ID: 397496
Cookbook: browseurl.jbs
Time: 00:56:07
Date: 26/04/2021
Version: 31.0.0 Emerald

Table of Contents

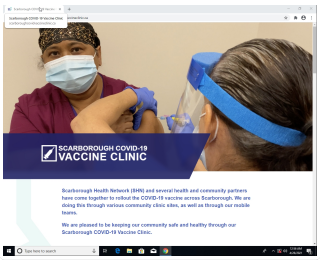
Analysis Report http://scarboroughcovidvaccineclinic.ca

Overview

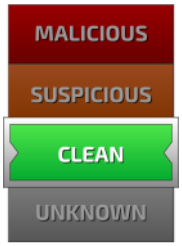
General Information

Sample URL:	http://scarboroughcovidvaccineclinic.ca
Analysis ID:	397496
Infos:	

Most interesting Screenshot:



Detection

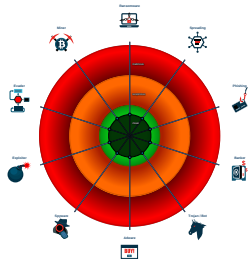


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5444 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://scarboroughcovidvaccineclinic.ca' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6060 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1504,4227342176911685725,17676476267147671780,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1808 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

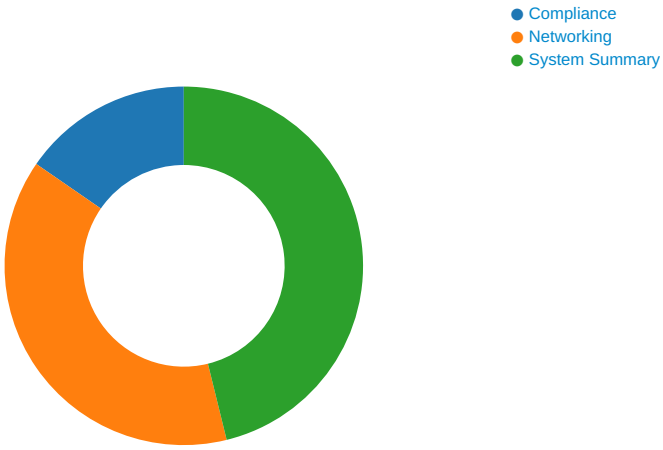
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



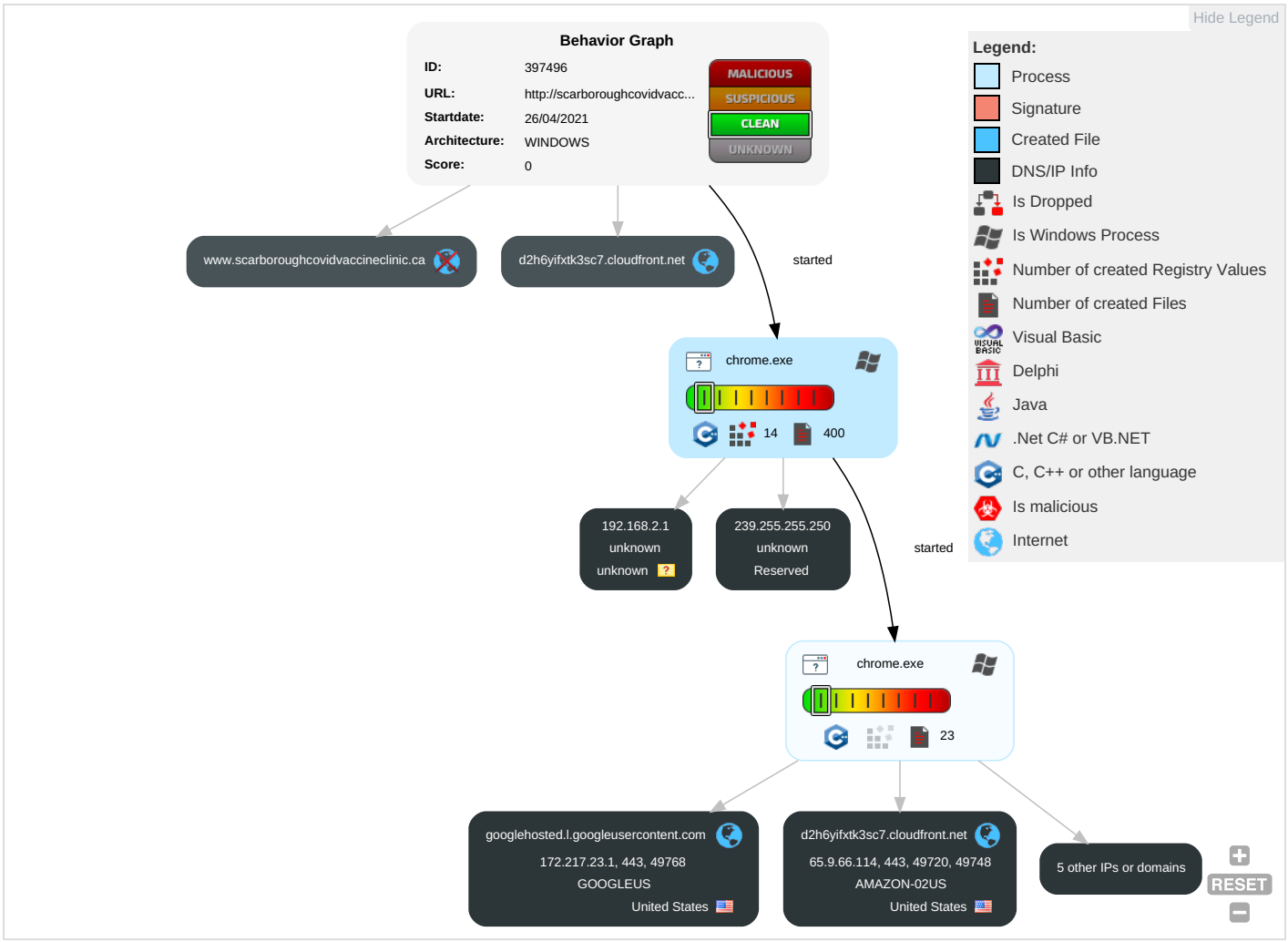
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
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	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic 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	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://scarboroughcovidvaccineclinic.ca	0%	Virustotal		Browse
http://scarboroughcovidvaccineclinic.ca	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
scarboroughcovidvaccineclinic.ca	0%	Virustotal		Browse
www.scarboroughcovidvaccineclinic.ca	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://scarboroughcovidvaccineclinic.ca/w	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.scarboroughcovidvaccineclinic.ca	0%	Virustotal		Browse
http://https://www.scarboroughcovidvaccineclinic.ca	0%	Avira URL Cloud	safe	
http://scarboroughcovidvaccineclinic.ca/	0%	Avira URL Cloud	safe	
http://maps.gstatic.cn/mapfiles/transparent.png)	0%	Avira URL Cloud	safe	
http://maps.gstatic.cn/mapfiles/api-3/images/mapcnt6_hdpi.png	0%	Avira URL Cloud	safe	
http://maps.gstatic.cn/mapfiles/api-3/images/mapcnt6.png	0%	Avira URL Cloud	safe	
http://scarboroughcovidvaccineclinic.ca/Scarborough	0%	Avira URL Cloud	safe	
http://https://www.scarboroughcovidvaccineclinic.ca/scripts/main.js	0%	Avira URL Cloud	safe	
http://https://scarboroughcovidvaccineclinic.ca/	0%	Avira URL Cloud	safe	
http://https://www.scarboroughcovidvaccineclinic.cah	0%	Avira URL Cloud	safe	
http://https://www.scarboroughcovidvaccineclinic.ca/Scarborough	0%	Avira URL Cloud	safe	
http://https://www.scarboroughcovidvaccineclinic.ca/img/favicon.png	0%	Avira URL Cloud	safe	
http://https://www.scarboroughcovidvaccineclinic.ca/2#Scarborough	0%	Avira URL Cloud	safe	
http://https://www.scarboroughcovidvaccineclinic.ca/#Scarborough	0%	Avira URL Cloud	safe	
http://scarboroughcovidvaccineclinic.ca/2#Scarborough	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d3ju03wkwsvm74.cloudfront.net	65.9.66.41	true	false		high
d2h6yifxtk3sc7.cloudfront.net	65.9.66.114	true	false		high
googlehosted.l.googleusercontent.com	172.217.23.1	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
scarboroughcovidvaccineclinic.ca	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
www.scarboroughcovidvaccineclinic.ca	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

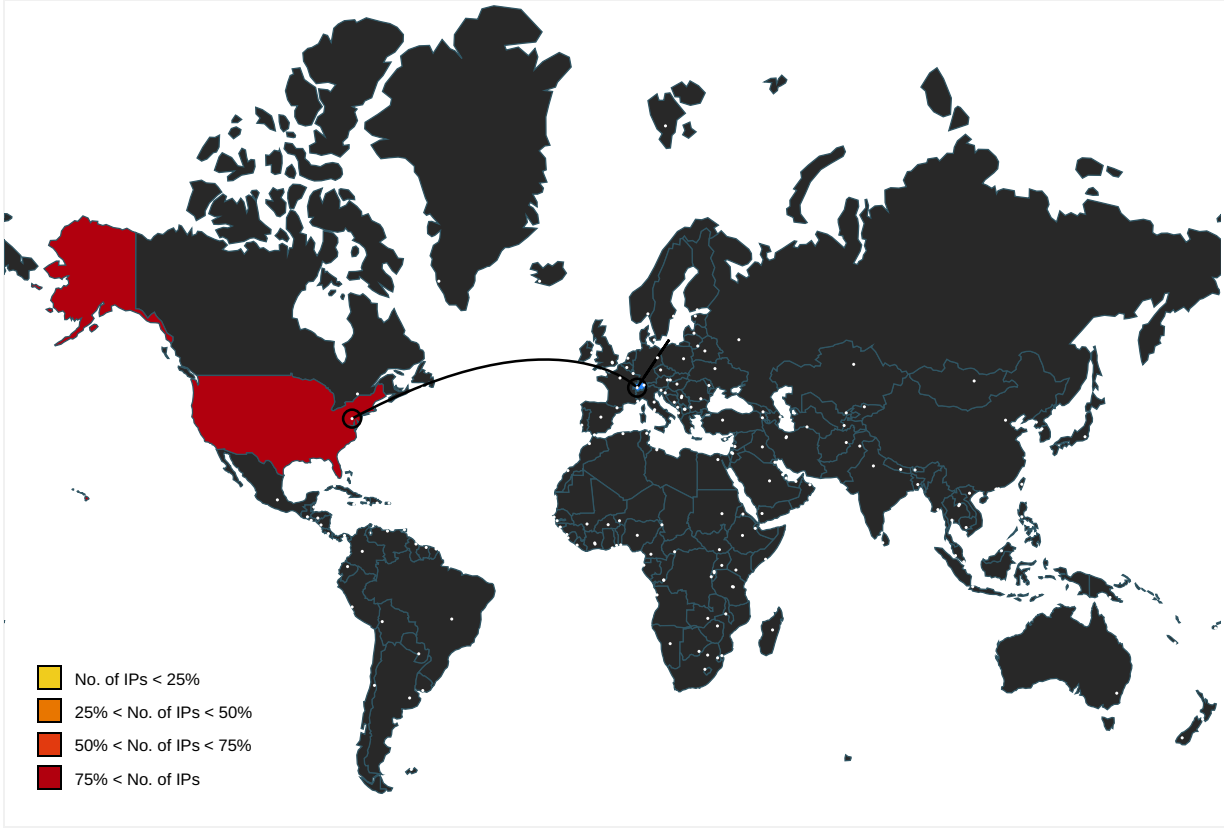
Name	Malicious	Antivirus Detection	Reputation
http://scarboroughcovidvaccineclinic.ca/	false	• Avira URL Cloud: safe	unknown
http://https://www.scarboroughcovidvaccineclinic.ca/	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://scarboroughcovidvaccineclinic.ca/w	a81ab65c52e7e79e_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.scarboroughcovidvaccineclinic.ca/	Current Session.0.dr, Favicons.0.dr	false		unknown
http://https://dns.google	ca62a7f1-7a9c-4484-92e9-95f305ee5dd4.tmp.2.dr, d8cf2033-ee1e-4c30-a219-264e6d3e5124.tmp.2.dr, a0215c8c-894c-46e2-81b5-352f9c6c84ba.tmp.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.scarboroughcovidvaccineclinic.ca	Current Session.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://maps.gstatic.cn/mapfiles/transparent.png)	8bc35d0ff67b9910_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://maps.gstatic.cn/mapfiles/api-3/images/mapcnt6_hdpi.png	8bc35d0ff67b9910_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://maps.gstatic.cn/mapfiles/api-3/images/mapcnt6.png	8bc35d0ff67b9910_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://scarboroughcovidvaccineclinic.ca/Scarborough	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	d8cf2033-ee1e-4c30-a219-264e6d3e5124.tmp.2.dr	false		high
http://https://www.scarboroughcovidvaccineclinic.ca/scripts/main.js	358aba68fb857741_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://scarboroughcovidvaccineclinic.ca/	358aba68fb857741_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.scarboroughcovidvaccineclinic.cah	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.scarboroughcovidvaccineclinic.ca/Scarborough	History.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.scarboroughcovidvaccineclinic.ca/img/favicon.png	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://www.scarboroughcovidvaccineclinic.ca/2#Scarborough	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.google.cn	e48c5ac7e290c9ab_0.0.dr	false		high
http://https://www.scarboroughcovidvaccineclinic.ca/#Scarborough	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://scarboroughcovidvaccineclinic.ca/2#Scarborough	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.1	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
65.9.66.41	d3ju03wkwsvm74.cloudfront.net	United States		16509	AMAZON-02US	false
65.9.66.114	d2h6yifxtk3sc7.cloudfront.net	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	397496
Start date:	26.04.2021
Start time:	00:56:07

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://scarboroughcovidvaccineclinic.ca
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:	18
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@30/176@4/6
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 93.184.220.29, 104.42.151.234, 52.255.188.83, 168.61.161.212, 172.217.22.205, 172.217.20.238, 172.217.23.78, 173.194.187.138, 173.194.188.39, 172.217.23.40, 216.58.207.164, 142.250.185.206, 172.217.23.42, 172.217.23.35, 216.58.207.131, 172.217.20.234, 172.217.23.10, 172.217.23.74, 172.217.22.202, 172.217.22.234, 216.58.207.138, 216.58.207.170, 204.79.197.200, 13.107.21.200, 20.82.209.183, 184.30.20.56, 92.122.213.194, 92.122.213.247, 104.43.139.144, 13.88.21.125, 52.147.198.201, 13.107.4.50 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, clients2.google.com, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, r2---sn-4g5ednse.gvt1.com, elasticShed.au.au-msedge.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, www.googleapis.com, r5---sn-4g5e6nsy.gvt1.com, au.au-msedge.net, blobcollector.events.data.trafficmanager.net, clients.l.google.com, maps.gstatic.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, maps.googleapis.com, redirector.gvt1.com, www.googletagmanager.com, arc.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, r5.sn-4g5e6nsy.gvt1.com, prod.fs.microsoft.com.akadns.net, accounts.google.com, www-google-analytics.l.google.com, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, afdap.au.au-msedge.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, au.c-0001.c-msedge.net, r2.sn-4g5ednse.gvt1.com, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • 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 NtQueryVolumeInformationFile 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

ASN

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:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
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 GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\22b5276c-41d0-4459-aa46-bb0c0e819197.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):	165275
Entropy (8bit):	6.081802872287052
Encrypted:	false
SSDEEP:	3072:r1aw3DX4JNwA3Im6Xo7W1Vu/srl8CUFcbXaflB0u1GOJmA3iuR2:h3kZ3WXC1kuCSaqfllUOoSiuR2
MD5:	27C05FBB7E23C5677963E460D740897F
SHA1:	64C7754BE9CA4B06B190BBA1657C7DF6BAA0CE8C
SHA-256:	E32653CBD141828EE95AAF805247818A75EBB8D76B35D4F36EE9C5173810C80E
SHA-512:	5FB790A94DCEB5C7AFAA5336163BBA0947EC5811A8AF7779059E67CF1F60FB4280A649D7C3633FCCF43D61024B95D9CEDC4A28F28189681E925C33B37ED46F9
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":1.619423811842867e+12,"network":1.619391413e+12,"ticks":90826301.0,"uncertainty":4452570.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016961924"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\8aa04103-0f13-4baa-bdc2-68406a63ee75.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.746279202619277
Encrypted:	false
SSDEEP:	384:3nZGuwTZoMrS1NOrrviq3h6kZH0hGVcrH0iIxJUIcbrDym/kHk2G6FO8YWNX1m/e:jmBpCUFNwenEuwY/3WqKc6Gx5
MD5:	6D589D0755319260EC5DAC1E15B780F5
SHA1:	1FE359C1079F00E2EB31A279D3AF07AA6804635A
SHA-256:	60AD83A439EF2B37D330786300F2B7302029B1D8B14A0292CA2AD742D802A98F
SHA-512:	C74D73A6231131A40B99B56F9C7FD24A3BF48373AE8F8B57F2777BA86814F9A822C31ECA49D4582386FEA4BB0D17B29FC931BA101B7C2527BC84555B9BFCA56
Malicious:	false
Reputation:	low
Preview:	0j.............*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.......g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...?88.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\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftIE1G1mkftIE1G1mkftIE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC...................s}.....M..2.!..%sdPC...................s}.....M..2.!..%sdPC...................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\388c4fb2-df3e-4fc4-8d80-23f9374c956c.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):	5695
Entropy (8bit):	5.192592665082306
Encrypted:	false
SSDEEP:	96:n5tc96+PXfVNLCf5cVjok0JCKL8AlkT4MHY6bOTQVuwn:n5i8YfvYcg4K5lkT4hQ
MD5:	5439BD232E53556BF20C2D1452B2611E
SHA1:	3539DACC97B326D547A492ACD7A1906C89C51F47
SHA-256:	F3E895EA3F3C2D64BC12C350F27D334E73801CCF93F41D7947740343984073C0
SHA-512:	D06CA8F67DFAEDB71CDF79EDC0775209DEAB351761488BA2841822EFB8889EBACB50719102EF1087E253322241E81471C712D81ADAC2E35F3A9DDCE603657BC
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13263897409174853","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\435d239b-30fc-42e7-b4d6-8866801f08e1.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):	5694
Entropy (8bit):	5.193335609176677
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\435d239b-30fc-42e7-b4d6-8866801f08e1.tmp	
SSDEEP:	96:n5tc96+PXfVNLCf5cVjok0JCKL8JkyMFPbOTQVuwn:n5i8YfvYcg4KSky4
MD5:	A968B5AA592F64F73EADAF099FA15D03
SHA1:	7706EB49988ECB94F7D67F24599A0A65D2EBDB74
SHA-256:	79DB339D15740AD796909E8EB0E06614042B1AF32CC2458870D1A14F9070D376
SHA-512:	95AF4E2A03CDAE5B02D7DA1A5561A674803622B86A3B241B6B5F2ECE0A37AE3F7BBF9BCCB93081559F34A003C6FB8E29AA23D7F4B3ADC7940A3FCD95B4F178 16
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13263897409174853","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\515e42a6-f54e-4061-a9c6-cfeb34718707.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):	5099
Entropy (8bit):	4.979814690831882
Encrypted:	false
SSDEEP:	96:n5tc96+oXfpcVjok0JCKL80Kkf1AbOTQVuwn:n5i87fpcg4KDKkfA
MD5:	241D3B2AED4259F54C88852246298307
SHA1:	54300EF314B0B9342477BDE1365E0A0D32EA3C61
SHA-256:	E150C565D3E14076136221BC78678AC735914C544A72ECA13CEA53DBF7AE36C8
SHA-512:	8CCA0260BDA7715734515CE35782F3D36F9470EFBE1DDA0A5D616B0AEA53A5BE6005273F96B07D096B14ED17ECE167E135DE6A91D6ECD2973E88B4F0B58241 0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13263897409174853","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\592706c8-b1f4-4c03-a837-9ba59dd0f599.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):	1206
Entropy (8bit):	5.572906662446376
Encrypted:	false
SSDEEP:	24:Y529RAeUgr6I6H0UhVsTG1KUerkq/HeUeXby2qUeXvZ7wU1ZRUenHQ:Y5qieU26I6UUhVseKUewqPeUer2UefB4
MD5:	0A35EC874A55204E1A2D9087B3464908
SHA1:	1E382B5059A856775C41732451A1BB1A74B2BBA9
SHA-256:	535B3BD9097FF60C3B0C4F697C925E6ECC441B286632946FAC50CDAD7A8784FA
SHA-512:	631CA578929AB84B5125FF5E3814004E0BE84D2381CFA95A466EE5D30F5D5584CB6827CCA3280C27596F9E14EEF74B5008524B65E630B1AA647CEB90FDD2D7E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1650959812.276911,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1619423812.276915},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1650959811.648624,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\76ba52ea-133b-4709-8dc0-a40fff233c73.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\76ba52ea-133b-4709-8dc0-a40fff233c73.tmp	
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7f8844b7-cfd8-4504-bea2-ad5621be59ea.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):	5695
Entropy (8bit):	5.193996524373504
Encrypted:	false
SSDEEP:	96:n5tc96+PXfVNLCf5cVjok0JCKL8SkZj0bOTQVuwn:n5i8YfvYcg4KlkZi
MD5:	7F8CAB268FE0D78FF07E41E8A44AA5D0
SHA1:	D6E749747837BBB990C65680AFFF47E4D9CF0F6E
SHA-256:	EC6DD981AD366C690DFB639E7D69C4BADA5967F4413ED37290BF5FB49D0E01B9
SHA-512:	2C9503FD17BB9C913EDC9EBFE381E243B62773428F1E84D80481BB0C698A483E6B7C024130AC9C044E30CE1E673024F88E713C59E286A168C02EE073E0674C13
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13263897409174853","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8266be5b-2de3-4475-85c2-68cbf9c4a0d3.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):	16745
Entropy (8bit):	5.577547442258661
Encrypted:	false
SSDEEP:	384:ifPytILlY1XD1kXqKf/pUZNCgVLH2HfDbrU/1A6d4Y:CtLlsD1kXqKf/pUZNCgVLH2HfXrU/1lJ
MD5:	754C168D29879DB712B6730DB9CE20DF
SHA1:	75E58E25BFE895DF68A80812CC0DAB7D35D0F6F2
SHA-256:	A7C7F253BCDA013ADEAE183B915830A7FD740B05B3B28C5F642F11F5B4A5A3D3
SHA-512:	657D3034EE77BACCD499D7994EFDD1422DE85BB77271C9C5D9A9C63A52BAC2DCB37EEEB8C1573F931168DFCA92D180E20C6FF4C41616C6692928FC26BD216 E6
Malicious:	false
Reputation:	low
Preview:	{"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":"13263897408943406","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8f9ca9f6-e1d0-441a-9adc-195aebfc60b9.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):	22595
Entropy (8bit):	5.535867083049918
Encrypted:	false
SSDEEP:	384:ifPyt1LlY1XD1kXqKf/pUZNCgVLH2HfDbrUQHGfnT3pAxd4W:CiLlsD1kXqKf/pUZNCgVLH2HfXrUUGfC
MD5:	54E3CBD2E849884EF0FAFFCF2229E6CF
SHA1:	BE5ED3CEE83F96BD8B65F2D7799C6375B14B5E55
SHA-256:	C6930A828AF2965D36570213ACDEDF2B5A3BC596CE01B90CD75A36294707C79E
SHA-512:	CAF60ECAB9E6F6C0D48671CF26D7540C5977E46FA8B517C28BDDFAD9E56D59FF9D8175693517A995DA32DF1F1DF50084EFEDB3726F4A26060C838476165E76
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8f9ca9f6-e1d0-441a-9adc-195aebfc60b9.tmp	
Reputation:	low
Preview:	{"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":"13263897408943406","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.230081796241328
Encrypted:	false
SSDEEP:	6:mRo1/VTLEcN+q2PWXp+N23iKKdK9RXXTZIFUtp0o1/VTLAZmwP0o1/VTLXNNVkw3:xR4cN+va5Kk7XT2FUtphRE/PhRDfV5fv
MD5:	9B68E4EED8B1E783972A80CEBDF43829
SHA1:	205F8F54672F948DE2C1A8CE38B671E0C38FED0C
SHA-256:	63581883FA1116A91CDAE85056EEAD7446911387478238FB1F0AA43B71C64C00
SHA-512:	AB8CB2AFF399184DE271EB3605DB4E303214B178E6B14057348B7F1025BC147A8FA51C193E8380EDEAC8A7A0FA12EB5CA8914242F6B4BF4B2790E34F98766C5
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:06.412 147c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/04/26-00:57:06.424 147c Recovering log #3.2021/04/26-00:57:06.425 147c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.230060955213624
Encrypted:	false
SSDEEP:	6:mRo1/VTLjN+q2PWXp+N23iKKdKyDZIFUtp0o1/VTL8XZmwP0o1/VTL6UNNVkwOW+:xRd+va5Kk02FUtphRgX/PhR+KV5f5Kky
MD5:	E2886FA664A5F2F15AD3032160467EB5
SHA1:	92E418DA25EB1B34F8F740FEE4BFD55EE3BC0604
SHA-256:	7BB53A67105A523EFF23FE89E020B46150C3654F18BE09803BCAAA814E9B5DC1
SHA-512:	912E840BCE804AA78F297AC36E294C0EB5E8AA9B80B4ECEFBB95AE5EF19848BF59F215B214ABA60C247A61B290A9E752CE7EA43984A69A1DF8974436BD75BBD8
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:06.395 147c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/04/26-00:57:06.406 147c Recovering log #3.2021/04/26-00:57:06.407 147c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0cee26b990190c0c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.723824487789229
Encrypted:	false
SSDEEP:	6:mgl/PYZHfY7cEWcgu/RBlgVrlyuY0fCzbK6ttlgWTuY0fCwOkLqXnl/LIuY0fC:lu/WWcx/blQ0uANHlZusbku
MD5:	E4DF2B5783FAE6E31F46541DDB420703
SHA1:	38F3513AC35E1D595984BC3EEFC30AB500DBFBED
SHA-256:	D313E7B29F3B264448873EF323BAC34F2034BE5BA1444D77DD85CBB58CD79054
SHA-512:	6EC9D829EF2FAD1909FD95C8EF05938BFF4CE935AAD4B7D4E5E117B9E98C29260DCB114B1CC440D02436B32BBD23732898DA13BD261D62C3797D946D4540930
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...\....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/44/11a/util.js .https://google.com/;l..q./.....{.....j.5{.....a/..r.j..#m.m(F.mk...A..Eo.....%.....A..Eo.....;l..q./.....|.....j.5{.....a/..r.j..#m.m(F.mk...A..Eo.....x.....;l..q./. ...56A61394A16B1988F1C3D9C06419218EE210969E673214D3CD000D2D3F85A12D.j.5{.....a/..r.j..#m.m(F.mk...A..Eo.....6.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\358aba68fb857741_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.455418315124667
Encrypted:	false
SSDEEP:	6:mU5ZVYGLEq6JRMwRFZJRML5jBlgbkaHsHbK6t:pP6JRMkFZJRMNjBlxHN
MD5:	176E598F3C30DF89DA36D0468597ED1E
SHA1:	55FEE535BC8025FB692A3A6D3918C9D835874B12
SHA-256:	2FF9B720B4F423A351498F2CFDF5A81EBDCA69AD7055289F222BFA2AF35CDDDB
SHA-512:	23C9A551391FDB0977404BB808F239268D65B70996134AF987477DB03981E61F6AEE8C973A577D17189A025DE5185EDE5313641B0024465EEC95DECEC48BB0ED
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....._keyhttps://www.scarboroughcovidvaccineclinic.ca/scripts/main.js .https://scarboroughcovidvaccineclinic.ca/...q./.....d.....A.Hp.....CB..m.T...T.. ....'...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6008e5b71f103009_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	646
Entropy (8bit):	5.702330954021626
Encrypted:	false
SSDEEP:	12:0/C5r1BojhBrrED4x22KHlb/WpBYalUgpBlopvlsC/Wpjaldp:N5r1ajhNED4Er6BCAspiI
MD5:	66F46AA8B32169C31CAF18AEF5C33747
SHA1:	B27E2D360C455BDA301E72D22B230CDE5A0A2207
SHA-256:	883D44E6D2F0B206D04BF13D6E384D42011FD746259A4CFE38957C8BD8525519
SHA-512:	87854031B963CF91E979989761A4652989A003F8B658C699EF8CAE4E18D12A538DBD0D0AF7B4ACC4F15B53001A5C41716A663268BA5237FF056565A60643555B
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://maps.googleapis.com/maps/api/js?client=google-maps-embed&paint_origin=&libraries=geometry,search&v=3.exp&language=en&region=c a&callback=onApiLoad .https://google.com/g..q./.....h.....1...K.4O.cPX:.k?.?..d.ty^..P..A..Eo.....".....A..Eo.....q./.....Eh.....1...K.4O.cPX:.k?.?. .d.ty^..P..A..Eo.....2.\.....y..q./.....nh.....1...K.4O.cPX:.k?.?..d.ty^..P..A..Eo.....E.....!..q./.....h.....1...K.4O.cPX:.k?.?..d.ty^..P..A..Eo.....6.w.....)..q./..... .....h.....1...K.4O.cPX:.k?.?..d.ty^..P..A..Eo.....%D54.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8bc35d0ff67b9910_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	258248
Entropy (8bit):	5.8316608561882015
Encrypted:	false
SSDEEP:	3072:iHxvoMx7A1oRJGouJGoPlbQLj8AthtQfMKT:iHxvn7l6m6lbS8lhtvc
MD5:	B10724C1F43A84F10B27480C83F06C56
SHA1:	8BE1EC464E13D968D4A6AA97E86C8883927C2606
SHA-256:	D7F2F4DAA6C03C4F45B5B08D23BA8AA4A9B9396F96779D2E0040E0EB7B93BD3A
SHA-512:	E999E67ECBF336A6CFCB456F781C01E0F304A82953FE58E8573050571529D79DD813FD1293E3BA62D56EA1B027A5554866C745F7362E6120BDB385EC2F7EA77E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...+.6.....56A61394A16B1988F1C3D9C06419218EE210969E673214D3CD000D2D3F85A12D.....'..e....ON.....`^T.....f.,.....4..... .....x.....0.....D...4...$.....$... .....$...D...$...t... ..... ...0... ..... ..... ... ... ...<... ..... .....(...8.....0.....0..... .....(S.H..`H.....L`.....Q.@R.....google....Qb..b.....maps..Qd....._gjsload__...Qb.#8x....util.(S....f.`.....-.L`.....Rcv.....Qb.[e....._.....Qb.....jz....Qb.#3 .....oz....Qb.....uz....Qb..`.....xz....Qb...z....yz....Qbj.....zz....Qb.9B.....Bz....Qb*.uj....Dz....Qb.....Xaa...Qb..*"....Jz....Qb..6.....Zaa...Qb.\.V....$aa...QbF.....Mz....Qb.2 .....Nz....Qb.....Oz....Qb..d.....aba...QbNe.....Pz....Qb.;r.....Rz....QbfD.....Sz....Qb.e.a....Tz....QbjggL....bba...Qb6.....cba...Qb:.7B....gA....Qb.vM.....eba...Qb..]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e18e39732ec3c37_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	559
Entropy (8bit):	5.5786315517063585
Encrypted:	false
SSDEEP:	12:kkUStyf9BlHoRasBiQmlkRaspUlimlfkYRas/FmlDoRasImldoRas:LiDoRaVCRa9dRaXoRavRa
MD5:	3C22213729D33F64D2EA46DCC1F8040D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e18e39732ec3c37_0	
SHA1:	65B09ED69F063506339BCB5AB95345CA272B7493
SHA-256:	31366A6AC0156F86D763B9B84FA0EE130180789A7B3E6A2EEC9F47A4F53D6AD4
SHA-512:	53F361EE94C8BCFB0A2EB6047A0C6C8874E2422DE66DAA716805954EE799AF56CDB6E84F81CE1F9BC50324C6FCF98A3D1B9B9031CAAFE0ED8B79504392ADA4AD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[.....9q...._keyhttps://maps.gstatic.com/maps-api-v3/embed/js/44/11a/init_embed.js .https://google.com/....q./.....Ii.....rN}J.yV>?.w..1n..C..=.....#....A..Eo.....Y.....A..Eo.....q./.....Mi.....rN}J.yV>?.w..1n..C..=.....#....A..Eo.....*.....q./.....Ri.....rN}J.yV>?.w..1n..C..=.....#....A..Eo.....$.X.....q./.....ei.....rN}J.yV>?.w..1n..C..=.....#....A..Eo.....@tP.....q./.....oi.....rN}J.yV>?.w..1n..C..=.....#....A..Eo.....h.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a81ab65c52e7e79e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.6461624253610525
Encrypted:	false
SSDEEP:	6:mrGqltXYGLSmXZCe1a6/ZJRMpxlgHZVTE/Bligk4qDK6t:cHtnL1h/ZJRMflKZVKligkD1
MD5:	2CE0945E3F3D396519518A3AAA670961
SHA1:	AEBAEEE6466543BD8E997848D02F99A6A02C9A44
SHA-256:	9BBB080298807D7FE74EE88A841BBEDED85887659553C1ADF175041BB3045D0D
SHA-512:	0F8699CBBFC4D396A226EF65AFE3F53CE35C25A2610CA3CCD24C08ED800824FEBE4744B40EA22D18588769D4010C3417D4E869C3F306AAEDB7ABF840B15A0E2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g.....U....._keyhttps://www.googletagmanager.com/gtag/js?id=G-PZ7WJMBDD1 .https://scarboroughcovidvaccineclinic.ca/w...q./.....d.....'...=E'..Z?..)I..)..... .....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c0fd8601ed13b370_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	352
Entropy (8bit):	5.9033417410226905
Encrypted:	false
SSDEEP:	6:mmF9YZHfY7cE9uIKlgEZqXauYYK6tIL+c25sVqMBV+vrcXauY0R/:c/Wotl69c7HvQrw
MD5:	0ED9ACD75B5D9D840A45A0A5168D7E3F
SHA1:	13D8DABD0B31BC9B2AB31590D1A67AE0070BBAD3
SHA-256:	34BC15FFFE4DAE2755E9B910EFAF402C333B242E44C95D3AC14DBBBD452843E1
SHA-512:	0CEDF130567F6954B4FAB2C29C296038A54808425957E83F5ABB9A54F97C0498EE9713552F0B156A11B118DCF869F45FBCB6AEF28B0CCE7A647046D9EA870753
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....L...._keyhttps://maps.googleapis.com/maps-api-v3/api/js/44/11a/common.js .https://google.com/.^..q./.....{.....M...`...U..|".x..L.....9".9...A..Eo..... .....A..Eo.....^..q./..M..C1D3D72658F1486DF3515648F6F54A869263DD92C7146E77A435126F9233680B.M....`...U..|".x..L.....9".9...A..Eo.....(..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e48c5ac7e290c9ab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	85664
Entropy (8bit):	5.544243131872929
Encrypted:	false
SSDEEP:	1536:jxTjSchLHhyV2PBjVY5SwVeWzoZeQwEck15caO:jxTjScFBgcNVYSwJQwE2aO
MD5:	B3EC6CA7A633277020E1A27DE3F13D2A
SHA1:	9B16EACF29608B550C645BB676D713F6595EC8FA
SHA-256:	EDE49FF33C0FCD97723D93C99AD626E72509708B20B4E7F348008AA553EA7ADA
SHA-512:	2EAD897F429F7A31A4E6CE887906C6B58D1D93C21D3B392E71A68E41D9DE37A725B36FE7F4EFF474613B73702539EBD3646E04E3A64F8566EF796D5995ACB695
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....).1....C1D3D72658F1486DF3515648F6F54A869263DD92C7146E77A435126F9233680B.....'.%S....O....`M..+.....pE..P.....L..... .....8.....(S.H..`H.....L`.....Q.@R.....google....Qb..b.....maps..Qd.....__gjsload__...QcZ.."....common...(S...qE.`.....Q.L`$.....q.Rc..... ...R.....Qb.[e...._.....Qb>..b....sm....Qb.....rm....Qb..w.....tm....Qb~$.....vm....Qb..c....Dm....Qb...j....Gm....Qb.....Hm....Qb.V2.....Im....Qb".....Km....Qb*K?Y....Rm... .QbjX.Y....Sm....Qb..w_.....$m....Qb./U.....cn....Qb.....gn....Qb..I.....un....Qb^.Z.....wn....Qb&b.....yn....Qbzf.)....Fn....Qb.....Gn....Qb.!Y....Hn....Qbj.....In....Qbj.<,....Ln.. ..Qb.}.....Yn....Qb>..+....bo....Qb.....co....Qb...c....jo....Qb*.Gj....ro....QbR.....qo....Qb.xf.....to....Qb2.7.....vo....Qb.s.....yo....Qbv.@.....Go....Qbn.e)....Mo....Qb.....Qo.. ..Qb.....Ro....Qb.t.....Uo....Qb.z4.....Wo....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.036066230160834
Encrypted:	false
SSDEEP:	6:WAH/jc6+qWvM0Uxkl0hUHb5cnAf/gUZEzQ3zbn3pHkQ+IRwHO:7/Ym4lHunAAzyz7V4hO
MD5:	87837D330C166807EC0335EA379A0C3A
SHA1:	910359EB1EBCF733AA95D36BAB6F4D3CAB0BEC74
SHA-256:	FBA6836AA772F62B5E23C2ECBB9184B96EE098429AEFEDD9500593B7DBBA2890
SHA-512:	36B9BD8C3F74159BB7942B4C04E2EE0AD350661AAD2F2B318833A836E84DD1BBADB8D1C195DE4B0E5DBADA65A78E5A99C0E010702EA2D19A7FAD18796EEC0 1F7
Malicious:	false
Reputation:	low
Preview:	....X.`.oy retne.....Y.....{..]....q./.....&.....q./.....Z.....q./..P.....p.....q./.....7<.2....@...q./.....0.....`@...q./.....R\....Y..q./.....Aw..h..5.Y..q./..... ^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q....._.KPu../.....+<P|...X.KPu../.....q./.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	1.043559920464724
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwcwHCmE/Pu/aA/Lr7XmeveO:TekLLOpEO5J/Kn7UmUPeZV
MD5:	DB4D5C697AB248759490970BFE3E1560
SHA1:	F7061895104F79E7AB6BB2A507B96F1B8E9AE247
SHA-256:	E7D95ECE9056DA19881EB813006AFB9246A127E79137934368831B533099BB9E
SHA-512:	AAA19B5CB47B7735758AFD88D4FCFFAF82F77498901832F3886D53527A1C57A9A22C56508995CBBB8526B2DDC67674EE6C1BFCF4FDF3D33B635E6B0AFFFF809 5
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9689062978006806
Encrypted:	false
SSDEEP:	24:ccLgAZOZD/AEhqLbJLbXaFpEO5bNmISHn06Uwc8:c8NOZ7q5LLOpEO5J/Kn7UX8
MD5:	0827B9AFC5E9CC423884359909AA10AB
SHA1:	5491368537FB9A5324EB3C9850EE4A857AA0C9CF
SHA-256:	EC5249A7753BCDAC812C2951458901187836A220FDB65EB861260EA081D6E511
SHA-512:	763FDD0206A30573295614E7B46E9BB7980BACAF559573CC0CDAC904AA7CEA8D3901AEF3AED72F6853B13EDD9520F12F79662F94A34CE65B5602C1D86BEFE2 A
Malicious:	false
Reputation:	low
Preview:	.....9..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6758
Entropy (8bit):	3.425734463672444
Encrypted:	false
SSDEEP:	48:34GkjxiC4Y5xSUtwDBjGOyuEMbCvxFeUDvkY57qpwDB2bC12iFteUqkY5JCMr7w4:34zEWu1exnMy2iFpm2/Rd5Ix72rSG4n

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
MD5:	8691D695A6D668F725151245B00A91B5
SHA1:	AA9D9D7297E7DAFEA9141526391BBB86A10684DB
SHA-256:	1A8369CB5602AB66DBAF3007EB7795A78A068DC332176000E81EC6E386488272
SHA-512:	F111091DD423F45C58BB07DDAD4D0DD63B7364347791A726905D920E7C5CF4F9DA9F6647263A938EF87F89945805B6A4C289E01AE33CBBA24D9BE5550767CEF
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...b01a1ad0_fe0d_4113_8308_1ebdb812e79f.....+@..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....-...https://www.scarboroughcovidvaccineclinic.ca/...# ...S.c.a.r.b.o.r.o.u.g.h. .C.O.V.I.D.-.1.9. .V.a.c.c.i.n.e. .C.l.i.n.i.c.....h.....`.....}.....}..... ..... ...b...-...h.t.t.p.s.:././.w.w.w...s.c.a.r.b.o.r.o.u.g.h.c.o.v.i.d.v.a.c.c.i.n.e.c.l.i.n.i.c...c.a./.....8.....0.....8..... ..... .....0.....(.....@.....h.....h.....`.....X.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.2552454936431205
Encrypted:	false
SSDEEP:	6:mRo19XvVOq2PWXp+N23iKKdK8aPrqIFUtp0o19VZmwP0o190ZkwOWXp+N23iKKdr:xhAva5KkL3FUtphz/Ph+Z5f5KkQJ
MD5:	36C653C854E1A926BB1DA8F3CD56419A
SHA1:	A1E5DB147A058104A67F53EE1EE2087845353078
SHA-256:	58ABE70AB81ED6B2F9A9DFBDAFDC4688CD2ECE5AB397C1BDE2C0F3C06A5874E6
SHA-512:	C3847C7F2AD86D41887541EFCF502A16B13EE2969F2EC7FAE558CDDC1EEEF4321DA58178362474E46F64F0F4E12D10AC3228BEF07362C05714BA41BEB9C6374
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:56:49.179 5d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/04/26-00:56:49.180 5d0 Recovering log #3.2021/04/26-00:56:49.181 5d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.244059633262395
Encrypted:	false
SSDEEP:	6:mRo1GBYyq2PWXp+N23iKKdK8NIFUtp0o1G011ZmwP0o1G0jRkwOWXp+N23iKKdK2:xGBYyva5KkpFUtphG0X/PhG0jR5f5Kk2
MD5:	382E1595690B3F64D3DE8C54A158DD4C
SHA1:	9D5C1CCA3BD8075E1C4BB207C5AC140B8020BF7A
SHA-256:	AB7C5504AB3B9E6F4C95487AAE1A90ECF47083CAE3729F44D3E59CAC317BFDA5
SHA-512:	31EF0FD585EAA98690283C15221405F8B6514CFC491C64A4A378EAE75FAB703A25F3C0E33DE06DC4026A69D1A6BE7D62BA09D882A73B809E021702F1DFAEAA0 8
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:56:51.287 16a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/04/26-0 0:56:51.289 16a4 Recovering log #3.2021/04/26-00:56:51.289 16a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclJ5 n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	18432
Entropy (8bit):	2.7991375194650736
Encrypted:	false
SSDEEP:	96:zBCAmVH6awebDdeKp3L62ezkY43mcDgN8XN+9C:VrmqebDd/ZL62+imcDy9A
MD5:	76E4A85D8D60D619EA24A79D2245A0D7
SHA1:	33353CD98031226B042B049D2994F6B25C02E86A
SHA-256:	B18B5FF4A83945E158BD4BE0AA790382F2816B9CB0F841C86F7DB71FE34E2B85
SHA-512:	9DE2B635DC3F9D7FD5CE3D97302CF15685BA5705513AA837277E807957CB505EE2FB93C0B56BF0B1440A59C81B2A8A7FB2C5CD1921EA58F4F2B925F5A326AEFA
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7757605094790907
Encrypted:	false
SSDEEP:	24:yuAyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwlF3n:YdBmw6fU8F3n
MD5:	88558C964CBE548319D8336BAF53BE30
SHA1:	77C583F959BEEFF46D6B0D11F64FA4FBB0733122
SHA-256:	D93830937E60E41DD6F34F30EACDB149FD4D5962A8F18171F114B80E064B8D43
SHA-512:	61A360802294E4294691612F8D02C6BC4AE2F2505ADC9486C83718BF6B0533C1E057C82648B7BA5EEE14F9BB5E6ABE81EC06F281351CB91167BA266C6D01F352
Malicious:	false
Reputation:	low
Preview:	.....Xo..... ....

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):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.291068343062367
Encrypted:	false
SSDEEP:	6:mRo1/VTLsUf+q2PWXp+N23iKKdK25+Xqx8chI+IFUtp0o1/VTLDZZmwP0o1/VTLu:xRl+va5KkTXfchI3FUtphRPZ/PhRhV5M
MD5:	68F10D16F6DE4AFBBED73300603A8673
SHA1:	2C7246F880432843DD16C4AC57CA7B4EE3E9F711
SHA-256:	DC67A48AE1AB9AFA6F7847D5E73F57C7D50A5F1CCA06344550CF7DC65DAAC092
SHA-512:	15DCD65F88482DB42C720DE3B0D5DC11E7507BA9BAB4F53C26E1183114653113B28F6C2538478D608A744ABC5917D0DAEEC18EC02E0F51CDF28E8385F77C2D D
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:06.283 147c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/04/26-00:57:06.290 147c Recovering log #3.2021/04/26-00:57:06.294 147c 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\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.219406212586614
Encrypted:	false
SSDEEP:	6:mRo1/VTLnK+q2PWXp+N23iKKdK25+XuoIFUtp0o1/VTLbaZZmwP0o1/VTLLVkwOG:xRO+va5KkTXYFUtphR+/PhRnV5f5KkTZ
MD5:	B1A830EA930C8DA1AE2CF8B3C6DE75F5
SHA1:	3508C6B36B4AD8FCD2A46D1D151BD572B558A71C
SHA-256:	EF969A666816E517CD35D217D5C4D5D1DAF4B39263619C56C13B0A787B5B5E0F
SHA-512:	4B43C0B0775466F665AAD756B0FC6CD2CD1A69B441DA07B39E8923383CA3FBA6F450911458E701B3A43C318DCB4698729D6E27FE5E134C1C07A0ED51F58D737
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:06.211 147c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/04/26-00:57:06.215 147c Recovering log #3.2021/04/26-00:57:06.216 147c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.245209023054356
Encrypted:	false
SSDEEP:	6:mRo1/VTLMjUf+q2PWXp+N23iKKdKWT5g1IdqIFUtp0o1/VTLYZmwP0o1/VTLOmFd:xRsUf+va5Kkg5gSRFUtphRc/PhRSyNVx
MD5:	196D51A614BAE568099ECAC7FA48E283
SHA1:	243A708B6D98CF53C8075C75790D606FE1793902
SHA-256:	EA6EC9A614AAF9B384B26357488A76FCBD1B22E7AA326A5806C0420C3CCE0947
SHA-512:	E642B7C7A6226BFBB36ED25FE0A8AB20E9718B83C26942C8E6D528F7C041655BDEE00A082C1AC7D4DF4CC25ED497024E1AC655A4DC4B11C8FE0A66139A7D9 A3
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:06.104 147c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/04/26-00:57:06.118 147c Recovering log #3.2021/04/26-00:57:06.120 147c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.1900337485902151
Encrypted:	false
SSDEEP:	12:TL+A/nEZJRMb+Zcd14XEZAtf26JRMb+Zcd14XEZEQJRfn2SsBRs2V+Re6JRMlKZa:TLxEH0ldw0laE92vAjoyI
MD5:	ECF556BDEEF381A08DE0AD5DC03F2F0C
SHA1:	B477937BC46A6192FFD338DA873BE37440E94155
SHA-256:	844AD8483A88C6DBC1FC9ED14B6F49E07FA31A56CE3E21AA7001EF60167AAFF8
SHA-512:	FFE9E52010665974961E22F3B5A93AB6F8179A79FF9608BFB6A33FA75DE59FD5DB6A93F4EA66A572C9E688A705FA86DA935DE0B4A61925D286A179F675E90089
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

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):	845
Entropy (8bit):	5.453039841132112
Encrypted:	false
SSDEEP:	24:7NQlEULnybrWKYyfDKDHR3gAE2dR1yJMY4K9Wj65:7NZMybrlzfDKDRwAxd2B9S65
MD5:	D965AA4118165F3E821D5CDCFAFCADB2
SHA1:	FCEE9E1BAD1904F4716D98C7E795F9B8B358D619
SHA-256:	69B372CA778C2B7CD97F2C5BBB7D921C520A6E2F245DFCCF24086729F5A83E04
SHA-512:	58DDBAAEEC952E448846605EBDF3CCBA03976A5D4BD1EBF6F36E1A691FFCBE678CF27539F5EDA708652969E92ADF0F15F5893578BE6A7AEC9B9D0E86A38A73FF
Malicious:	false
Reputation:	low
Preview:	....."`....19..ca..clinic..covid..http..scarborough..scarboroughcovidvaccineclinic..vaccine..https..www*.....19.....ca.....clinic.....covid.....http.....https.....scarborough...!..scarboroughcovidvaccineclinic.....vaccine.....www..2.....1.....9.....a.....b.....c.....d.....e.....g.....h.....i.....l.....n.....o.....p.....r.....s.....t.....u.....v.....w...:c.....B.....o..... .....*(http://scarboroughcovidvaccineclinic.ca/2#Scarborough COVID-19 Vaccine Clinic:.....y..... .....*-https://www.scarboroughcovidvaccineclinic.ca/2#Scarborough COVID-19 Vaccine Clinic:.....J#.....%.....*.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33356
Entropy (8bit):	0.04761656801783403
Encrypted:	false
SSDEEP:	6:M0x74kDt81vSli3vS5LJvg9bNFlWCj/l5E/l3n:M0xHDS1vSliq5LpqLBj/e3n
MD5:	87BE5DD0EC39FA090D72490ADEDC8A06
SHA1:	F5732CA836284C667977F61213E87FA3D739B3E0
SHA-256:	CE0D73EA8C77BD1677BB379D8618D993087CC664E1712A86092EE62F3E4A0176
SHA-512:	831F49B154D380B1D9DD7B5C0519BC785917C5DB849797F4E5A89E3CAE4C2D3FFAC9F8A2DE5555C7E71FF48F1525F7A52657129D960D3DBEC71C0D2274CC50
Malicious:	false
Reputation:	low
Preview:	.....w..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.473290129923746
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
SSDEEP:	48:NY5sGD+X00Ina7VnMxq8dbJ5BIRIJGbQSefgGXNrS0U9RdiN9gk:N6DO9Ina7VnMxpdbJ5BIRIJGbQ5fgGdx
MD5:	F0B21CD209A7CF9CE2AE2B16B99716EA
SHA1:	2A64398C618CE671722DE61FFE957ED068167BA0
SHA-256:	F39EEB06B159986D518635BB2541F3707CF5D1C7B0FA3C2BB63ED7E27986BD7A
SHA-512:	6DADBFDE06C14DB8B35049EA0BF00749CBDDB1D576D068EB506A6A630FC4A0048B9D1838D0874019E8B1D8BFD2E6D8AF916F8D848EC19341F20632B481C8AAFF
Malicious:	false
Reputation:	low
Preview:	.(....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..498166000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-04-26 00:57:07.37][INFO][mr.Init] MR instance ID: f7261b0b-0cd7-4294-8a30-236a4dbab8eb\n","[2021-04-26 00:57:07.37][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-04-26 00:57:07.37][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-04-26 00:57:07.37][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-04-26 00:57:07.37][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-04-26 00:57:07.37][INFO][mr.CastProvider] Query enabled: true\n","[2021-04-26 00:57:07.37][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.24593593442353
Encrypted:	false
SSDEEP:	6:mRo1X0pQL+q2PWXp+N23iKKdK8a2jMGIFUtp0o1XgWGKWZmwP0o1XoQLVkwOWXp+:xXaQ+va5Kk8EFUtphXgWGKW/PhXoQV50
MD5:	A94374D42F747D8F192EFF96AA427CAF
SHA1:	F86C6E91C9118B924DC4E6F85E368C953AE6D871
SHA-256:	EA8DE1A910E33CBF5D3921A596053C759C45870D2A0B3DF813F13FEE3DC66E65
SHA-512:	64A5DA81E57C2BA6A1EEE98DD7F4084FF6DD052E6D40CAF0BB8DA96DA80F1307DC4A1ACA5FCC7E08779A1EE97CF11EC37BC17E5D4F1A40576DB761AFB8CBEEA99
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:56:48.975 15ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/04/26-00:56:48.976 15ec Recovering log #3.2021/04/26-00:56:48.977 15ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.243394582438435
Encrypted:	false
SSDEEP:	6:mRo193q2PWXp+N23iKKdKgXz4rRIFUtp0o19TXZmwP0o19skwOWXp+N23iKKdKgi:xRva5KkgXiuFUtph1X/Phm5f5KkgX2J
MD5:	8CAE0826262DA9E8A168C149BF98E6B5
SHA1:	140CDAEA231A7AB48CBC4F59FE6A4DED1E64C3B7
SHA-256:	2B0AE9802BAA73B741B26F65848978AE5A0D1682802525D854C6001C38BBBD9B
SHA-512:	DAE0FEFDA9D3BDB35B8F70CE6088A9219C9296D6154EACE487569B791379034600C476A97431238ECF287FE1109BDD1C43ED27E7CB4C32B867D6C89B1BE970A
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:56:49.213 1480 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/04/26-00:56:49.214 1480 Recovering log #3.2021/04/26-00:56:49.215 1480 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	1.0110860993942918
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoR:wIElwQF8mpcSJ2Yx1
MD5:	615C42B2D540F24B5886CAF6ADC0200F
SHA1:	77EA40D9E3CB923DA423F27ABC51A9F6C063F7F7
SHA-256:	4908CC0A570FE2D753A5C69A2822BB77596726E35EE064B0FB88305D9EF8B516
SHA-512:	0D819A78357C0DF71F0965222F24D4A26BF8E15ADE2AF14906FA6B0BC60F05C3A48069430AB97C86A2BC85E192AB74F4AD5046FB2A1073606F27C593DBB9EFA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8242942229416002
Encrypted:	false
SSDEEP:	48:ShWqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUa6:SIhIElwQF8mpcSz
MD5:	02960B71CA5633FB945F4535C2BCAF2E
SHA1:	AAE99C0696922C5BDA51DFF13207B03E6BB76FF2
SHA-256:	984B5A9ACB4609B4EA9EFD68557EC21922322D2AF8707135967CD9F1404D4E55
SHA-512:	AE1B53417F7825FA8E845BFB0870467210FCAA8EF2D95ACE37325F966A1121A4A6071833615890AE0FBE2EF2F885458F8D2A8FCBB5583BF17B42E7D68A6AF36A
Malicious:	false
Reputation:	low
Preview:	.....n.g.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	222
Entropy (8bit):	4.177745475505683
Encrypted:	false
SSDEEP:	3:5lmh9tdllajEGfdPe1U6SLICADlL1FUL1FUL1FUL1FUL1:5lmfla4gsMLICA5EEEE
MD5:	B131A89D327B232D9F14D95A8B316BBC
SHA1:	EEB1C8B1FEB3A63D79FA5DC0B0F110FD98A3BD4F
SHA-256:	939A2122DFD6F4B0BE2A0068D986301221471C225BC37465541CF6D4AC178D16
SHA-512:	0CA2EF222EAB8494788B76960FFD74EE151257A5D04DF59616F1266A68E217ACE220143FB8075B02E8EDEC8845FA3A61F2CC6A22FB2079BA4076D5AE677E14F
Malicious:	false
Reputation:	low
Preview:	..&f.....7..Oe.....next-map-id.1.Fnamespace-b01a1ad0_fe0d_4113_8308_1ebdb812e79f-https://www.google.com/.0V.e.....V.e.....V.e..... ....V.e.....V.e.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.184843808712214
Encrypted:	false
SSDEEP:	6:mRo19zq2PWXp+N23iKKdKrQMxIFUtp0o19TEXZmwP0o19TFFkwOWXp+N23iKKdKf:xtva5KkCFUtphe/PhF5f5KktJ
MD5:	C48C8164AF172D3A0B144F7B6A89D7A1
SHA1:	34B74BE11D933E426E9DD0378A6830A7C2AD5CBF
SHA-256:	AAD217AE257C6B4C297B6EEEF170D45C3DFCB1B37B652D85B8B44849C25F797C
SHA-512:	5A7E42D675D6C738549088882AFB675A1FBB33B752A439C47A14251866C801E97BA30184D6A04D9E44FA09E72525FA02F5D1FF9A2BA3F58FAB4A8916498A4CD7
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:56:49.129 5d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/04/26-00 :56:49.130 5d0 Recovering log #3.2021/04/26-00:56:49.131 5d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.210289954070846
Encrypted:	false
SSDEEP:	6:mRo1XX0MQQ+q2PWXp+N23iKKdK7Uh2ghZIFUtp0o1XSFUgZmwP0o1XSFUQVkwOWA:xXX0Vva5KkIhHh2FUtphX2Ug/PhX2UIK
MD5:	ED416C921C66F240A666CEF0489893AA
SHA1:	DF40CBB33C292C9D31D16070B306629C74580671
SHA-256:	DC7F1B9B2888AA201E7C986AD6EEE00180CC664CF75AD47CAE8D212FA8F5A232
SHA-512:	AD59CA5F4FF97DD3DCE276192157343ABDD810CA8824BF3323C655F9BEBD546CC234AF2BC5B16CFED83CF558274F2E3E9E318873E26AE636F026A4EC3230624
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:56:48.928 1298 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/04/26-00:56:48.930 1298 Recovering log #3.2021/04/26-00:56:48.930 1298 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.283828758409286
Encrypted:	false
SSDEEP:	6:mRo19jOq2PWXp+N23iKKdKusNpV/2jMGIFUtp0o19lZmwP0o193kwOWXp+N23iK4:x8va5KkFFUtphL/PhB5f5KkOJ
MD5:	C48995D8555FF30495201AB6C7E34238
SHA1:	394E7CB1B06940DC6BF30A86ED11DE7BCE0A453A
SHA-256:	296E9E14F8D334D5EEE766EB77616ECA7F25C6BEA48594D6D442FDECE32F80BF
SHA-512:	1EB92B24F7903B2FF77FBCF92C97831E07AA605728CF1986D78A70A83D0EA862E7B4E968B504FEF6EDDBD7965C061CEFDD3026019C6814AA07E64926451FD1B
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:56:49.184 1480 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/04/26-00:56:49.186 1480 Recovering log #3.2021/04/26-00:56:49.186 1480 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.267591009415786
Encrypted:	false
SSDEEP:	6:mRo19NEIq2PWXp+N23iKKdKusNpqz4rRIFUtp0o19nQDZmwP0o19nQZkwOWXp+NK:xlva5KkmiuFUtphFY/PhFA5f5Kkm2J
MD5:	5A47A67ABD5A13659F73CEEABE663255
SHA1:	48D36A0D20A5FE8B87AFF2A3394CA36CC2BCB694
SHA-256:	ED316AB15C4030601A97BE3A33EF22F12FACDC05B628E8D38534B2C4A2FBF379
SHA-512:	E603B8FFDF2ACBED349BF00D442A5B78DD509E17E958B6D0E4347076B22510CB32CD5116410DC3B5F967E828C59F71C7757025DA03D20D5BB272D42BF8D7EEF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:56:49.204 5d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/04/26-00:56:49.206 5d0 Recovering log #3.2021/04/26-00:56:49.206 5d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.304649385798882
Encrypted:	false
SSDEEP:	6:mRo1/V2dSVq2PWXp+N23iKKdKusNpZQMxIFUtp0o1/VVSgZmwP0o1/Vu0IkwOWXJ:xYdOva5KkMFUtphrX/Ph05f5KkTJ
MD5:	E428050880E59E5E2607D054213E86A3
SHA1:	30DD83B288F2AD4207531C6A1B490B036CA62E2D
SHA-256:	C4E86BF04EE049C859EB350EF9EEC2EBC7160A56EDD32434978CE64DCCD1CCA0
SHA-512:	A50DD72750DB02FC11672EDBD3BC0A24927B433126BC718191C5F5E69D96CD96A6596C52B9E31CE972097725E48495E32659D7B124DB5F3CA7E93561CC284C0
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:05.396 664 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/04/26-00:57:05.397 664 Recovering log #3.2021/04/26-00:57:05.398 664 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\a0215c8c-894c-46e2-81b5-352f9c6c84ba.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.195297300864171
Encrypted:	false
SSDEEP:	12:xRytyva5KkkGHArBFUtphRyJf9/PhRyJfpR5f5KkkGHAryJ:xRyia5KkkGgPgLRypRyff5KkkGga
MD5:	DEDE9431FF9C04160527EB1D14EF4D0C
SHA1:	4BB3A7BEB3B13191DD73CAA9AD31F59C702AE81B
SHA-256:	D7D88CDA5B9A62CAE75D9147B1B9E60BECCC5A6B4836CFF218286B4A51B1B485
SHA-512:	06AC1448FE2723AA2A7FA3F60A0AAE9444F9F1D17DEA8AFED752C0926E48432512B02375D29D2AF56A337B51D128EDA7CF9CF2045E569454D13A5E69F358EB6D
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:06.344 16a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/04/26-00:57:06.346 16a4 Recovering log #3.2021/04/26-00:57:06.346 16a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.269144705832796
Encrypted:	false
SSDEEP:	12:xRzva5KkkGHArqiuFUtphRxT/PhR25f5KkkGHArq2J:xRTa5KkkGgCgLRxFRgf5KkkGg7
MD5:	767518F01680A48A7618A09925D08206
SHA1:	E0FEB559D16F05E8FB9BECF2561EF77CC9895E72
SHA-256:	8155743D61DBCBD114C07084B411AFAB2F55E978CA0A272E5DCEEB478DF34E85
SHA-512:	21F854BEB81EBD480CA971A9F5B32510F8B541A0B6115664E69ED143A34909DA09132F4236319B390DBD3707466983000F6B7C040EBC2B092994F794DC31CC34
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:06.355 1438 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/04/26-00:57:06.358 1438 Recovering log #3.2021/04/26-00:57:06.359 1438 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.217756572694061
Encrypted:	false
SSDEEP:	12:xfTyva5KkkGHArAFUtphfn/PhfqR5f5KkkGHArfJ:x0a5KkkGgkgL5Af5KkkGgV
MD5:	F035686EB2D8C597BF8E4A5A9B3E8475
SHA1:	7D3AAA2847741B5FCFBC252B010AA7782A15C19B
SHA-256:	28A8750861BA96930D4FD816AAAF30EF192F4D6B993F37E6B8E1F08BA093AFF3
SHA-512:	F8766F86DD2DE7D1DA5AA35F2AAAB3291C11200244B03F3DA368AE195822F95C629CAC59B03A16DFE9FA5565F1637BB1B39879AFF520A469EE4E579B8ADA773B
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:21.683 16a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/04/26-00:57:21.683 16a4 Recovering log #3.2021/04/26-00:57:21.684 16a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\ca62a7f1-7a9c-4484-92e9-95f305ee5dd4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.290997335507955
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
SSDEEP:	6:mRo1XUFUQ+q2PWXp+N23iKKdKpIFUtp0o1XnSgZmwP0o1XROdSQVkwOWXp+N23iQ:xXUWVva5KkmFUtphXSg/PhX4dSI5f5Ka
MD5:	A62177B7DB75A913F0D0C556B65C14EF
SHA1:	A0259393D6614C8C336B465C5FBC1A76A4AC059E
SHA-256:	16BA268941864DAB7E83189A2AD70DBD9D96878B77A8DBF003393173BF111391
SHA-512:	775F352870E00F39E881C4330975EE3AC1BE47DBB6376413739A31A3238D39B3E735FFE7B09AE50410576A7F1F60E507AD082AA857FF99F952F47E2BF8FDE3E5
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:56:48.936 1298 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/04/26-00:56:48.939 1298 Recovering log #3.2021/04/26-00:56:48.941 1298 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.360339259107006
Encrypted:	false
SSDEEP:	6:mRo1/VSk+q2PWXp+N23iKKdKks8Y5JKKhdIFUtp0o1/VlqZmwP0o1/VlGVkwOWXj:xAva5KkkOrsFUtphC/Phu5f5KkkOrzJ
MD5:	D2EE0A1962D2A79FDFFAE3CF1178E0ED
SHA1:	57D0697B7C2326E1C92F7DF87E66B57F3FA876B6
SHA-256:	ADF74B21938CD5F1EC3DF455D381510F7B1A71C691908959F079BDC036278B4C
SHA-512:	5A2B3A6DD0914B86AA4A3DD93883F6C61AE6302923E44E1819E888F5E09F9E03C6370E25CB6D8CE4A5D8BC4D5697FC5730D731E90C35E90A6A2DA6A2582F817D
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:07.380 1438 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/04/26-00:57:07.381 1438 Recovering log #3.2021/04/26-00:57:07.381 1438 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	3.9387218755408684
Encrypted:	false
SSDEEP:	3:UN/YUs9mdA:UQ1
MD5:	FCDF633FB2F561EF5C5D9E01A82E30CD
SHA1:	E74F495E84D4F5AD63F9AF3ECF93BF7813CD82D6
SHA-256:	DE392ADAC08CACE4CA385F6BF11B67CBBF26BF864F3B7C766EDD73D9E59B00F8
SHA-512:	364C333451623D56E45D62C4CC8BE9BD946680CAC2403AF33AFE03D1066CF0A3C9C1462566F885B70D88F8679ABBA9971F87C577AF2A685363E8C34230B6F72A
Malicious:	false
Reputation:	low
Preview:	.....h.}.IX.....z...@2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d8cf2033-ee1e-4c30-a219-264e6d3e5124.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d8cf2033-ee1e-4c30-a219-264e6d3e5124.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.541909803629454
Encrypted:	false
SSDEEP:	3:tUKODo1/VQtOZmwv3sDo1/VQVl0V8ssDo1/VQVl0WGv:mRo1/VlZmwP0o1/VemVv0o1/Vemtv
MD5:	C26BF0EF59A5F80A8125C5F6B05EC475
SHA1:	E3E291540A9D7E07B38A2731CD1948C095D5090C
SHA-256:	ACC82CEF5C2BDC4F3650E1BF4D18C0E1C9AFC786E37B796DC2B1084C5D6855F7
SHA-512:	391AC07822B1190A43BC4C7F2783A28B324B15DF4573BF64B06FBDDE75E77DFB4508472C11F7096ADE0DF13EEFD9DCAE1023F929EABCDA91A31C6F18C2A870C2
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:05.518 147c Recovering log #3.2021/04/26-00:57:05.781 147c Delete type=0 #3.2021/04/26-00:57:05.781 147c Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e900ae8d-479f-4649-8949-2ccb46fa3efd.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):	22596
Entropy (8bit):	5.535807281771452

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e900ae8d-479f-4649-8949-2ccb46fa3efd.tmp	
Encrypted:	false
SSDEEP:	384:ifPyt1LlY1XD1kXqKf/pUZNCgVLH2HfDbrUQHG4nT3pA1d47:CiLlsD1kXqKf/pUZNCgVLH2HfXrUUG4H
MD5:	5B072680032D2CB13FFB6914FCF7D3F1
SHA1:	D00229E2BE6B094ACF7388199F009EBF2BA12B79
SHA-256:	4ED7D277CF17973009D110A636A9A2207FEBC5AD1309FE8D0E5E2F51A5963698
SHA-512:	C1FBE7B3EE47BB209A5E3BAD8FEFE950E0D30D343BC0442A6F1FE510F2BA4E0D92698A5B66C4EE3EC4E879614F03242806DCFC14CE99C4521974B7909F786C8
Malicious:	false
Reputation:	low
Preview:	{"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":"13263897408943406","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.208081222548428
Encrypted:	false
SSDEEP:	6:mRo1/VTLEWuMVq2PWXp+N23iKKdKfrzAdIFUtp0o1/VTLEo5SgZmwP0o1/VTLEQx:xR71Vva5Kk9FUtphRN5Sg/PhR/I5f5KF
MD5:	F669E368307D024E0AD07667A65FE198
SHA1:	60349CD2F538A3407C961A7BFB5AE82E1A4FD766
SHA-256:	D147F035575B050A971CC59A32B8E2E288724DA07C39C237E236BC3215589603
SHA-512:	1653795FB993A6DDDA3A220E46EDFBE204E6202835CBC66528E3341169BFA59DC176A95B095A1BE84D8B3AEFDA14BB7106A5AF6499F3E2791A60B788C6FA427A
Malicious:	false
Reputation:	low
Preview:	2021/04/26-00:57:06.543 1664 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/04/26-00:57:06.544 1664 Recovering log #3.2021/04/26-00:57:06.545 1664 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

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:tbdlrnQxZaHlGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\a34e2ea5-83b0-4bb3-bbc0-f0612741e2c3.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):	165275
Entropy (8bit):	6.0818027908876475
Encrypted:	false
SSDEEP:	3072:x1aw3DX4JNwA3Im6Xo7W1Vu/srl8CUFcbXafIB0u1GOJmA3iuR2:X3kZ3WXC1kuCSaqfIlUOoSiuR2
MD5:	B30D3A3583B6E02C07B4595E67A8F11B
SHA1:	1718BBE8CB2DD17F323C639056ACC63B4FC65D70
SHA-256:	23C1367B3433F809AB5DA8CDA1631EF973EE6D8E8B277FC46065A71082B0AE7E
SHA-512:	2678D04BC6FEBC14BC9630F8F04B2B3D44CCD06095ED39DAA1760255B8AC2AD7B11C9E13DBD9BAF363972F5505D42BC2C603E99DA3C5B289D2BE0AB62303CBF
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":1.619423811842867e+12,"network":1.619391413e+12,"ticks":90826301.0,"uncertainty":4452570.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\e7a04550-726a-454e-a042-a5c47a7cf04b.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):	165275
Entropy (8bit):	6.081802850049132
Encrypted:	false
SSDEEP:	3072:xQRw3DX4JNwA3Im6Xo7W1Vu/srl8CUFcbXafIB0u1GOJmA3iuR2:2ukZ3WXC1kuCSaqfIlUOoSiuR2
MD5:	8D3755A71AD3F1E8CF35BA2AEDC71CFC
SHA1:	0B67CB471505C9D0BECAD41FFCB103E0B6ABC4D8
SHA-256:	089F96BF852FB1629F2F92E4D7B7702469ED481934B03F0D2D53E780DACEB4CA
SHA-512:	015739DB755FD9012E1C18721FAA8CF75DADBD15EFBC16D1FDD62E46E593912C418634B37965F6AED13E585493FEFE4E89A0FF00C5DCCF3C92D15F28D7F8026
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":1.619423811842867e+12,"network":1.619391413e+12,"ticks":90826301.0,"uncertainty":4452570.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\faca1b08-1666-4336-adab-223b99855fef.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	modified
Size (bytes):	94708
Entropy (8bit):	3.7469046416194325
Encrypted:	false
SSDEEP:	384:RnZGuwTZUjMCVrtS1NOrrviq3h6kZH0hGVcrH0ilxJUIcbrDym/kHk2G6FO8YWNX:pemBpCUFNwenEuwY/3WqKc6Gxr
MD5:	37BCBC403A24C1081725A45ADD674F3B
SHA1:	7C4559A71B618A77B37D7C04E8177FAB9A6FCA6C
SHA-256:	3AE8BC44D712E0980D3AC24690A6FE9AC8A1E3A7DFA21CE8153AEE125F520723
SHA-512:	2D0C1E5094C0F3F7D5F42833E89DA91D4810DE3E6547B177C7B39FCA053403ADFF07D388AE21123C59C621A2BCFAC650B4A4641E48D83E991FB114F5CAD59C1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\faca1b08-1666-4336-adab-223b99855fef.tmp	
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...?88.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\0329aef2-f641-44b8-98ca-4bfb376b7935.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..& ..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,.. .W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6.. @?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\11578fb4-f5ca-46d1-96e4-4be513c96b9f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./ ?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q...:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\7dd70858-2df7-4d74-a389-74eac1cdfe3c.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\b8adec44-fb4f-412b-9fb9-1ea414bbda13.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\11578fb4-f5ca-46d1-96e4-4be513c96b9f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0.."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0IprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\ar\messages.json	
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:IPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\ca\messages.json	
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7ADB
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "1522140683318860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\de\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "......... ....".. },.. "1428448869078126731": {.. "message": "......... ......".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "........ .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0blt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71E EEE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\es\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas describe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB1120272356
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "1522140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... .... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A526195205021
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\fi\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "152214068331886 0351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "180276746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C00 0
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "128276876460319075": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-s mooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smoot h".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51 B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Se fige".. },.. "1213957982723875920": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "1428448869078126731": {.. "message": "Fluidit. de la vid.o".. },.. "1522140683318860351": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "1550904064710828958": {.. "message": "Fluide".. },.. "163 6686747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\gu\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "....".. },.. "16366867476874963 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": ".....".. },.. "18503975003120203 88": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

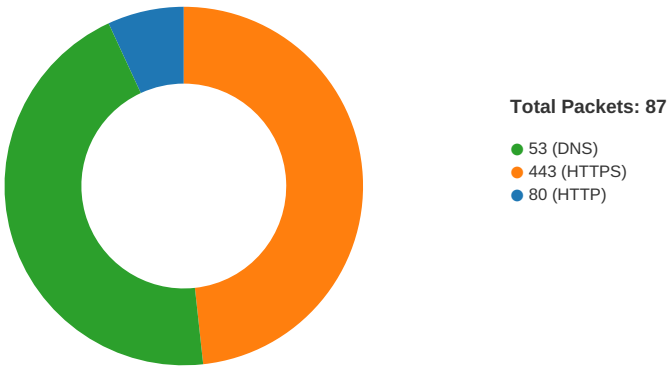
C:\Users\user\AppData\Local\Temp\scoped_dir5444_1061496856\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "..... ... .?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874963 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": ".....".. },.. "18503975003120203 88": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 00:56:51.821715117 CEST	49716	80	192.168.2.3	65.9.66.41
Apr 26, 2021 00:56:51.823066950 CEST	49717	80	192.168.2.3	65.9.66.41
Apr 26, 2021 00:56:51.859457970 CEST	80	49716	65.9.66.41	192.168.2.3
Apr 26, 2021 00:56:51.859570980 CEST	49716	80	192.168.2.3	65.9.66.41
Apr 26, 2021 00:56:51.860018969 CEST	49716	80	192.168.2.3	65.9.66.41

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 00:56:51.860817909 CEST	80	49717	65.9.66.41	192.168.2.3
Apr 26, 2021 00:56:51.860902071 CEST	49717	80	192.168.2.3	65.9.66.41
Apr 26, 2021 00:56:51.897841930 CEST	80	49716	65.9.66.41	192.168.2.3
Apr 26, 2021 00:56:51.901267052 CEST	80	49716	65.9.66.41	192.168.2.3
Apr 26, 2021 00:56:51.941425085 CEST	49716	80	192.168.2.3	65.9.66.41
Apr 26, 2021 00:56:52.192244053 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.232897043 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.232997894 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.242814064 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.280505896 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.283310890 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.283363104 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.283406019 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.283431053 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.286401033 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.286429882 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.286478043 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.318577051 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.318701029 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.318867922 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.356695890 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.356731892 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.356760979 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.356996059 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.357342005 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.360367060 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.360419989 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.360435963 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.360471964 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.360480070 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.360517979 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.360532045 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.360578060 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.361457109 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.361502886 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.361535072 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.361557961 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.362449884 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.362492085 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.362519979 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.362550974 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.363501072 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.363557100 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.363586903 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.363614082 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.364558935 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.364609957 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.364669085 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.364732981 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.365628958 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.365668058 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.365740061 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.365787029 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.366679907 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.366722107 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.366800070 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.366868019 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.367722988 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.367762089 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.367818117 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.367888927 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.368774891 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.368817091 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.368894100 CEST	49720	443	192.168.2.3	65.9.66.114

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 00:56:52.368968010 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.369847059 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.369889021 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.369955063 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.370009899 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.370902061 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.370960951 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.371022940 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.371105909 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.371949911 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.371990919 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.372061968 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.372117043 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.372999907 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.373048067 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.373101950 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.373151064 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.374053955 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.374177933 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.396727085 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.396800995 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.399980068 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.400027990 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.400091887 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.400449038 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.400496960 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.400553942 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.401546955 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.401587009 CEST	443	49720	65.9.66.114	192.168.2.3
Apr 26, 2021 00:56:52.401650906 CEST	49720	443	192.168.2.3	65.9.66.114
Apr 26, 2021 00:56:52.402616978 CEST	443	49720	65.9.66.114	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 00:56:42.378541946 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:42.435700893 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:42.951714039 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:43.006181002 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:44.094038963 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:44.140069962 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:44.839948893 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:44.887399912 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:45.673944950 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:45.736727953 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:46.788674116 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:46.834717035 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:47.904578924 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:47.963021994 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:50.152734995 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:50.198626995 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:51.406575918 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:51.464759111 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:51.652566910 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:51.655770063 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:51.658668041 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:51.659461021 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:51.717891932 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:51.718089104 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:51.730014086 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:51.819614887 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:52.021255016 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:52.113162994 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:52.177898884 CEST	53	57084	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 26, 2021 00:56:52.191471100 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:52.275911093 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:52.337903976 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:52.451030016 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:52.496711969 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:52.739840984 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:52.785631895 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:52.922851086 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:52.974545002 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:53.014023066 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:53.065722942 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:53.261070967 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:53.336536884 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:53.622997999 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:53.640908003 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:53.684643984 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:53.705686092 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:54.157033920 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:54.211163044 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:55.254511118 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:55.309092045 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:55.868525982 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:55.917119980 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 26, 2021 00:56:56.952233076 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:56:56.998313904 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:06.309573889 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:06.375871897 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:07.640722990 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:07.704674959 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:08.843451977 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:08.906390905 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:15.725248098 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:15.771420002 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:25.361365080 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:25.452924013 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:28.832161903 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:28.888051987 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:29.783339024 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:29.829241037 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:31.509438992 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:31.560925007 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:32.877835989 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:32.923924923 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:33.800301075 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:33.846210957 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:35.218780994 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:35.265753031 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 26, 2021 00:57:38.051994085 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 26, 2021 00:57:38.097950935 CEST	53	49361	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 26, 2021 00:56:51.658668041 CEST	192.168.2.3	8.8.8.8	0x3e5d	Standard query (0)	scarboroughcovidvaccineclinic.ca	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:52.021255016 CEST	192.168.2.3	8.8.8.8	0xa98a	Standard query (0)	www.scarboroughcovidvaccineclinic.ca	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:55.254511118 CEST	192.168.2.3	8.8.8.8	0x301d	Standard query (0)	www.scarboroughcovidvaccineclinic.ca	A (IP address)	IN (0x0001)
Apr 26, 2021 00:57:06.309573889 CEST	192.168.2.3	8.8.8.8	0xa30e	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 26, 2021 00:56:51.819614887 CEST	8.8.8.8	192.168.2.3	0x3e5d	No error (0)	scarboroughcovidvaccineclinic.ca	d3ju03wkwsvm74.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Apr 26, 2021 00:56:51.819614887 CEST	8.8.8.8	192.168.2.3	0x3e5d	No error (0)	d3ju03wkwsvm74.cloudfront.net		65.9.66.41	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:51.819614887 CEST	8.8.8.8	192.168.2.3	0x3e5d	No error (0)	d3ju03wkwsvm74.cloudfront.net		65.9.66.25	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:51.819614887 CEST	8.8.8.8	192.168.2.3	0x3e5d	No error (0)	d3ju03wkwsvm74.cloudfront.net		65.9.66.80	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:51.819614887 CEST	8.8.8.8	192.168.2.3	0x3e5d	No error (0)	d3ju03wkwsvm74.cloudfront.net		65.9.66.114	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:52.191471100 CEST	8.8.8.8	192.168.2.3	0xa98a	No error (0)	www.scarboroughcovidvaccineclinic.ca	d2h6yifxtk3sc7.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Apr 26, 2021 00:56:52.191471100 CEST	8.8.8.8	192.168.2.3	0xa98a	No error (0)	d2h6yifxtk3sc7.cloudfront.net		65.9.66.114	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:52.191471100 CEST	8.8.8.8	192.168.2.3	0xa98a	No error (0)	d2h6yifxtk3sc7.cloudfront.net		65.9.66.12	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:52.191471100 CEST	8.8.8.8	192.168.2.3	0xa98a	No error (0)	d2h6yifxtk3sc7.cloudfront.net		65.9.66.11	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:52.191471100 CEST	8.8.8.8	192.168.2.3	0xa98a	No error (0)	d2h6yifxtk3sc7.cloudfront.net		65.9.66.53	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:55.309092045 CEST	8.8.8.8	192.168.2.3	0x301d	No error (0)	www.scarboroughcovidvaccineclinic.ca	d2h6yifxtk3sc7.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Apr 26, 2021 00:56:55.309092045 CEST	8.8.8.8	192.168.2.3	0x301d	No error (0)	d2h6yifxtk3sc7.cloudfront.net		65.9.66.114	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:55.309092045 CEST	8.8.8.8	192.168.2.3	0x301d	No error (0)	d2h6yifxtk3sc7.cloudfront.net		65.9.66.12	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:55.309092045 CEST	8.8.8.8	192.168.2.3	0x301d	No error (0)	d2h6yifxtk3sc7.cloudfront.net		65.9.66.11	A (IP address)	IN (0x0001)
Apr 26, 2021 00:56:55.309092045 CEST	8.8.8.8	192.168.2.3	0x301d	No error (0)	d2h6yifxtk3sc7.cloudfront.net		65.9.66.53	A (IP address)	IN (0x0001)
Apr 26, 2021 00:57:06.375871897 CEST	8.8.8.8	192.168.2.3	0xa30e	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 26, 2021 00:57:06.375871897 CEST	8.8.8.8	192.168.2.3	0xa30e	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.1	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- scarboroughcovidvaccineclinic.ca

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49716	65.9.66.41	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 26, 2021 00:56:51.860018969 CEST	980	OUT	GET / HTTP/1.1 Host: scarboroughcovidvaccineclinic.ca Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Apr 26, 2021 00:56:51.901267052 CEST	981	IN	HTTP/1.1 301 Moved Permanently Content-Length: 0 Connection: keep-alive Date: Sun, 25 Apr 2021 06:32:32 GMT Location: https://www.scarboroughcovidvaccineclinic.ca/ Server: AmazonS3 X-Cache: Hit from cloudfront Via: 1.1 547a50460a0cda7ae3dafb1c0b6d0e1a.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-C1 X-Amz-Cf-Id: UCNogzRunvLFQ54cGbCo0fOEeUoGpYeyLw24M-P21TF1qtAkZ5676A== Age: 59060

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 26, 2021 00:56:55.403188944 CEST	65.9.66.114	443	192.168.2.3	49748	CN=scarboroughcovidvaccineclinic.ca CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Mar 05 01:00:00 CET 2021	Mon Apr 04 01:59:59 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 26, 2021 00:56:55.423552036 CEST	65.9.66.114	443	192.168.2.3	49749	CN=scarboroughcovidvaccineclinic.ca CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Fri Mar 05 01:00:00 CET 2021	Mon Apr 04 01:59:59 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5444 Parent PID: 4892

General

Start time:	00:56:47
Start date:	26/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://scarboroughcovidvaccineclinic.ca'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	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 Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 6060 Parent PID: 5444

General

Start time:	00:56:49
Start date:	26/04/2021
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=1504,4227342176911685725,17676476267147671780,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1808 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly