1B8751F124B9643E56493F035D8ADDAA6D3101834F42112E08468DE4E5A713B513E578A45A960A49F00E4851B03E90C071308F30A05DB64A63D6
Malicious:	false
Reputation:	low
Preview:	2022/05/23-18:36:44.891 8e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/23-18:36:44.893 8e8 Recovering log #3.2022/05/23-18:36:44.894 8e8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\MANIFEST-000001

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAIxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C23 75B
Malicious:	false
Reputation:	low
Preview:	.|.."....leveldb.BytewiseComparator.....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

Size (bytes):	1518
Entropy (8bit):	4.811210421839074
Encrypted:	false
SSDEEP:	24:Y26aL3M33ayFGRaXa63aDaaraqavatZa+RdsdsdR/RdsdRdMH6bmQYhbG7n/iy:Y2nzM3qyvK6qDHGXCtwWsQRLsVMH6DYm
MD5:	93D4742B778B57E16F36BFC5AB1D0C37
SHA1:	735350CA83B78C79931EF07E2CF7876A0EBBBE95
SHA-256:	693605B295BCA50FBBE6BFB6209BB5ADEA9D6595376C3D0712E02EDFA8BA8623
SHA-512:	F4560C9B290DCA9928D2E898F31699268CD57195DA7E822A0FBA25C6A5F31BFE2088BC786765BD69D260426AB929B62994C21BCBC15FBEC4FAA57A8DDFEB6E 43
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expi

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4926
Entropy (8bit):	4.940942805272787
Encrypted:	false
SSDEEP:	48:YcMkKSChkliTqb7qAliqTlYGlQKHoTw0pLArf4MqM8C1Nfct/9BhUJo3KhmeSnpl:nELh+1pIKIg5k0JCKL87bOTlVuHn
MD5:	C058F527641E28C00F4643E17C9D9AEC
SHA1:	5BE29F823B5A4316536A139AC2BECEC740A3D9E7
SHA-256:	4E132A163198297705CA591384844A4C69D2DC78342C8CAB62EED44AFE9AD6E8
SHA-512:	B3F685B90DAEDDA9A488A07BC8A17A79829BF8ADFD0144108576B97AFC0825FADB9235BEC7E08722FFD1E6ED410A2889D92D5D3D1C586A39390DCCFEF6A0A 769
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13297797395101631","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"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":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\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):	19796
Entropy (8bit):	5.564609551682092
Encrypted:	false
SSDEEP:	384:aDrrdt1LLlwaF/XD0Z1kXqKf/pUZNCgVLH2HfDrtrUtHG+RwTTOcL4r:ULlHoZ1kXqKf/pUZNCgVLH2HflrURGQ5
MD5:	9490CA6AE6BBCA34A988D262E527D849
SHA1:	9303A2EF5CD6E71F33E1076B6D7A3874C1153EC4
SHA-256:	8D1AECD45FEE289EB6D4382D3A9F85A0E26EF8933C5815BBF634BEF7FAB32B47
SHA-512:	F928DB51548544DA197B15C491E9CFC662D86F21EC8ACDD779F2325B75F137CED4AEE6858D71C5EC7595765FB4971E051B3E0A1E2CF6628C05F4D9B2373AA7 1
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":"13297797394227631","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\8135de14-17be-421c-bd30-6b80022c300e.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):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Reputation:	low
Preview:	....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\7b0bada7-4e37-41b9-b758-ce559423173a.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):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Reputation:	low
Preview:	....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d1bb6ed4-0fc9-47ee-9bdb-16955623f9fc.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):	4899
Entropy (8bit):	4.935270175656227

Encrypted:	false
SSDEEP:	48:YcMkKSChkliTiqAliqTlYGlQKHoTw0pLArf4MqM8C1Nfct/9BhUJo3KhmeSnpNGC:nELV+1pIKIg5k0JCKL8bbOTlVuHn
MD5:	107F938607259305450A5C9327358F4C
SHA1:	EFFB4F4DDB0CA7A4470BE85F1841F6EB7C8D7152
SHA-256:	80C55DD43765BD595A310138341E6AA6A75991D0C3DE680F2FB8F1CA8E4EBB7A
SHA-512:	4647B6D996437E46A4996A8E1796B2D8AAE0F788D9FDE34A6D88F22EC60E5EA896724E6F460D5112E4E61749B102E9438F89E0BAFA0D7E0146F8C259FF2AC2AE
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13297797395101631","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"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":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e1601f14-0baf-4c44-b944-fbc3ff095db7.tmp

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

SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ecd3ade0-7446-4742-b7e0-0e74ce79b606.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17703
Entropy (8bit):	5.577224136422392
Encrypted:	false
SSDEEP:	384:aDrrdt1LLlwaF/XD0Z1kXqKf/pUZNCgVLH2HfDrtrU2RwTTOrL4Z:ULlHoZ1kXqKf/pUZNCgVLH2HflrUlwmW
MD5:	5A9C6D919395B15CF8E8345821038A11
SHA1:	CE49691D0542E7AC0BBB002CFED7AF538374FF27
SHA-256:	4C0CF0B914ED32FC4367E63FE9C9A9419DFD47DA3C06F1CD6A10A22B7388B461
SHA-512:	DC051C2464676FFAA3FD1C7ADEA45EA005AF17464A6AD832D7111754631BBFB2252FCB27ECA3D6AE36D3C49196C9B1B8819D12C0A044CEA3EA892E117FB56957
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":"13297797394227631","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	197353
Entropy (8bit):	6.045317130343995
Encrypted:	false
SSDEEP:	6144:MeX5kVfXhSm/TCXnqn3A9IaqfIlUOoSiuRZ:MUkhxSa+qK3oW
MD5:	93070C26E5C2164B4E555FE48AA74A1A
SHA1:	79309ED5F7969B7B2083D3FB88A09642B5E3948A
SHA-256:	CEC2D3C206B5CBC49135D4765B202FC92558F8523267D14AAF3377EF15D4CBCE
SHA-512:	51D15CCD86DC89A57F8B6EBE579B3A93AFB70ACD4AAEB6DFE9733663F5FCC5889F33BC62ABC3A7151F824DE82D711180AC418EC2280F54E778ABAB423581DFEF
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653323796630281e+12,"network":1.653323798e+12,"ticks":120608476.0,"uncertainty":3921729.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129218414"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	102308
Entropy (8bit):	3.751670768380554
Encrypted:	false
SSDEEP:	384:IvvSaSs3pUHsiVPheVNSrnvGO3Ve0JH4j9GCRQrblyOXxYZ2V4IlbrDimfr5r4yl:/y2ZxSx8NQefEIcBnS2OKcOGxH
MD5:	AF119149B31590E7D2B12E033A3B1BC0
SHA1:	1F679848C8C2B03016F7AA4E6EBC26FBCFDBCCAD
SHA-256:	9F926FA9BF1B728A59A71581AC5488A29EAF9AEA6A9ACC59A224FDE587721389
SHA-512:	EE458CA4863A2673042116DDCD4668388545ED22141746EFE63D138F114084E6AAE7F57E11408019CEAD5DFF08EFB0C1DD0E68449B6CCA9A19F0A5B22AC4616
Malicious:	false
Reputation:	low
Preview:	.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\ac6978bf-7026-4c41-bfff-93ee96fca5b3.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):	197259
Entropy (8bit):	6.0450558217431345
Encrypted:	false
SSDEEP:	6144:8eX5kVfXhSm/TCXnqn3A9IaqfIlUOoSiuRZ:8UkhxSa+qK3oW
MD5:	C74612BC0DB65E91A4B88217A40E30DC
SHA1:	9DEB348A4FBECE59817D0256B66D635E68B67690
SHA-256:	E7368DA2187ED725A2D18043CE8774827593328F7B877B8AA590FFAB9839120C
SHA-512:	8BE5AE2A23F23A2FF1154DDE351C2547AF15A08D1E0D2FE6B7C94B4165EF870C7709F1BA9918EF75866EF4DFFBE939977BAB98800CE5BC3375BE68FEEF9A74D5
Malicious:	false
Reputation:	low

Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653323796630281e+12,"network":1.653323798e+12,"ticks":120608476.0,"uncertainty":3921729.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129218414"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\e52ab124-25e8-4e0d-a21f-e0bc333a9e33.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	102308
Entropy (8bit):	3.751670768380554
Encrypted:	false
SSDEEP:	384:IvvSaSs3pUHsiVPheVNSrnvGO3Ve0JH4j9GCRQrblyOXxYZ2V4IlbrDimfr5r4yl:/y2ZxSx8NQefEIcBnS2OKcOGxH
MD5:	AF119149B31590E7D2B12E033A3B1BC0
SHA1:	1F679848C8C2B03016F7AA4E6EBC26FBCFDBCCAD
SHA-256:	9F926FA9BF1B728A59A71581AC5488A29EAF9AEA6A9ACC59A224FDE587721389
SHA-512:	EE458CA4863A2673042116DDCD4668388545ED22141746EFE63D138F114084E6AAE7F57E11408019CEAD5DFF08EFB0C1DD0E68449B6CCA9A19F0A5B22AC461(6
Malicious:	false
Reputation:	low
Preview:	.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\ec4755f6-288a-42cd-8b80-74fcad40c1a7.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):	197259
Entropy (8bit):	6.0450558217431345
Encrypted:	false
SSDEEP:	6144:8eX5kVfXhSm/TCXnqn3A9IaqfIlUOoSiuRZ:8UkhxSa+qK3oW
MD5:	C74612BC0DB65E91A4B88217A40E30DC
SHA1:	9DEB348A4FBECE59817D0256B66D635E68B67690
SHA-256:	E7368DA2187ED725A2D18043CE8774827593328F7B877B8AA590FFAB9839120C
SHA-512:	8BE5AE2A23F23A2FF1154DDE351C2547AF15A08D1E0D2FE6B7C94B4165EF870C7709F1BA9918EF75866EF4DFFBE939977BAB98800CE5BC3375BE68FEEF9A74D5
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653323796630281e+12,"network":1.653323798e+12,"ticks":120608476.0,"uncertainty":3921729.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291206129218414"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\ff8cec4f-784d-4fbc-ab99-ac62643f9375.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	101588
Entropy (8bit):	3.7515366121705824
Encrypted:	false
SSDEEP:	384:2vvSaSs3pUHsiVPheVNSrnvGO3Ve0JH4j9GCRQrblyOXxYZ2V4IlbrDimfEr4yWg:Vy2ZxSxFNQefEIcBnS2OKcOGxX
MD5:	6240B0DBAB4078269DC9B06CE048311B
SHA1:	A113B9B7EF4226F60BFCAA738B3873659810F55B
SHA-256:	9E1E87D4FCFE9B7623CD4FA17967BBCE2661E6E495499DF675BDBC56B75A9255

SHA-512:	465D2211F2E40228D0B6DC364877A0673DDDB27AB69E270A644BE33A4BC3A222469FACD08AE3E0B0FC71A7112C4C29776D6DED7D7DCD7FB2AEB363348F760 81
Malicious:	false
Reputation:	low
Preview:	.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e. 1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0. 0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o. m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f. f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1....D...C. :.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\009bacf4-9b7f-4e02-a72c-e856ae49f4a4.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
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..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\1560_1366170689_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3034
Entropy (8bit):	5.876664552417901
Encrypted:	false
SSDEEP:	48:p/hEc9q0S+UTKYM43z8nqMsfWRUWEADM/W9n7lqFkakzcVTGkcYTPi6zM:RGcg5z/jjjHgUnV278+aWLy4
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA
SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F5 02
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1 sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIs nJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWN sX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfc GxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmd XNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2g iOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271CE
Malicious:	false
Reputation:	low
Preview:	{. "COMMENT": [. "This file serves as a template for the resource info description used by ", . "the NaCl Chrome plugin. It is kept in the NaCl repository to prevent ", . "hard-coding of NaCl-specific information inside the Chrome repository.".], . "abi-version": 1, . "pnacl-arch": "x86-64", . "pnacl-ld-name": "ld.nexe", . "pnacl-llc-name": "pnacl-llc.nexe", . "pnacl-sz-name": "pnacl-sz.nexe", . "pnacl-version": "5dfe030a71ca66e72c5719ef5034c2ed24706c43".}

C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A15840
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.l=....J.$<.....f..... .....NaCl....x86-64.....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C .....p.....`....C....C..B..... .....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2776
Entropy (8bit):	3.5335802354066246
Encrypted:	false
SSDEEP:	48:b/5D5V5ej5ej5PjDdaTS6aTTw6DV1DtFouoyDOsTy:b/hbEEVJB1ZFhLDOsT
MD5:	88C08CD63DE9EA244F70BFC53BBCADF6
SHA1:	8F38A113A66B18BAA02E2C995099CF1145A29DAA
SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....X.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..SP..h..... ..fff.....J.$<[.,$J.l=....J.$<.....f.K.....`.....P.....z.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_crtend_o

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	2.799960074375893
Encrypted:	false
SSDEEP:	12:Bvx/ekjlM/NQQmTfR9yp9396QQmTfR9C6wRqD8MTDDw7lEOkSbfuEAXwX6BX2U8b:bDjO/NbmT3296bmT3Twk8qDwh7b7CD8
MD5:	75E79F5DB777862140B04CC6861C84A7
SHA1:	4DB7BDC80206765461AC68CEC03CE28689BBEE0C
SHA-256:	74E8885B87ED185E6811C23942FD9BD1FBAC9115768849AF95A9DECF6644B2EA

SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC253
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....NaCl....x86-64.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f)...text..comment..bss..group..note.GNU-stack..eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....!..... ...../../../pnacl/support/crtend.c.__EH_FRAME_END__..... .....@.....H.....P.....H.....

C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=7511538a3a6a0b862c772eace49075ed1bbe2377, stripped
Category:	dropped
Size (bytes):	2163864
Entropy (8bit):	6.07050487397106
Encrypted:	false
SSDEEP:	24576:HPHonIwYZJ0ykwVO7Owf31yJKzCtxO8RSV4lY+PbeHVxCtjFV4lBNeSAmfGqa+A7:HvSMRwf3SKmlY+PyPvnM2Gq+
MD5:	0BB967D2E99BE65C05A646BC67734833
SHA1:	220A41A326F85081A74C4BB7C5F4E115D1B4B960
SHA-256:	C6C2D0C2FC3E38A9BFA19C78066439C2F745393F1FD1C49C3C6777F697222C76
SHA-512:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E4896
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>.... .....@.....!.....@.8...@..... .....{.....W..... .....@.....@.....P.td.....h.....h.....4b.....4b.....Q.td.....NaCl....x86-64.....GNU.u.S.:j..,w...u...#w..... ?.....Y@.....@.....1@.....B@.....P@.....@X@.....``@.....h@.....pp@.....H.@.....@.....@.....@.....@.....@...`..@.....@.....A.....A.....p.....@..... .....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@..... ... .@...`...`...`...`.....`...`...`...`...`...`...`...`.....`...

C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	40552
Entropy (8bit):	4.127255967843258
Encrypted:	false
SSDEEP:	768:xlP+1fzyUNVU5LmKxeOnjpD5eA/eUnUUxvT:xlP+1ryYMTekpD5eAWjuvT
MD5:	0CE951B216FCF76F754C9A845700F042
SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A634E
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 624 `.....,...8...Z(..e...e...t...t...y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`.....fmod.fmodf.memcmp. memcpy.memmove.memset.__nacl_read_tp.__pnacl_init_irt.longjmp.setjmp.__Sz_fptosi_f32_i64.__Sz_fptosi_f64_i64.__Sz_fptoui_f32_i32.__Sz_fptoui_f32_i64._ _Sz_fptoui_f64_i32.__Sz_fptoui_f64_i64.__Sz_sitofp_i64_f32.__Sz_sitofp_i64_f64.__Sz_uitofp_i32_f32.__Sz_uitofp_i32_f64.__Sz_uitofp_i64_f32.__Sz_uitofp_i64_f64.nacl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@. A.....D..D1.....8fI.~.M.....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	132784
Entropy (8bit):	3.6998481247844937
Encrypted:	false
SSDEEP:	384:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAIL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F

SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 942 `...;...|.....4...x..#...-...4l..E...M...U...]...n...u...~X...4.....L.....t...p.....`.....''...*...1...:...D...K...T ...\...d...r|..|0.....x.....L.....\...8.....__clzti2.__compilerrt_fmax.__compilerrt_fmaxf.__compilerrt_logb.__compilerrt_logbf.__ctzti2.__divdc3.__divdi3.__div moddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi .__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt _abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__ udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.

C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E 38B
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 94 `.....\_pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t''..A.D..... .....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163f dd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC. NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	3.21751839673526
Encrypted:	false
SSDEEP:	24:MOcpdhWE5O/bZbmT3296bmT3TwQwDnvD/+R3:MHuECdaTS6aTTwXDvD/+l
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62 CFC
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 30 `.....\_pnacl_wrapper_start..// 20 `.dummy_shim_entry.o/./0 0 0 0 644 1840 `..ELF.....>.....@.....@.....PH..,$J.l=....J.$<.....f..D.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native _client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x..... ....C....C..... .....rela.text..comment..bss..group..note.GNU- stack..rela.eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....

C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6ilfHM8KLM2J3jqjnkZ:uqufB

MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD00
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>.... .....@.....@.8...@.....$.....!.....!....'.....G..... .....@.....@.....P.td.....D.....D.....Q.td.....NaCl....x86-64.....GNU.0.m=F>k....&...i..... ..0C.....0C..0C..0E.....0C.....0E.-DT.!.?.-DT.!.....?.....-DT.!...-DT.!.?.....?.....?.....?."...".."...".....@.....`.....`..... ....@...`..... ...@...`..... ...@...`.....`... ...@...`.....`...`.....@...@..... ....1..`3.. 4..`-..`-...:...:...F..@H..`H...H...F...F...G...H.. H. ..F..@G...I.. I..@I..@G...G...I...I...J...G..`I..

C:\Users\user\AppData\Local\Temp\1560_1366170689_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped
Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	12288:gXqUSpBjwQO2o8k+7zjidg4euCAauOILffvCpGy4Wh3BTFmHpq82K2/KsvPyla9d:gafZwcOdNe2auOepCBTFmJq3Kf8ksr
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>.... .....@.....@.8...@.....0.....0.....Y..... .....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl....x86-64.....GNU.K..J.'..b.....<S...`...`... ...@... @.....@.....Y@.....p.....@.....?.....?.....A.....5....?5.5...?.5....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..? .y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... .....`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\1560_1366170689\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Reputation:	low
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\1560_1366170689\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	573
Entropy (8bit):	4.859567579783832
Encrypted:	false
SSDEEP:	12:BLqG6yDJmL4mLDlG9hQ181G46XzrXc+EFfNqpaiOc+T5NqXIOclNqXL:BkylmL4mLDlJ18116XsRNqtZeNqXIZlE

MD5:	1863B86D0863199AFDA179482032945F
SHA1:	36F56692E12F2A1EFCA7736C236A8D776B627A86
SHA-256:	F14E451CE2314D29087B8AD0309A1C8B8E81D847175EF46271E0EB49B4F84DC5
SHA-512:	836556F3D978A89D3FC1F07FCED2732A17E314ED6A021737F087E32A69BFA46FD706EBBDFD3607FF42EDCB75DC463C29B9D9D2F122504F567BB95844F579831
Malicious:	false
Reputation:	low
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "description": "Portable Native Client Translator Multi-CRX",. "name": "PNaCl Translator Multi-CRX",. "manifest_version": 2,. "minimum_chrome_version": "30.0.0.0",. "version": "0.57.44.2492",. "platforms": [. {. "nacl_arch": "x86-32",. "sub_package_path": "_plat form_specific/x86_32/". },. {. "nacl_arch": "x86-64",. "sub_package_path": "_platform_specific/x86_64/". },. {. "nacl_arch": "arm",. "sub_package_pa th": "_platform_specific/arm/". }.].}.

C:\Users\user\AppData\Local\Temp\3689bbbf-4517-4cc8-afbd-a661c56c9959.tmp

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

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\009bacf4-9b7f-4e02-a72c-e856ae49f4a4.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326088
Malicious:	false
Reputation:	low
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C

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

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CI B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488 CB
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\en_GB\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEA D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF5 2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F 7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\hi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA755
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "messa ge": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D0 96E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\hu\messages.json

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

File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\id\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA 12
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\it\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\ja\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498

Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ....."... },.. "app_name": {.. "message": "Chrome ....."... },.. "craw_app_unavailable": {.. "message": "....."... },.. "craw_connect_to_network": {.. "message": "....."... },.. "iap_unavailable": {.. "message": "....."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Chrome ....."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\ko\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome . ..."... },.. "app_name": {.. "message": "Chrome . ..."... },.. "craw_app_unavailable": {.. "message": ".. .. .."... },.. "craw_connect_to_network": {.. "message": "..... ....."... },.. "iap_unavailable": {.. "message": ".. .. .."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Chrome. ....."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\lt\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema"... },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema"... },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima."... },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo."... },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome.."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\lv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQkkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D

SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF0
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\nb\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCB5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app_unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap_unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\nl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXl8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8AA7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\pl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfiIu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOflC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777

Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna."... },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci.."... },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be com pleted."... },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\pt_BR\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw _app_unavailable": {.. "message": "Aplicativo indispon.vel no momento."... },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede."... },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\pt_PT\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTnPlOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F 24
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel."... },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede."... },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\ro\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.61125938671415
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hl3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\ru\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSl3ZGG7OJHZMSl3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjT03On:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F632
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ....-..... Chrome".. },.. "app_name": {.. "message": "..... ....-..... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "..... . .....".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... . Chrome.".. }.. }..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\sk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.640777810668463
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOfTYCUAi0D:1HEl4G8WYpetPmD8ZpcH7aOGAOfzUeD
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59D
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 completed.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\sl\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	4.5101656584816885
Encrypted:	false
SSDEEP:	12:1HEJGcyvmbZGGGcyvmbZ+WYpU34OBOEtf+dgca1ZO8ZpU34GcQArERff03OyZnLh:1HE4cyY4TcyY8WYpNoWa1w8ZpQcQ6AfK
MD5:	3943FA2A647AECEDFD685408B27139EE
SHA1:	0129DD19D28373359530B3B477FE8A9279DABB7D
SHA-256:	18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
SHA-512:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC09D
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\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\sr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	743
Entropy (8bit):	4.913927107235852
Encrypted:	false
SSDEEP:	12:1HEJssbdOGGssbdO+WYpU347xBP+dgcucO8ZpU34s1muP03OyZnLAOfTYzDYD:1HEKsb59sbTWYplx4Xud8Zpy1mNOGAOv
MD5:	D485DF17F085B6A37125694F85646FD0
SHA1:	24D51D8642CDC6EFD5D8D7A4430232D8CDE25108
SHA-256:	7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818
SHA-512:	0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . Chrome ...-.....".. },.. "app_name": {.. "message": "..... . Chrome ...-.....".. },.. "craw_app_unavailable": {.. "message": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": "..... . ...".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... .. . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\sv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	630
Entropy (8bit):	4.52964089437422
Encrypted:	false
SSDEEP:	12:1HEJJMkbGGJMkb+WYpU34OACwz+dgNPGFZO8ZpU34JgpXLSb03OyZnLAOfTYLdlD:1HErMkaqMk6WYpTOcb8ZpDgdZOGAOf8Y
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\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\th\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	945
Entropy (8bit):	4.801079428724355
Encrypted:	false
SSDEEP:	24:1HEKa1dDa1/WYp6UFi72SmlG8ZpyactrW2SAOGAOfvSLD:WK2DNYp6U4y3bpyLxwGFW
MD5:	83E2D1E97791A4B2C5C69926EFB629C9
SHA1:	429600425CB0F196DDD717F940E94DBD8BFF2837
SHA-256:	2FECA577F43D97BAEEA464741D585892103585208FD0A935B810A03BDCE83C88
SHA-512:	60A5928DAA8CB4341487F477C56B5A98B83EDE50E5F4F55A802E01FDDAB86F3E795D391953D3D9214552D14D3F58C5A183693C613720FC12FC387D7B8F9B9AB
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... Chrome ....."... },.. "app_name": {.. "message": "..... Chrome ....."... },.. "craw_app_unavailable": {.. "message": "....."... },.. "craw_connect_to_network": {.. "message": "....."... },.. "iap_unavailable": {.. "message": "..... .....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\tr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	4.710869622361971
Encrypted:	false
SSDEEP:	12:1HEJ9Y8GG9Y8+WYpU34wWT+dgGb0GO8ZpU34wryd7T03OyZnLAOfTYGbPKG:1HE0jWYpyRnG8Zpyr/OGAOfFPn
MD5:	2CEAE0567B6BB1D240BBAD690A98CA3B
SHA1:	5944346FBD4A0797B13223895995CAB58E9ECD23
SHA-256:	A7CB86F30C9C31FE5540282C308BA96ADB4EC16EF98C87129EB88105E5BEF5FC
SHA-512:	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\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\uk\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	720
Entropy (8bit):	4.977397623063544
Encrypted:	false
SSDEEP:	12:1HEJ7wILkSlXZGG7wILkSlXZ+WYpU34zb1Oy2P+dgSV1EjiTO8ZpU347qtfP2CTW:1HElwEkK4uwEkK8WYpd/dTV1e8Zptq5S
MD5:	AB0B56120E6B38C42CC3612BE948EF50
SHA1:	8B3F520E5713D9F116D68E71DAEED1F6E8D74629
SHA-256:	68ABA284751EB9C856032062EF9B1651E2A1E5CE5FDA0977FFC97D63BA7BED9E
SHA-512:	CD852A58217F739C1CD58567FF432D31A7AD3F68C884ABBA1DA95799BCD1545C6A5D3B06F319681C12B78AD0A709828DE4B22736316F148D21F5DB76A5BCCBF
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ...-..... Chrome".. },.. "app_name": {.. "message": "..... ...-..... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\vi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	695
Entropy (8bit):	4.855375139026009
Encrypted:	false
SSDEEP:	12:1HEJMAZrSFZGGMAZrSFZ+WYpU34WFHoz+dgdklzoO8ZpU34NFHoz03OyZnLAOfTU:1HEI4B8WYpAKytFZ8ZpXKMOGAOfd6D
MD5:	7EBB677FEAD8557D3676505225A7249A
SHA1:	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 completed.".. },.. "please_sign_in": {.. "message": "Vui l.ng ..ng nh.p v.o Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\zh_CN\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped

Size (bytes):	595
Entropy (8bit):	5.210259193489374
Encrypted:	false
SSDEEP:	12:1HEJ01GG01+WYpU34zeHz+dgfO8ZpU34YKiO03OyZnLAOfTYB6U:1HEplWYpISv8Zp+JOGAOfa6U
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\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_locales\zh_TW\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	634
Entropy (8bit):	5.386215984611281
Encrypted:	false
SSDEEP:	12:1HEJ2j62GG2j62+WYpU34m7T+dgc8nOO8ZpU34mvIO03OyZnLAOfTYAuH:1HEuSZCWYpsStwP8ZpROGAOfCH
MD5:	5FF50C673CC0C661D615F0CFD0E6DCA0
SHA1:	60DFF98DEAB9C4746B288BDD9C94B3BCAE5EAA85
SHA-256:	C6F8C640F3353A7B9B1432A0C139C1AEEC40133800E6C9B467B63991AD660308
SHA-512:	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\user\AppData\Local\Temp\scoped_dir1560_997754626\CRX_INSTALL_metadata\verified_contents.json

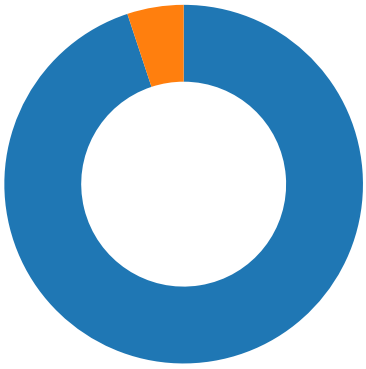
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	7780
Entropy (8bit):	5.791315351651491
Encrypted:	false
SSDEEP:	192:RktDNJ2UzsL5KcASyoH+CouKP/iNGRo/oRHMIT:AZQflcsU
MD5:	0834821960CB5C6E9D477AEF649CB2E4
SHA1:	7D25F027D7CEE9E94E9CBDEE1F9220C8D20A1588
SHA-256:	52A24FA2FB3BCB18D9D8571AE385C4A830FF98CE4C18384D40A84EA7F6BA7F69
SHA-512:	9AEAFC3ECE295678242D81D71804E370900A6D4C6A618C5A81CACD869B84346FEAC92189E01718A7BB5C8226E9BE88B063D2ECE7CB0C84F17BB1AF3C5B1A3 C4
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfbG9jYWxlcy9iZy9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiZHUtdGRPdUNWcmxDY254Q0poRkg2NXpLU05vb1RiUE56bDNHbzdRMGJ3SSJ9LHs icGF0aCI6Il9sb2NhbGVzL2NhL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJ6ZGtWaF9XdkxJWlhkck5xWHBvSHNRMGh1ZGtSM2d1QlMzb2VsTEZLNklVIn0seyJwY XRoIjoiX2xvY2FsZXMvY3MvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6Ik9nUkNIZlVoam9xOU93NHFfaEhvTTQxNzNMelJyYkVpUVdsRXNRSzhscFkifSx7InBhdGg iOiJfbG9jYWxlcy9kYS9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoiN2JVWW1LYkhQUUNRMXBGcmUzTHJySEhwWk9xN1c2Zk5hT0laWmdKUERTTSJ9LHsicGF0aCI6I l9sb2NhbGVzL2RlL21lc3NhZ2VzLmpzb24iLCJyb290X2hhc2giOiJOV3FkU3Rfc1NFMm9KT2VuSUZtM0pMRm9iOGtBZ3ZTa3RtZGpCRGJWazdBIn0seyJwYXRoIjoiX2x vY2FsZXMvZWwvbWVzc2FnZXMuanNvbiIsInJvb3RfaGFzaCI6ImgyaEZ0YUJoLXJQUEtoUm00QkFWM0VEZmhFbnh5MElGOVhYT3Z0aHhlNjAifSx7InBhdGgiOiJfbG9jY Wxlcy9lbi9tZXNzYWdlcy5qc29uIiwicm9vdF9oYXNoIjoid0pSZDFmM3NxMERFVTJHLXd

Static File Info

No static file info

Network Behavior

Network Port Distribution



Total Packets: 59

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:36:37.070306063 CEST	49758	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:37.070347071 CEST	443	49758	142.250.185.110	192.168.2.4
May 23, 2022 18:36:37.070444107 CEST	49758	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:37.070882082 CEST	49759	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.070916891 CEST	443	49759	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.071002960 CEST	49759	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.071899891 CEST	49760	443	192.168.2.4	142.250.184.205
May 23, 2022 18:36:37.071921110 CEST	443	49760	142.250.184.205	192.168.2.4
May 23, 2022 18:36:37.072012901 CEST	49760	443	192.168.2.4	142.250.184.205
May 23, 2022 18:36:37.072280884 CEST	49758	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:37.072308064 CEST	443	49758	142.250.185.110	192.168.2.4
May 23, 2022 18:36:37.072854042 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.072892904 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.072972059 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.073167086 CEST	49759	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.073188066 CEST	443	49759	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.073560953 CEST	49760	443	192.168.2.4	142.250.184.205
May 23, 2022 18:36:37.073577881 CEST	443	49760	142.250.184.205	192.168.2.4
May 23, 2022 18:36:37.073802948 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.073827028 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.128336906 CEST	443	49758	142.250.185.110	192.168.2.4
May 23, 2022 18:36:37.130425930 CEST	443	49760	142.250.184.205	192.168.2.4
May 23, 2022 18:36:37.130654097 CEST	49758	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:37.130691051 CEST	443	49758	142.250.185.110	192.168.2.4
May 23, 2022 18:36:37.131004095 CEST	49760	443	192.168.2.4	142.250.184.205
May 23, 2022 18:36:37.131032944 CEST	443	49760	142.250.184.205	192.168.2.4
May 23, 2022 18:36:37.131252050 CEST	443	49758	142.250.185.110	192.168.2.4
May 23, 2022 18:36:37.131443024 CEST	49758	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:37.132795095 CEST	443	49758	142.250.185.110	192.168.2.4
May 23, 2022 18:36:37.132875919 CEST	49758	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:37.133470058 CEST	443	49760	142.250.184.205	192.168.2.4
May 23, 2022 18:36:37.133573055 CEST	49760	443	192.168.2.4	142.250.184.205
May 23, 2022 18:36:37.139899969 CEST	443	49759	137.208.57.37	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:36:37.143074036 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.149110079 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.149148941 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.149405956 CEST	49759	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.149441004 CEST	443	49759	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.150917053 CEST	443	49759	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.150974035 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.151031971 CEST	49759	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.151065111 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.510420084 CEST	49760	443	192.168.2.4	142.250.184.205
May 23, 2022 18:36:37.510662079 CEST	443	49760	142.250.184.205	192.168.2.4
May 23, 2022 18:36:37.511131048 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.511271954 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.511953115 CEST	49759	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.512223959 CEST	443	49759	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.512358904 CEST	49760	443	192.168.2.4	142.250.184.205
May 23, 2022 18:36:37.512388945 CEST	443	49760	142.250.184.205	192.168.2.4
May 23, 2022 18:36:37.515450954 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.515471935 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.533550978 CEST	49758	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:37.533725977 CEST	443	49758	142.250.185.110	192.168.2.4
May 23, 2022 18:36:37.537933111 CEST	49758	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:37.537955999 CEST	443	49758	142.250.185.110	192.168.2.4
May 23, 2022 18:36:37.557985067 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.558011055 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.558130026 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.558171034 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.558221102 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.558231115 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.558247089 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.558274984 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.558290958 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.558325052 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.558343887 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.558355093 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.561444998 CEST	443	49760	142.250.184.205	192.168.2.4
May 23, 2022 18:36:37.561552048 CEST	49760	443	192.168.2.4	142.250.184.205
May 23, 2022 18:36:37.561577082 CEST	443	49760	142.250.184.205	192.168.2.4
May 23, 2022 18:36:37.561594963 CEST	443	49760	142.250.184.205	192.168.2.4
May 23, 2022 18:36:37.561662912 CEST	49760	443	192.168.2.4	142.250.184.205
May 23, 2022 18:36:37.569341898 CEST	443	49758	142.250.185.110	192.168.2.4
May 23, 2022 18:36:37.569441080 CEST	443	49758	142.250.185.110	192.168.2.4
May 23, 2022 18:36:37.569535017 CEST	49758	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:37.569555998 CEST	49758	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:37.579097986 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.579145908 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.579200029 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.579428911 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.579477072 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.579500914 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.579809904 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.579855919 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.579870939 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.579899073 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.579914093 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.579946995 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.579974890 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.579989910 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.580147028 CEST	443	49761	137.208.57.37	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:36:37.580172062 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.580275059 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.580302000 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.580321074 CEST	49761	443	192.168.2.4	137.208.57.37
May 23, 2022 18:36:37.600085020 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.600132942 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.600246906 CEST	443	49761	137.208.57.37	192.168.2.4
May 23, 2022 18:36:37.600285053 CEST	49761	443	192.168.2.4	137.208.57.37

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:36:36.923665047 CEST	56076	53	192.168.2.4	8.8.8.8
May 23, 2022 18:36:36.926424026 CEST	60758	53	192.168.2.4	8.8.8.8
May 23, 2022 18:36:36.943068981 CEST	53	56076	8.8.8.8	192.168.2.4
May 23, 2022 18:36:36.945729017 CEST	53	60758	8.8.8.8	192.168.2.4
May 23, 2022 18:36:37.037158012 CEST	60647	53	192.168.2.4	8.8.8.8
May 23, 2022 18:36:37.056699038 CEST	53	60647	8.8.8.8	192.168.2.4
May 23, 2022 18:36:41.917514086 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:41.943592072 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:41.945625067 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:41.972651005 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:41.972700119 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:41.972724915 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:41.972749949 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.029751062 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:42.039904118 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.039938927 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.039959908 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.039980888 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.040369034 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:42.040592909 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:42.107794046 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:42.448319912 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:42.449230909 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:42.482105970 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.492731094 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.492773056 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.492791891 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.536372900 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.645061016 CEST	443	58173	142.250.185.110	192.168.2.4
May 23, 2022 18:36:42.686836958 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:42.687257051 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:42.687366009 CEST	58173	443	192.168.2.4	142.250.185.110
May 23, 2022 18:36:42.810112953 CEST	58173	443	192.168.2.4	142.250.185.110

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 18:36:36.923665047 CEST	192.168.2.4	8.8.8.8	0x67f9	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
May 23, 2022 18:36:36.926424026 CEST	192.168.2.4	8.8.8.8	0x2a87	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
May 23, 2022 18:36:37.037158012 CEST	192.168.2.4	8.8.8.8	0xc8dd	Standard query (0)	cran.r-project.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 18:36:36.943068981 CEST	8.8.8.8	192.168.2.4	0x67f9	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 18:36:36.943068981 CEST	8.8.8.8	192.168.2.4	0x67f9	No error (0)	clients.l.google.com		142.250.185.110	A (IP address)	IN (0x0001)
May 23, 2022 18:36:36.945729017 CEST	8.8.8.8	192.168.2.4	0x2a87	No error (0)	accounts.google.com		142.250.184.205	A (IP address)	IN (0x0001)
May 23, 2022 18:36:37.056699038 CEST	8.8.8.8	192.168.2.4	0xc8dd	No error (0)	cran.r-project.org	cran.wu-wien.ac.at		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 18:36:37.056699038 CEST	8.8.8.8	192.168.2.4	0xc8dd	No error (0)	cran.wu-wien.ac.at		137.208.57.37	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- accounts.google.com
- cran.r-project.org
- clients2.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49760	142.250.184.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:36:37 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-05-23 16:36:37 UTC	0	OUT	Data Raw: 20 Data Ascii:
2022-05-23 16:36:37 UTC	34	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 23 May 2022 16:36:37 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: script-src 'report-sample' 'nonce-6oL3_yw6ubhn0Pe7gl03aQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-6oL3_yw6ubhn0Pe7gl03aQ' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-23 16:36:37 UTC	35	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:36:37 UTC	35	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49761	137.208.57.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:36:37 UTC	0	OUT	GET /src/contrib/fansi_1.0.3.tar.gz HTTP/1.1 Host: cran.r-project.org Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-05-23 16:36:37 UTC	1	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 16:36:37 GMT Server: Apache Last-Modified: Thu, 24 Mar 2022 07:50:06 GMT ETag: "7578b-5daf21833c878" Accept-Ranges: bytes Content-Length: 481163 Connection: close Content-Type: application/x-gzip
2022-05-23 16:36:37 UTC	2	IN	Data Raw: 1f 8b 08 00 aa 22 3c 62 00 03 ec 5b d9 8e 1b c7 7a f6 75 3f 45 99 86 8f 48 83 6c 0e 39 8b 16 58 51 c6 b3 c8 72 24 59 e0 8c a2 73 30 63 cc 34 bb 8b 64 69 7a 61 aa ba 87 a2 04 03 7e 81 20 38 97 01 12 38 e7 e6 24 b9 ca 45 ae 73 13 bf 89 9f c0 8f 90 ef ff ab 7a e1 0c 47 d6 89 2d 1b 41 4c d8 22 bb ba 96 7f df ea 9f 49 90 1a d5 ff e0 bd 7e 36 f0 b9 bd bd 4d df 83 db 3b 43 7e 1e 6c 6d f1 b7 fb 7c 30 d8 1a 0e 6e 6f 0c 07 c3 6d bc 1f 0c 36 b7 76 3e 10 db ef 17 2c fb 29 4c 1e 68 21 3e 88 d5 74 2a cd db e6 49 fd 96 d7 ff 57 3f 13 e6 ff d3 dd 27 07 47 cf 76 f7 0e de cb 19 c4 e0 1d cb ef 75 fc 1f 42 3a 98 ff 9b 3b c3 9d 8d ed 1d f0 7f b8 7d 7b fb 03 b1 f1 5e a0 b9 f2 f9 7f ce ff 8f c4 43 99 4a 1d e4 32 12 e3 a5 d0 d9 ab e5 54 a6 c3 7b 22 ca 44 9a e5 42 46 2a a7 17 b3 Data Ascii: "<b[zu?EHl9XQr$Ys0c4diza~ 88$EszG-AL"I~6M;C~Im|0nom6v>,)Lh!>t*IW?'GvuB:;}{^CJ2T{"DBF*
2022-05-23 16:36:37 UTC	18	IN	Data Raw: 50 6b a0 40 a3 34 dd 32 7e b6 80 e8 43 12 5b ec 30 a7 cf 88 18 76 89 aa 21 8b b0 45 cb 13 e1 11 77 ce 6a 19 e5 a4 87 50 5c 77 78 08 a2 bb 15 21 e4 f8 57 13 9f 79 cd 75 b6 e6 aa 38 df af 1d be a1 96 8e e2 02 44 72 10 12 9b 0b db 68 56 83 5e 8b 12 45 6a 44 15 48 ae 13 3f f2 36 17 7d 19 27 2f f2 8a 77 01 5f 30 67 98 b4 82 b9 0d 93 97 32 6d 59 e3 cb 83 b7 12 0b 09 96 0b c3 da da d0 b4 8c 01 b2 46 94 38 10 5b d1 d6 39 a0 d1 cb 70 21 8c e1 57 55 5f 41 56 48 bc 84 46 44 62 28 38 8f b0 0e 41 54 18 21 a0 9b 14 45 d7 69 b0 c4 4a e1 a3 05 cb 38 e8 8f 72 e1 2b 78 46 bd 78 c4 58 a1 03 ab e2 3c 2a 67 71 63 8a 9e 17 1d f6 29 6b b0 6c 02 5b 57 21 0c 10 d8 1f c3 63 1d e2 69 44 3c 6d ef 8d 9f 99 0f f0 06 b8 c2 30 3e 09 b8 1f 3f 56 69 30 6a e9 3c 84 71 63 8a 3c 45 ad 00 43 Data Ascii: Pk@42~C[0v!EwjP\wx!Wyu8DrhV^EjDH?6}'/w_0g2mYF8[9p!WU_AVHFDb(8AT!EiJ8r+xFxX<*gqc)kl[W!ciD<m0>?Vi0j<qc<EC
2022-05-23 16:36:37 UTC	37	IN	Data Raw: d1 44 43 99 c1 74 02 79 4d 79 70 59 51 3b 9b e0 56 1c 82 09 1b be a1 b4 5c 9e 23 89 3a 99 00 26 25 4b 8e b4 b2 71 dd 9a 27 c7 e2 49 96 19 7c 50 6f 1d 8d 39 a3 cc ce bf 4c 5d 94 69 92 4c 2c 85 26 fb 23 e1 10 4c 80 92 2c a9 a2 ee 7a 5a 94 05 2a 5f 14 f0 ec b2 0b a8 36 ee 64 9e 33 8d a2 05 a9 27 d8 51 14 45 58 05 9e 9b d1 ea 30 92 8d 9a 1a d2 a0 25 50 c0 11 fd 15 4f 30 b5 02 a9 92 9a 19 80 1e 68 d5 9a 06 a7 0d cc 28 0d 84 7d 13 55 f5 52 00 15 fd 51 a6 ad 01 85 08 1c 49 d0 f2 60 09 d1 23 98 44 2d 1d 96 ec 1a 8d bd 93 bb c1 c4 c3 38 fe fb 7f 5c cc ed 9f f4 63 c9 7f 85 10 74 2f 7b 00 76 2e ff b3 b3 72 f2 73 e2 ed ff fc 54 fd 9f c6 f9 d9 cb f1 3f 5a 43 f2 08 50 49 66 85 a8 df c9 67 9e 3d cc 03 e4 b7 59 87 82 d2 b6 55 1d 08 63 5b 45 7a a6 bb 93 7e 9a 6a 9b 93 61 Data Ascii: DCtyMypYQ;V\#:&%Kq'I|Po9L]iL,&#L,zZ*_6d3'QEX0%PO0h(}URQI`#D-8\ct/{v.rsT?ZCPIfg=YUc[Ez~ja
2022-05-23 16:36:37 UTC	53	IN	Data Raw: 71 f1 35 ce 7f 3d fe f3 57 f1 bf 9e 28 3b f1 ff 52 e8 37 fa f3 cf e3 ff 45 45 c5 84 ff 8d ff fe df f8 fc 75 fd ff 8f 42 bf d1 9f 3f 8f ff 16 11 13 12 15 fa b1 fe 05 f9 85 84 44 fe 8d ff fe df f8 ec 8b ff 6e 22 f4 3f de 16 c0 fa 0a cb 87 e1 88 27 c3 d5 a9 5e b9 2c 39 a4 78 1a 31 81 f2 91 23 07 71 92 8e 84 1b 28 09 56 28 3a 3d 7a ac 81 3b e7 90 eb f7 72 54 91 dc 62 19 3f 32 7d cb e2 d1 19 c6 e1 8a 23 92 e5 93 e2 d5 2c ed 81 31 d9 83 31 4b 57 c4 fc 1e 0d 79 7a 89 f9 2e 78 3f 1a 3a 98 f0 79 58 bc b7 79 aa e9 e6 18 9f 71 67 51 65 e9 7c 06 b1 90 ed e6 38 99 a3 91 50 5f 9f 7e 5f 5f df d8 e6 97 1d cf f5 61 2f d5 38 61 76 57 da 87 3b a4 6a bd ad dd 3c 47 be 9c 24 51 4d cd 59 12 1f 39 2f 2f a0 a1 3f b0 32 20 5d 32 97 9e a2 27 93 98 a2 4a 7f 26 ef 45 b3 90 97 71 a4 Data Ascii: q5=W(;R7EEuB?Dn"?'^,9x1#q(V(:=z;rTb?2}#,11KWyz.x?:yXyqgQe|8P_~__a/8avW;j<G$QMY9//?2]2'J&Eq
2022-05-23 16:36:37 UTC	69	IN	Data Raw: 4f 37 e5 9c e4 cb aa 4c 39 1d 2f 6e 22 3f bb 5c e4 a4 5e 61 c0 cd a1 8c 20 eb ca 53 58 3e 52 c7 31 f1 f8 ea 30 04 7e c0 d1 a7 67 2b a7 40 19 19 9f 4b d5 a9 fe aa 82 6d 89 90 d8 ec c6 d3 a5 31 12 8b 71 85 6a d1 e6 eb 53 ce 7a 31 15 fc 11 83 ba 2a 62 a7 58 2d e3 2e 4b 9b 89 87 06 a8 31 56 af dc 3e 4a 4f 96 54 27 ae 73 7c 31 ec a0 b8 e2 57 d5 b7 a6 f6 07 83 98 92 99 24 0b 28 a6 3e 5c 2c c6 73 d0 62 55 13 43 96 2d cd 94 31 70 4c 2e 9b 25 1a b3 24 1e f3 69 5a eb 20 fd 38 bc 58 7f 58 e9 f3 7b 7f 8a 4d 62 44 01 e7 09 52 f7 f1 60 dc d3 38 72 31 2c 90 a0 bc 20 ec 94 e9 cf b9 12 cb 28 4e ba c5 9b af cd d7 4e de c4 5b c1 07 2e ea a3 3e f1 38 e3 4b 96 61 ad 74 5b 79 f7 64 97 3e 63 ed 08 5f ec 7c 50 42 74 0b b0 41 86 4c 77 d6 2f ea 1b 9d f8 c0 bd 03 a5 48 1f 94 24 8b Data Ascii: O7L9/n"?\^a SX>R10~g+@Km1qjSz1*bX-.K1V>JOT's|1W$(>\,sbUC-1pL.%$iZ 8XX{MbDR`8r1, (NN[.>8K at[yd>c_|PBtALw/H$

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:36:37 UTC	85	IN	Data Raw: 0c 68 48 fe 4c 6d e9 4c 73 25 d0 98 00 c5 04 74 fc 27 94 e9 88 4b 20 56 5d 08 06 0b e0 f0 e7 8e 0e 68 e4 3f f4 75 4c 10 1b 38 2f 60 6f 3a a2 0f 5f 83 30 9a 02 a2 01 d0 cc cd cc d4 c1 c4 ef bb cb 77 a1 7e 42 fe 7e 5c a8 03 02 8c ae 01 53 c1 cd 36 48 14 b8 69 05 8d b1 ef 97 a6 f6 88 70 83 ab 9f 2e 98 8d ac 1c 60 10 3c d4 0b a6 a3 a4 cb fe 33 35 6e 08 db de 7a f0 3e 23 8b 17 1c 0e f8 7e 86 e5 05 08 b0 71 10 fd 8a 21 04 0c 6a 0b 92 ff c7 c4 00 d6 c0 1d 88 7b c7 9d 63 ce 7b 44 b8 82 0b c3 df 7f 52 04 7c bb fb 83 3b e0 2d 12 e5 0b fe 5e c0 1f 18 c1 04 44 d8 23 3d ad d9 19 cd cc d0 7b 36 19 b9 ff 20 bf 7d 05 f0 76 43 ec fe ee 05 e6 64 35 22 c8 1f a0 77 a3 26 dc 01 1b 80 1d 13 8c fe 47 08 0e 08 0f 08 03 1e b7 2b c4 2d cc 0d ee f8 04 45 8e de e8 0a b1 47 80 c1 1e Data Ascii: hHLmLs%t'K V]h?uL8/`o:_0w~B~\S6Hip.`<35nz>#~q!j{c{DR|;-^D#={6 }vCd5"w&G+-EG
2022-05-23 16:36:37 UTC	101	IN	Data Raw: 73 0c 6b 14 2e 5d 6c ab 78 90 f5 70 c2 a8 37 5a e3 5b 7e 3f 5d 2f 95 db f5 45 4f e2 07 0f 8b de a7 6e dd e7 53 59 7d 71 86 58 e7 43 91 6b b4 01 a8 ba ea 2d fb 6c bb 8c d9 29 19 ca 6b ef 5f 3f 4a 23 7f 57 ba 94 94 c3 37 96 80 2a 6a 7b 7d db e5 ba cd f2 e9 b1 38 d3 4e ac 47 4f 94 ef 4e e8 54 98 79 eb 98 a8 26 2c 76 3f 11 a6 34 5e 22 0d fc 20 c0 eb 6d f7 f9 6b 04 a1 21 fe bd 17 7e a3 48 e2 5d 5c 2a 8f 43 f2 2f d0 2e 99 04 5d 80 7a f4 70 18 ac 89 17 a1 3b 87 c7 59 c5 91 84 50 3a 1a 7b fb 42 3b 3f 4f 11 9b c5 11 9b c4 c5 fb 4b fa 1c e7 f2 3e 6b db 73 6b fd ed 5d 57 02 c5 c6 85 59 95 06 29 f6 f4 0c 54 6b 61 8f f0 9d 4f 27 ac 1f a3 9d f4 b1 39 e9 53 f5 75 cd f1 86 f7 a8 5a 04 79 75 d1 fc 9a d4 8d ad 0b 11 21 19 f1 41 9d 8a 16 23 72 2c 1f 08 e9 ea 8c 06 4f 6d 7b Data Ascii: sk.]lxp7Z[~?]/EOnSY}qXCk-l)k_?J#W7*j{}8NGONTy&,v?4^" mk!~H]*C/.]zp;YP:{B;?OK>ksk]WY)Tka O'9SuZyu!A#r,Om{
2022-05-23 16:36:37 UTC	117	IN	Data Raw: 28 d9 4c 24 cb 6b 64 f4 d7 c9 2d f5 8f 3b 8f 35 c8 b4 8a 66 31 ea 0a a4 74 6b e5 26 0a 37 6f 8f a8 17 9f b9 72 12 23 72 1a 79 04 15 f5 fd 70 68 c4 8d 1c a1 86 cb c8 a1 20 2f cc 6c af 40 63 bc 6b 64 c7 52 8d de 6d 7e 56 bd bc a1 45 fa 99 2d 2f 42 6f 47 48 c1 43 00 fa f8 66 06 9a 33 23 d7 d3 c2 84 2f 89 11 3d 8c 94 04 35 57 d3 ca 38 57 85 7c bc 4e 4a 28 5c 78 12 4a 51 38 90 8d 63 23 14 19 94 27 42 58 82 49 a8 43 70 93 d9 5e a5 e4 4e 98 1e e3 7d 97 49 d5 51 c8 17 81 73 0f 2f e5 0d e9 f6 aa e0 a8 f3 2a 5d 3d 8d c1 44 3a bd 86 7b fd b4 28 85 a6 28 5e 98 09 f8 8b e6 92 ac e6 d3 17 f8 9a e8 a7 c8 da 6f 2f b4 ce f4 3e dc 4c d1 f9 8a 5a f9 cd ae 4e 99 87 26 88 be eb f2 24 1e 0f 4d 84 c2 00 2a ad 21 45 a2 52 f9 dd f3 d7 ca 48 68 f5 cf 9d 3d e1 60 a4 91 11 d5 cb 44 Data Ascii: (L$kd-;5f1tk&7or#ryph /l@ckdRm~VE-/BoGHCf3#/=5W8W\|NJ(\xJQ8c#'BXICp^N}!Qs/*]=D:{((^o/>LZN &$M*!ERHh=`D
2022-05-23 16:36:37 UTC	133	IN	Data Raw: 5a 2a ed 76 56 93 02 99 4c 0f 6c fd 6c cd ca d7 95 ad a4 b3 53 10 d3 d5 76 1a 43 93 de 16 de dd e9 55 38 43 de 0a d7 1e 95 57 cb 5f 57 cf 2f 3c 0d ad af 55 5e d3 4a f0 7d eb 81 fc 44 a4 e7 3f 36 c9 20 f2 99 77 23 f4 9e c4 c5 71 6a 17 fe 45 d5 6f f7 12 be a8 ad 5c c8 79 9e 22 bb 22 41 f9 c7 9c 4a ab c8 43 37 75 8d 88 69 ac 29 29 11 0a e7 f9 de f8 60 d9 18 b8 6f dd 32 d3 f7 cd af ce 12 e5 dd bd 5f 2e 1f be ef f2 25 69 73 2e b4 79 e8 a5 83 9c 6b 94 12 8c ee a6 7d b7 88 49 88 96 5e c4 13 95 a7 61 d2 a1 ff d8 ba 9e 1e 51 23 e4 eb 36 4d 2e 3c 1e 69 19 96 aa 5f 41 9d 31 2c f3 f7 74 72 c1 b4 dc 15 45 be 2b f0 6d a1 e8 ff 41 85 df 73 50 ad 4d da f0 c3 4b fb ab f4 9e 37 3f f4 fb a8 98 b6 b7 f3 b1 ab 24 a5 53 f1 11 9f d9 32 56 b6 0e 1b c7 e7 63 bf 7a b1 86 ab bb 7c Data Ascii: Z*vVLllSvCU8CW_W/<U^J}D?6 w#qjEo\y""AJC7ui))`o2_.%is.yk}I^aQ#6M.<i_A1,trE+mAsPMK7?$S2Vcz|
2022-05-23 16:36:37 UTC	149	IN	Data Raw: a8 1a cb 06 e7 92 8b d2 55 20 6a 9e 8b 45 4c e7 c8 09 ac 43 ef 20 f1 2b 3a bb 16 6c 14 60 c6 c2 55 1f c3 95 a5 71 0c fa 42 59 6c e8 26 b4 37 41 e0 a3 6e 0e 13 ed 34 ab 04 52 28 40 a3 41 20 8d 32 33 20 cb 81 d2 b8 27 48 86 ae 7b 47 44 c3 ef 3c 16 45 d1 4d f4 8e de b3 81 56 f2 ae b6 41 28 c3 49 78 17 e5 0f 59 4d 4d 2c 01 cb f1 2d aa ad eb a0 b8 c8 d3 f4 8b a1 b2 3b 8a a5 24 83 63 24 3f 83 86 87 8d de 2e f7 89 07 2f ea 53 91 c1 8c 24 27 50 82 a4 07 0b b3 ca b7 13 05 d9 f6 d9 d9 43 90 c3 0e 80 70 00 52 7c cb b8 cc 22 50 32 ec 06 21 e5 0d 32 31 03 66 31 c0 8b 59 a4 ec d8 28 67 76 2f c0 7a e2 70 b3 df 44 5f b9 b9 78 10 d8 6a b4 51 79 44 9d dc 9b 48 6b 6a d0 e3 e9 30 14 0d e8 b6 72 f8 13 8e ac 02 a2 ad da 38 19 ce 8c 77 cf 96 04 18 05 5b 22 21 e9 45 56 88 da a3 Data Ascii: U jELC +:l`UqBYl&7An4R(@A 23 'H{GD<EMVA(IxYMM,-;c?./S$'PCpR|"P2!21f1Y(gv/zpD_xjQyDHkj0 r8w["!EV
2022-05-23 16:36:37 UTC	165	IN	Data Raw: 65 3d e3 71 ef 56 54 f8 7b f8 9c 29 7b a4 b1 ad 77 fc f0 6b 4a d3 f4 b5 99 78 fb 41 51 47 39 e6 7b 92 a5 31 c8 03 22 93 5a c3 a4 0a 53 d5 93 c3 94 87 69 d3 d4 4f 9c ab 90 bc c5 07 b5 7d 2a f1 4b a2 ff e9 fd 5c fb e9 46 6e c5 5d 08 b9 a0 71 5a 52 98 13 29 73 16 dd 54 49 5b 89 37 d5 54 bb 8f d2 12 75 64 e2 b4 95 a5 2c ef 65 3b 20 35 58 21 7a 34 ed 14 9b 23 a2 84 4c 51 b9 30 78 e4 6d 31 6e f4 e9 7e cd f5 29 74 1d 7d c6 c5 f0 5c f2 5a 3f cf af 4b 70 53 7a 29 be 6a 8a b7 b0 e3 9b 87 99 51 c5 90 1b 78 95 11 13 9b d0 e2 fd 89 13 6b ad 94 da 48 f1 d4 6f cd ad 19 70 e2 52 24 1f 86 ae 86 54 22 d3 dd 8d 2f 24 8b 36 86 d9 0c bb 8c 25 c7 58 c9 4a c8 a7 eb 74 52 a6 14 4c 4c 78 a6 76 d3 fc 91 e9 13 46 00 06 f3 7c 21 a1 d9 45 cf 29 32 f0 9e b6 5c 29 97 48 b5 04 be 3c 84 Data Ascii: e=qVT{}{wkJxAQG9{1"ZSiO}*K\Fn]qZR)sTI[7Tud,e; 5X!z4#LQ0xm1n~)t}\Z?KpSz)jQxkHopR$T"/$6%XJ tRLLxvF|!E)2\)H<
2022-05-23 16:36:37 UTC	181	IN	Data Raw: ab 1f b4 30 87 8a cf b6 f4 42 e6 f2 ee 62 bb 77 90 d9 e0 46 3f 6c e8 9e b0 b8 06 c0 23 86 42 89 d8 10 e7 ee 83 4c 7d 6f 99 9c 1b 0e e5 08 f2 a1 0c fb e4 ec 50 4d 1e 7d 01 ad ec a6 ac 50 69 41 75 dc 69 a2 c7 5c c9 89 6b e9 0d 62 69 52 c5 39 61 97 65 35 90 ba 4f 05 b0 8f 23 f4 22 88 1e 35 5e 14 88 e0 4a 52 41 70 74 38 8b aa 82 fd c2 6f ca 38 8e ff 7a 61 8a a9 d8 77 3c c3 57 01 9e 87 17 3b 0a d2 e0 b7 2c b9 7d b7 dc 69 85 de 20 7f 11 c2 ab d6 f9 96 48 02 a6 b9 00 91 24 df 07 5d a8 5e ca 3f 0d ba 7f 5d 07 5d b4 f8 ed 9b ef 6c a7 05 90 77 bd 5b 61 3d d6 88 d9 d0 a1 23 63 c9 64 38 b2 39 71 b5 d6 37 a1 8f 6e a7 bb e4 d1 e1 3f dc fb 6b af 83 48 9c 32 1e 96 2d 60 bf ff 54 16 15 d4 d8 3d 21 6b 5c 3b a8 6e 77 f4 7d 35 c8 50 17 17 e0 ce e6 c5 35 f3 81 9e 1c 17 7a 86 Data Ascii: 0BbwF?l#BL}oPM}PiAui\kbiR9ae5O#"5^JRApt8o8zaw<W;,}i H$]^?]]lw[a=#cd89q7n?kH2-`T=!k\;nw}5P5z
2022-05-23 16:36:37 UTC	197	IN	Data Raw: 6a fd 5c e8 19 58 7f f9 0c cf b4 03 c6 ba 91 df c3 22 01 00 60 78 d2 79 4f 65 a0 5d 8a a1 2f 3e 83 dd 00 c1 17 93 f7 22 83 e9 89 ee 7d 98 ff 2f 2b 46 a7 5b 21 3a b7 0a 12 d4 9f 8b fe a9 32 e8 f8 60 62 6a cf dd f1 96 08 81 56 1c f4 79 75 07 12 b4 49 fe 1d 5d 4b 3f d0 f4 47 c2 d5 8f 8f f1 77 bb 1c 2d 5e 3e 9f 2f f8 69 eb cf 9f ac 68 2c 43 80 8e 23 f8 76 5c 61 b0 c9 f6 5e c8 cb fd 11 11 97 46 eb 3d 91 89 bc a9 d6 54 4a 03 25 af 78 97 50 f2 b9 bc 23 29 28 03 c5 06 05 e6 b4 e5 0d 58 d8 5c ad 4b 02 ed d8 fb 56 6e 6a 3e bf 8e 70 09 0e 34 0e 22 70 b4 43 5d 81 df c0 87 73 3c 11 3f 68 10 a0 12 f6 12 f6 fa 4e 72 1d e4 81 dd 75 c9 25 34 08 e5 4f 89 09 3c 81 67 03 43 20 04 a6 3d 19 e8 9e 4f 47 4f 30 7f 8c 58 d3 de f8 26 07 e4 23 1a e5 05 1d e8 92 79 34 bd 84 6b 04 28 Data Ascii: j\X"`xyOe]/>"}/+F[!:2`bjVyuI]K?Gw-^>/ih,C#v\a^F=TJ%xP#)(X\KVnj>p4"pC]s<?hNru%4O<gC =OGO0X&#y4k(
2022-05-23 16:36:37 UTC	213	IN	Data Raw: 2e 62 10 96 cd b0 61 48 eb c0 1f 2a 96 a5 12 e5 d6 02 7b 7e 38 b9 b0 d5 63 ee c6 63 d7 f8 34 cb 4c ed 8b 41 53 45 f4 45 1d b9 e1 89 79 ab 0f 8a 68 72 a3 d7 2c ae 0e a2 05 7f be 43 1b b5 56 1f 3d 23 5b ce 97 e3 63 54 d9 4e 7a 35 bb b1 7a b0 34 e7 e4 aa e2 43 3f 52 6a ae 99 c9 d8 b7 2f d5 92 98 aa 71 77 c3 e1 ba ee a5 42 47 04 6f a2 dd ee 98 6e db d8 70 4f 89 8b 09 a2 78 bf 6e 8c 15 2d b3 3c 2e d2 17 1b cd c2 1b f4 64 e5 75 f5 a3 74 41 05 03 fb 2b 8f 48 59 8d a5 04 a5 71 ee 9d 5a 21 19 99 cc 6b 23 11 e5 54 62 11 cc 7d 5b 78 7a a6 38 52 fd 0d bb fa 8b f8 8d 8d 69 37 df 64 1a 33 c1 2a ad 65 57 91 b4 06 23 2c c1 2a f3 ce 37 a7 75 a2 bb ae f7 3e 7d 4d 7a 3d db 7e f3 e9 14 96 02 99 bc 61 cb 60 41 54 47 e0 c5 ea a5 24 26 82 6c 8f 4f 33 57 29 d4 9b 27 1c 22 3f d3 Data Ascii: .baH*{~8cc4LASEEyhr,CV=#[cTNz5z4C?Rj/qwBGonpOxn-<.dutA+HYqZ!k#Tb}[xz8Ri7d3*eW#,*7u>}Mz=~ a`ATG$&lO3W)"'?

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:36:37 UTC	229	IN	Data Raw: a0 40 ed 4a e8 7f 49 05 ea 03 aa 04 14 2f d0 5a 32 7c db e2 8f d0 fb fd ff 0b 1d 7c bf f7 81 a2 1d 94 5f 03 7b 53 50 7a 51 4b c7 b6 67 1c ff 66 45 ff d1 37 2b 1f 3b b0 1e e6 c6 8e 66 82 7b 2e c5 b7 95 07 b8 0f 20 c8 d9 39 c9 ff 04 03 0c 02 b4 7e a6 c0 10 fe 04 ca ca b2 cf 0a 07 3e d9 9f 80 81 72 c1 3f 12 79 00 48 63 68 60 03 fc e7 40 f3 23 e7 ff 6a d0 6c 7f 33 ea 9f 03 fd 7c d8 3f 87 fd c7 b8 ff 06 fc 1f 5c be e7 7f ff ab ad 80 61 ff 6d b3 7d 69 61 04 a7 8a ee 5f 6c c4 f2 77 43 fa e7 62 fe 1e f2 9b d5 fc c9 6e 88 8d 11 c4 c8 0c 6a 64 b9 6f 41 50 5b 1c 6e 28 89 90 81 ea b8 f2 9a 80 5c 2f 69 63 04 03 2d 15 ad 2b 1d aa c6 0a 88 9e 6d 58 c9 bf 71 56 51 28 f4 01 64 a8 84 39 6a 14 5f 1a b9 ed 35 32 74 03 42 b5 9f b7 71 3b 68 f3 63 d5 9e 53 45 8e 02 f8 91 7a 17 Data Ascii: @JI/Z2|_{SPzQKgfE7+;f{. 9~>r?yHch`@#jl3|?\am}ia_lwCbnjdoAP[n(\Vic-+mXqVQ(d9j_52tBq;hcSEz
2022-05-23 16:36:37 UTC	245	IN	Data Raw: fb e8 78 47 37 f6 fa 5e b2 5d 21 ab 2c a2 67 9f 48 44 2c 7b bb 22 5f e9 05 d5 86 1d a4 25 54 04 70 5e 56 62 02 33 d9 29 26 38 af 84 dc 5b b4 50 04 9a 3e 07 98 7e 0b 63 29 f1 b4 96 e8 68 90 ae 60 69 aa f4 59 b0 1d 39 b6 27 8e d8 bc a2 a8 fc e7 b3 b4 42 02 71 02 ea 77 d2 25 3d 15 96 ae 72 db 72 05 d3 6e d9 b9 59 9b f6 72 d9 bb 59 b7 5a 92 d4 cf 3d 05 ee 54 f6 24 6e dd 41 fe 94 5d 6a 45 b9 e9 df 89 85 af a4 24 5d 7e ba b2 e6 f3 fe dc df 4f d8 f7 1d 21 92 dd 04 36 5f 8f b6 67 54 f5 07 09 3d a0 da e1 67 95 6f 0b 0a d4 59 76 57 2d 6d 6b a9 da 9a 2c 4a 97 6a c1 a3 e7 df 4d fd 35 48 5e 58 f0 6a c1 cc 29 a9 88 b7 93 af ce df fa 6e b2 ae bb 32 11 08 c7 a3 9d de c5 9c ec 83 0c 2b ce 33 07 ee 61 9c af 7c 06 9e 6a e1 c1 a6 3b d6 29 3e 24 16 75 52 98 93 b2 7e c4 df 5e Data Ascii: xG7^]!,gHD,{"_%Tp^Vb3)&8[P>~c)h`iY9'Bqw%=rrnYrYZ=T$nA]jE$]~O!6_gT=goYvW-mk,JjM5H^Xj)n2+3 a|j;)>$uR~^
2022-05-23 16:36:37 UTC	261	IN	Data Raw: ea 25 32 63 01 ec 8f 67 12 76 9e 17 02 04 49 29 6d b2 07 00 3c b5 47 c6 9b 06 20 73 3b 3c f3 36 48 c9 ea 43 c9 a8 53 60 da 59 04 d0 d2 bb 04 92 ea bc 41 71 2f 5a 06 a3 51 36 2a e7 cf 4f d0 76 ed e6 fa 72 5f 47 d8 9a 4b c0 39 2c 84 42 d1 1d 9d ba fd 87 0c 0f 56 b9 db ac 93 a9 36 e0 4f d4 a7 17 9d f5 6c 9f 55 9a e1 6e 44 3a 6b 0d 81 57 eb e8 ca e9 0b 60 7f cf ed 30 b4 b4 2c 91 02 7c 9d 02 a1 4f 5d de 35 37 6b c4 c7 af f5 58 28 90 3b d0 c3 f2 ab c3 b3 f4 5e cf 0b f7 bb 45 9a a9 e9 f8 4b 8f 3c e7 f9 84 97 fa be 75 f7 af 4d 9a 6b ed 01 60 b7 21 54 91 a2 c2 1d dd fe 91 02 d3 3f ab 4d ed 1c c7 15 77 78 ca 73 17 9b ec f0 98 95 4d 07 0a f2 83 3a 27 8b f6 60 71 ad 0b 2d 1f 56 79 c1 c6 ba 41 ed d5 aa f0 fb 68 86 cf 15 55 b1 eb b3 76 d1 0c 6e 19 dd 96 3b 81 a1 f7 31 Data Ascii: %2cgvI)m<G s;<6HCS`YAq/ZQ6*Ovr_GK9,BV6OlUnD:kW`0,|O]57kX(;^EK<uMk`!T?MwxsM:``q-VyAhUvn;1
2022-05-23 16:36:37 UTC	277	IN	Data Raw: c1 f3 11 79 37 76 0b d7 3c f2 77 7b 1a d1 7e ce 59 12 6a 15 85 79 53 d1 f5 e1 3f ef 1b f2 39 bc b2 a2 66 5a bd 78 62 2e 79 77 36 09 f1 a0 7e 88 f3 d1 96 de 4d ff 1f b5 d7 25 e0 bb fe b8 7b e2 6b 8c ba 1d f8 eb b2 fc a6 a3 3c 3f bb 1b 04 73 20 bf 56 56 19 ed 89 49 8d 9f 32 20 7e b8 30 f0 5b b7 f2 20 cf 46 3b 78 51 ca 08 8f 9c 17 f1 87 64 09 dd a5 c4 a3 2b e7 24 42 1f 58 4f eb f2 b6 53 75 81 df 1e e7 0b 5c 1a 6c a7 e2 93 e5 67 49 56 d3 5b bd f0 6d d8 9e 62 51 e0 92 36 5d e0 f9 b7 19 6a 7e e0 b7 a1 06 aa c7 2d 19 6a c0 8a 75 d0 8f 3e 32 3d d5 61 e1 cd 7f 55 be c2 b8 67 f3 25 c2 03 4b 4b b9 b4 65 8d ba 15 02 ef a5 e9 ad 29 b8 9d c4 81 15 52 3f b5 cf 73 7b 2b d7 43 3f b6 8c 0f 91 12 a0 95 0c 58 f2 4b 7f 31 1a ab 0f d8 ef 45 76 d8 b4 d9 ce f7 d2 9f 71 7a 2a 72 Data Ascii: y7v<w{~YjyS?9fZxb.yw6~M%{k<?s VVI2 ~0[F;xQd+$BXOSu\lgIV[mbQ6]j~-ju>2=aUg%KKe)R?s{+C?XK1 Evqz*r
2022-05-23 16:36:37 UTC	293	IN	Data Raw: 53 cd be 40 00 d7 e9 fe 24 15 9f 36 e5 7c 7e d8 5f fb 32 ca 97 a2 9e a0 7b c1 6e a5 85 a4 23 e7 48 78 4d 01 ed c1 60 2f 62 2f 38 04 a7 ff b0 be 55 be 76 22 a2 66 0f 11 90 59 17 98 03 70 05 c9 ee 07 59 7e cc 0a a5 4f 0b 07 14 7f d2 96 4d 7d 27 90 9c 25 a8 60 c2 bc a3 ee e7 71 ef de 95 00 3e 96 f1 26 88 ab b0 11 4a 8b f7 04 18 05 e2 e3 93 12 60 a7 44 ef 22 b8 8d f6 6b 29 ec f7 ab 42 0f 26 c8 82 28 01 b3 6b 2e 70 90 3b 11 85 2c c5 ac 46 0f 5c c1 7f 5d cb 78 fd 1c c8 19 98 50 68 ef 34 05 b6 ec a4 39 19 63 43 ee 14 a4 0f 16 0f f9 77 b7 e2 94 ee 92 ae 89 14 f9 82 19 fa 1a d8 45 ab 60 43 8b 2f 28 7d 85 81 9a d1 62 f8 64 9e 7e 6f 0e 87 3f 0f c0 f6 68 41 65 f9 39 20 c9 1e 22 23 06 ce 83 fd 80 6b c0 ce 7e db b9 b2 24 94 21 fe 77 0d 6c 52 91 54 c0 f6 02 07 40 c3 ea Data Ascii: S@$6\|~_2{n#HxM`/b/8Uv"fYpY~OM}'%`q>&J`D"k)B&(k.p;,F\]xPh49cCwE`C/(}bd~o?hAe9 "#k~$!wlRT@
2022-05-23 16:36:37 UTC	309	IN	Data Raw: 90 15 20 4d 00 16 02 94 ce 56 d6 ff 14 29 d2 3b 1c e0 30 7b f0 6f 05 01 d8 c1 a9 52 10 10 7b c8 0f b5 80 01 07 44 3a 21 80 03 50 b9 95 a3 bd 0d 4a 1c c6 df 2c 1f 0c b2 07 ec 1a 88 02 20 63 47 94 af 35 d6 00 a9 1f a5 13 c0 71 2c 80 58 02 18 20 c8 18 39 89 15 b0 cc 40 da 03 d2 36 ad 4e 45 0e e0 32 87 da 03 a8 a1 c8 45 11 b0 3e 31 35 85 20 10 50 40 b6 8d 65 ae d6 10 20 8e fc 95 50 16 10 50 47 98 42 41 a7 ca b2 ff ee a7 80 bc 6a 80 35 15 30 04 6c 8d 40 11 06 06 c4 6e 05 82 36 66 42 51 c4 7d f7 44 40 ad 50 1b 37 80 7c 94 12 ff f0 81 6f ba 3c 65 ea 9b a7 7f f3 38 a4 30 a4 50 68 ad 4e f9 fb 6e e8 80 5b 01 ce e4 68 ef 68 0d 36 01 e6 42 80 81 85 21 30 59 63 99 b5 39 12 e6 0f db fc 47 a6 07 0c 44 06 b1 53 5e 80 15 22 30 cc 1a e2 0a 30 6e f5 8b 14 00 9f 13 04 b9 02 Data Ascii: MV);0{oR{D:!PJ, cG5q,X 9@6NE2E>15 P@e PPGBAj50l@n6fBQ}D@P7|o<e80PhNn[hh6B!0Yc9GDS^"00n
2022-05-23 16:36:37 UTC	325	IN	Data Raw: 90 10 30 c0 e8 1b 1a 26 4e 5e 60 e6 ef 41 d1 08 f9 fe 53 26 46 e4 9f 46 33 b2 80 dc b1 41 20 e4 a5 11 d8 c1 c8 c1 16 6c 02 71 60 a2 d1 47 70 72 71 f3 f0 f2 f1 d3 30 23 7b bf ef 47 f4 0f c1 04 90 bb 62 fe a3 1d 8e 00 0c b4 20 67 08 23 72 f7 36 fb d3 bd 93 00 d1 da 23 83 d4 a9 9d 9b 01 62 47 c6 69 10 d8 da 1a 6e f2 6d 27 40 e4 cb 44 00 b9 a2 06 cb 21 5d d2 c8 01 a0 dd c8 d8 d1 cc 8c 05 29 32 d4 db 4e 1d 91 fb b3 21 51 d8 23 dd 14 b5 63 24 12 0a b5 0f a2 d3 37 ec 48 a9 20 1b 91 74 40 61 4e 50 07 28 30 88 e9 b7 42 e2 62 66 fe ab 30 4c 90 7c a2 5e 8e 80 e4 16 b9 79 92 27 f3 9f 45 e9 6c 0f b6 fd 26 ca bf 99 82 17 35 c5 e9 3b aa 91 ca 62 e4 f8 2e 42 41 c6 d3 0e 24 2e 23 13 84 35 d3 29 10 0b 88 93 8f f9 8f 1e ae 3f 75 b1 00 f1 cb 94 0d 02 33 15 65 04 31 a2 a8 37 Data Ascii: 0&N^`AS&FF3A lq`Gprq0#{Gb g#r6#bGinm'@D!])2N!Q#c$7H t@aNP(0Bbf0L\|^y'El&5;b.BA$.#5)?u3e17
2022-05-23 16:36:37 UTC	341	IN	Data Raw: 18 99 34 84 5b e8 dc 66 a8 b3 85 4f bb 42 67 2d a9 3d 18 ee ad b5 23 17 9d 4d b8 fe ea 51 4e 42 64 9d 7b 59 fa 7e 2e 43 84 8f 2e 9c 5d d4 64 77 d7 e6 7e 2e a3 06 2e 6c 67 1b 3f ec a0 22 f2 5a a3 e9 aa 1e 3a ed de dd 6b 2b 98 98 ff 6e e7 a8 a3 47 0b 5f 68 5f fe 32 21 c3 31 2c b1 4e 98 e1 cc 8e b6 83 96 df ad 7f e0 63 97 a3 f0 ff cf 7c 66 fe 2c 8e 30 58 7e bf 95 f8 e6 85 cd 45 17 fa e8 2d d3 df d8 6b b3 de 83 b2 f1 0e de 7a a3 0f bb 36 7e 74 20 bb be 6b 6a ab cc 73 53 f5 9e 5f 31 ca 9c 08 58 9d d2 39 b2 9b e7 54 bf 47 2f 1b 6e 4c 7b b2 f5 ca 2d c9 d0 36 3d de 9c b3 e1 ad dd 30 bd 6f 6c c5 64 63 ab cf 99 0f 3f de 3c 75 73 c4 fb 9b 47 4f dd 0c fc d6 36 ce 6a cd 2a 19 df 2d 39 23 de 2f 32 5f d0 27 eb 65 bb 47 71 25 21 65 de ce 85 45 5d f8 c3 7b 3e 9b 35 f1 ca Data Ascii: 4[fOBg-=#MQNBd{Y~.C.]dw~..lg?"Z:k+nG_h_2!1,Nc|f,0X~E-kz6~t kjsS_1X9TG/nL{-6=0oldc?<usGO6j*-9#/2_'eGq%!eE]{>5
2022-05-23 16:36:37 UTC	357	IN	Data Raw: a0 bb 8b 44 99 84 4a c1 17 64 d0 47 28 a4 d3 4c 39 64 2d f0 8c 81 c7 ab 90 6e a1 c9 ad fe 86 49 b1 c9 fb 1f f2 37 34 44 99 1c 1c 71 f0 57 85 aa b6 7d 01 37 83 e6 4e 00 92 0c 3a de c1 b4 c8 a7 38 60 93 67 49 84 90 18 80 c4 23 57 2a c5 c9 12 04 27 09 6e d5 24 78 2c 0a f1 69 27 50 49 f2 b8 24 34 80 37 b9 82 63 1a 0a 37 15 60 a5 44 20 fc ec 06 04 46 40 0b e0 41 d0 84 6c 9e cd 97 64 61 c1 86 51 86 4c e9 85 64 6d 6c 7a 4e 22 19 c6 2c c6 0e 9a 55 2d bd d1 10 09 09 62 ec e8 31 08 9d 06 c6 e2 c3 ea 47 0b ec 13 76 40 8a 14 1a 9b 5f 21 52 65 29 64 6c f2 f6 46 67 b1 95 17 e0 82 84 1b 61 05 68 7d 90 81 01 6c 03 ba 8d 09 8c 8f 62 c6 92 48 43 82 a7 3a fa 2d 97 87 ff 05 92 a4 8c 7c 0b e5 e9 44 01 3f 93 fc 88 e4 0d 5e cd 52 00 a6 62 e6 74 07 32 79 ae 2d 79 74 83 ed 1a db Data Ascii: DJdG(L9d-nI74DqW}7N:8`gI#W*'n$x,i'P!$47c7`D F@AldaQLdmlzN",U-b1Gv@_!Re)dlFgah}lbHC:-|D?^Rbt2y-yt

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:36:37 UTC	373	IN	Data Raw: 0b ac cb 91 d9 c1 e8 16 28 aa 1c 0e 23 63 fd c6 82 cb 87 e0 44 8c 5f 4a ad 21 b5 7a d5 4b 5e c1 0a 39 8a 2c a6 90 55 2d 35 ac d4 eb 8b 92 20 d0 41 6b eb 46 98 a3 48 0d f4 d1 9c 47 6e 2c 16 2d 01 e6 87 9e 01 74 40 3e 22 c7 17 9a f0 c9 72 8a 34 92 f1 a9 8f 0d f1 0c 76 6b 3e dc fe 95 42 c5 34 3e d8 95 b5 78 e4 e1 80 2b 7c fd c5 79 c8 98 97 71 06 0e d8 dd 02 7c 86 ff cb 61 3e 74 2c d4 3f 32 fd aa dd 2f fd 37 e6 5f 83 6a 02 8e 07 2d c9 a3 df aa 1f 00 1c 35 d1 9d 62 f2 50 47 41 27 02 cb 8a 8c cf 1a 74 03 0d 73 9e a3 73 be 86 93 a3 fa cc 38 ec 33 9d 65 af a4 0f ea 5c ea 94 64 17 aa 26 d7 99 5c 63 4a 55 a7 8e 4d b6 b5 bb 96 93 9a 6c c9 6c b1 6a 10 e0 39 9d 5b c3 09 4d d6 65 53 7f 3e b7 da 11 4d c9 95 30 f6 db 96 8a 30 21 45 f9 7e 80 10 fb c9 78 84 48 25 e0 d2 51 Data Ascii: (#cD_J!zK^9,U-5 AkFHGn,-t@>"r4vk>B4>x+|yq|a>t,?2/7_j-5bPGA'tss83e\d&\cJUMllj9[MeS>M00!E~xH%Q
2022-05-23 16:36:37 UTC	389	IN	Data Raw: d2 c8 d9 3a b9 ee eb 89 c1 a7 66 77 64 ba 43 9c 10 48 8a 79 f1 ce 4d f3 41 4f f3 7c 76 04 94 d7 0b 3a ba a0 86 fa d8 19 0f bd e4 19 bb 11 c5 3e 2e b2 2d 41 f3 5b 77 80 11 1d a0 af 46 22 59 7f 5d 44 bb 61 97 01 03 8b ec 04 17 82 aa 71 36 1d 47 bd 51 78 7d 1a 51 6b 9d c1 ba 32 67 84 30 84 69 00 7c c9 59 c4 14 31 b2 fd f8 4f 3b a8 b5 ae 5a ed 3a 92 b0 f4 b3 0d 1f 7c d6 7e 09 6b 68 32 84 f6 b4 ae 1e bf 14 0b 2f e3 ef 31 23 e0 85 1d 48 b9 d3 6e 10 01 bf d3 aa 6b df 5c 14 86 b4 81 c8 fa 68 51 4b 5e 47 76 bb e2 11 72 0f 0e 11 f8 f3 df 54 1b f9 5b 90 a5 3c 56 e8 2d d8 70 0a 34 ac d8 3d aa cb 29 8e b4 8d 03 a1 a3 6a 6c f6 1a 68 80 66 cc 6a 13 3a 4e 1e 90 d8 90 5b 90 b2 53 16 ad 62 e1 11 d0 c3 8b 6d 37 a1 5c bc 74 b2 a7 b4 59 13 de 92 94 71 f6 9f b5 90 30 b4 8b f1 Data Ascii: :fwdCHyMAO|v:>.-A[wF"Y]Daq6GQx}Qk2g0i|Y1O;Z:|~kh2/1#Hnk\hQK^GvrT[<V-p4=)jlhfj:N[Sbm7\tYq0
2022-05-23 16:36:37 UTC	405	IN	Data Raw: 2b 86 c4 3a 74 dc 32 32 90 6d a5 be 11 1e 5a 0c b2 c1 b3 d1 e4 b6 d6 e4 f1 20 a8 99 2c 5b 5e 30 b1 9c 2b 43 c6 2d e7 be 1b 21 b1 ee 0c 7c 7e 6d e0 87 46 bd e4 1c 8e 65 fc 35 34 94 b5 4f 6b 66 2e be 92 b5 e6 cc 35 89 da f1 7f 15 d7 bc 69 22 f6 59 d6 be a9 d4 b6 c9 f1 ff 86 e5 f0 a7 b0 7f 37 f1 7f ab ab 9d 1c ff d7 69 ad 7e e5 ff fe 8a cf 57 fe ef 2b ff f7 6f c6 ff 21 74 5c 92 ce 34 03 a9 2b 89 79 3b 0f 31 94 3b 8c 08 2b 0e 13 c1 e5 57 86 f1 ad f5 9c 35 26 a4 f8 83 5c 05 11 99 9f 54 56 c6 4f c3 fa 27 8a a0 98 dd 73 49 be 8c c5 69 59 17 a8 f0 b2 e8 fe e4 7b 84 4c 66 34 84 0e 93 6e 92 12 c2 d5 88 6a 7e 01 54 d2 c1 7a c5 3c 29 6b e9 c2 59 c3 fa 1d 99 28 b1 7e a4 63 6d 8c 5e 1e a8 b7 a7 82 65 c2 34 16 97 ab 2d 8d 45 59 1b d6 b1 9b a4 02 c5 88 dd a4 e4 e4 5d 03 Data Ascii: +:t22mZ ,[^0+C-!|~mFe54Okf.5i"Y7i~W+o!t\4+y;1;+W5&\TVO'sIiY{Lf4nj~Tz<)kY(~cm^e4-EY]
2022-05-23 16:36:37 UTC	421	IN	Data Raw: 67 11 5d c5 f2 33 55 56 78 3f 97 31 a8 f6 56 b0 34 5a f2 e8 66 54 4d fe 95 fd fa ac 46 66 9b 84 b5 19 fe 81 ab bd eb f9 d0 72 c0 03 9d b6 b6 95 bf a8 6f 7e ca 12 54 4e ed 3c 56 76 62 e4 0c cc 10 d4 b7 9f 47 13 ea 52 40 29 30 bc 26 1f 06 7d c4 91 4a 59 ca 68 b7 b4 2a 87 02 f6 f5 c6 34 b8 3a c9 49 2f e4 1d 3a e5 92 10 1f 0e 85 8c 24 62 0d 45 54 73 f4 c3 61 5d 04 35 19 bc 32 1d 23 42 2b 73 47 90 5c 86 64 20 f0 2c cd 59 ce e7 12 67 e6 8c aa 70 46 cd ab 29 3b 5a 18 e1 53 97 93 57 ac 3b 4e 45 b0 1b ae 50 8f 49 03 a1 da 8c 49 31 85 e9 54 2e 87 ee f9 42 3a 9f 64 42 19 0b 42 8c ca 79 5b fb 3e 22 9d d4 c0 ee f6 36 84 d2 a6 5b 57 a3 84 d9 5d aa 52 e9 83 76 47 7f 6b dd b7 e8 18 de 34 b6 ee f9 18 a8 48 63 a9 92 96 f7 8e 07 b5 10 76 c3 bc 6a 97 98 2c 5a a2 d2 11 fe 79 Data Ascii: g]3UVx?1V4ZfTMFfro~TN<VvbGR@)0&}JYh*4:I/:$bETsa]52#B+sG\d ,YgpF);ZSW;NEPII1T.B:dBBy[>"6[W]RvGk4Hcvj,Zy
2022-05-23 16:36:37 UTC	437	IN	Data Raw: 98 14 f4 9d 84 21 f3 19 36 5a e9 58 de e8 6c 03 33 4f cd 51 c5 c2 aa 93 43 76 96 b2 3b 5a 25 db 6a 2c c4 61 b5 69 68 9c a1 e2 3d 20 a7 04 92 6d 68 40 e7 61 87 7b b8 0b 02 e0 76 48 d2 ea 10 15 79 14 ab 98 24 14 6a d8 bd da 6c d7 1b 9e 95 a7 63 0b 6c 0d 2c 8c b0 42 02 7e 1b e9 a8 1d 78 dc 24 1c 5c 54 64 cb 3c 5c 6a b7 e5 9b 1c 19 8a dc 88 5d 50 48 c2 b8 d7 8e ea 93 ef 42 56 1f 51 f2 43 cb a7 13 4d c3 32 32 97 7c c5 dd 5d a0 e6 c9 cb dd 61 04 06 8e ac 92 f4 89 e1 55 3c 9a 8f d4 64 8f 22 87 16 0a 5a 6c 2c 74 6b c3 68 86 24 55 ea 6f a5 13 a0 2e 71 ef e0 b8 fb d3 f6 3f 1b 82 16 a0 6b 41 6f 4f fc 7d f0 66 1f e3 4b 6f d3 d4 1c c2 9c 18 99 8d 08 98 86 31 dc 78 82 1c 50 de 1a 0e 32 35 54 c5 2d 64 8f 50 98 88 52 4b e1 b7 c8 78 69 08 43 37 74 9b 0c 37 13 ee 50 54 f4 Data Ascii: !6ZXl3OQCv;Z%j,aih= mh@a{vHy$jlcl,B~x$\Td<\j]PHBVQCM22|]aU<d"Zl,tkh$Uo.q?kAoO}fKo1xP25T-dPRKxiC7t7PT
2022-05-23 16:36:37 UTC	453	IN	Data Raw: ba fb 47 42 48 d5 0e e2 17 ee 1e 52 41 bb 8b ba c0 94 5a 9d 19 e7 fe 6d c4 42 76 23 f9 c1 de 39 21 2e 03 97 06 ff f0 87 a0 40 27 f4 f9 75 bb 90 d6 90 b5 54 1d 49 66 ef d7 6c 52 10 3b a0 d5 a7 f7 9d 36 44 66 72 96 4e 07 ed 4f e5 ba 43 f6 71 eb 0a 2e 80 98 f7 cb 1f 7f a1 13 fc 54 96 ce ec 5c 5d 6e 68 fe e0 18 86 ff ca 2c c6 2b 97 48 74 6f 89 44 f0 f7 02 57 65 e1 74 0f 5b a5 2f ab 2f 11 5b b7 e2 12 b1 75 f7 a3 5c ec e1 b9 54 6d 3f d4 c5 55 23 33 9f 7b 37 87 91 b5 ab e6 e8 39 6d c8 c4 4c 05 7b 20 64 c0 ae 2b 8c f5 eb 20 cb a4 1c 19 ff 53 84 6a 70 ba 40 29 4b e0 5a 10 a7 95 6e 0e eb 1d 62 0f f9 95 17 83 56 b0 4b 24 23 6a 95 93 f0 70 44 af 2b c1 f9 0e 34 55 6e 33 85 db c2 5d 8d fd 9e 2d de 72 bb da 4c f5 9a 3b 25 fc 85 77 ab 56 cb 80 7e 21 4c 7f 54 6e 6e 6f e9 Data Ascii: GBHRAZmBv#9!.@'uTIflR;6DfrNOCq.T\]nh,+HtoDWet[//[u\Tm?U#3{79mL{ d+ Sjp@)KZnbVK$#jpD+4Un3]-rL;%wV~!LTnno
2022-05-23 16:36:37 UTC	469	IN	Data Raw: d0 e9 2c 49 c2 30 9e 57 70 29 31 87 83 22 10 ce 41 ea 9f c3 e0 bb b3 68 06 ac 04 95 a6 5e 6f 3a 1d cc 87 15 77 30 d5 2b f7 ff 7e 2b b0 1a 9b f3 a2 19 18 d4 1c 38 0d 20 fb 80 7c 09 fb 3e 0e 7b c0 ad 41 ce 87 43 34 9f 24 78 88 9c aa 6c 06 8c f3 fc d3 13 eb 3f ea 8f f8 36 a0 69 ff 37 eb 03 5f 79 41 02 db f3 fe 4b 3f 82 ff 36 e8 f6 7b f8 fe 1b f6 c3 f1 7f 09 7e cb 37 69 f3 f3 4f fe fe eb ec 3f 3e ed fc 26 7d dc 7c ff fb dd f1 e0 d3 fe ff 1e 3f 85 fd f7 6f 83 0f d4 c7 7b fc 3f 40 d8 1c d1 fe f7 47 21 68 14 40 27 bd e1 10 cf ff 27 ff 8f df fe a7 dd 6e d7 b6 d9 76 91 1e 06 75 d7 63 d7 c6 bd 7b 7e ba f5 5a b4 db 9e ad 31 47 fd 17 e4 1d 17 fc 29 ca 17 d1 b2 5e e3 58 22 0e 4d da 68 f1 c3 43 7a 92 54 91 e1 50 c0 e7 82 00 64 86 c3 c0 91 1f 96 d1 f6 ec c7 e8 e2 90 23 Data Ascii: ,I0Wp)1"Ah^o:w0+~+8 |>{AC4$xl?6i7_yAK?6{~7iO?>&}|?o{?@G!h@"nvuc{~Z1G)^X"MhCzTPd#

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49758	142.250.185.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

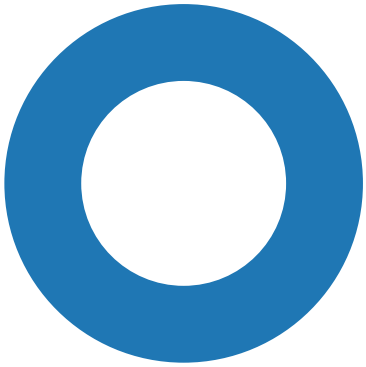
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-23 16:36:37 UTC	1	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2022-05-23 16:36:37 UTC	35	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-bozR8jDGx5KUfsGgPJ1jlQ' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 23 May 2022 16:36:37 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5621 X-Daystart: 34597 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-23 16:36:37 UTC	36	IN	Data Raw: 33 36 64 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 32 31 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 33 34 35 39 37 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 36d<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5621" elapsed_seconds="34597"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-05-23 16:36:37 UTC	37	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-05-23 16:36:37 UTC	37	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior

chrome.exe
chrome.exe
chrome.exe



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **1560**, Parent PID: **1728**

General

Target ID:	1
Start time:	18:36:31
Start date:	23/05/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://cran.r-project.org/src/contrib/fansi_1.0.3.tar.gz
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **2464**, Parent PID: **1560**

General

Target ID:	3
Start time:	18:36:33
Start date:	23/05/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1568,67622 21054703538292,13481123294093446 56,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6584**, Parent PID: **1560**

General

Target ID:	4
Start time:	18:36:39
Start date:	23/05/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=quarantine.mojom.Quarantine --field-trial-handle=1568,676222 1054703538292,13481123294093446 56,131072 --lang=en-GB --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=4772 /prefetch:8
Imagebase:	0x7ff7964c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly