ID: 339318
Cookbook: browseurl.jbs
Time: 20:55:02
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

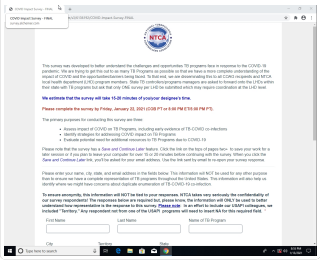
Analysis Report https://survey.alchemer.com/s3/613619…

Overview

General Information

Sample URL:	http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL
Analysis ID:	339318

Most interesting Screenshot:



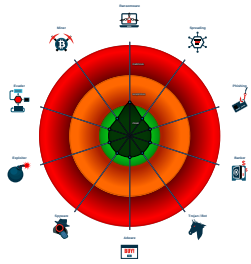
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 3272 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5912 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,552184152371578541 9,345617750357767133,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1692 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

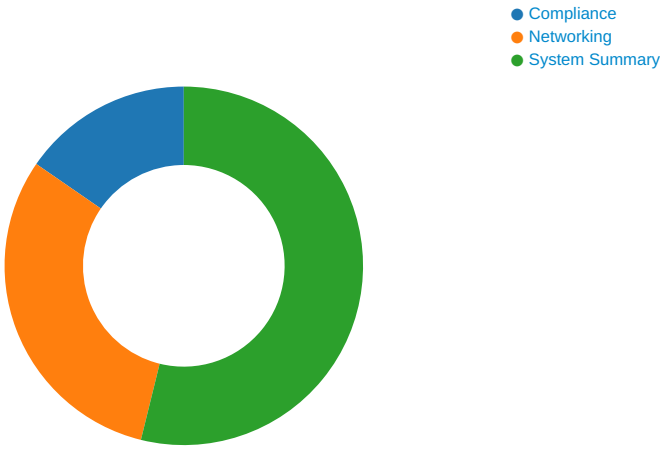
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



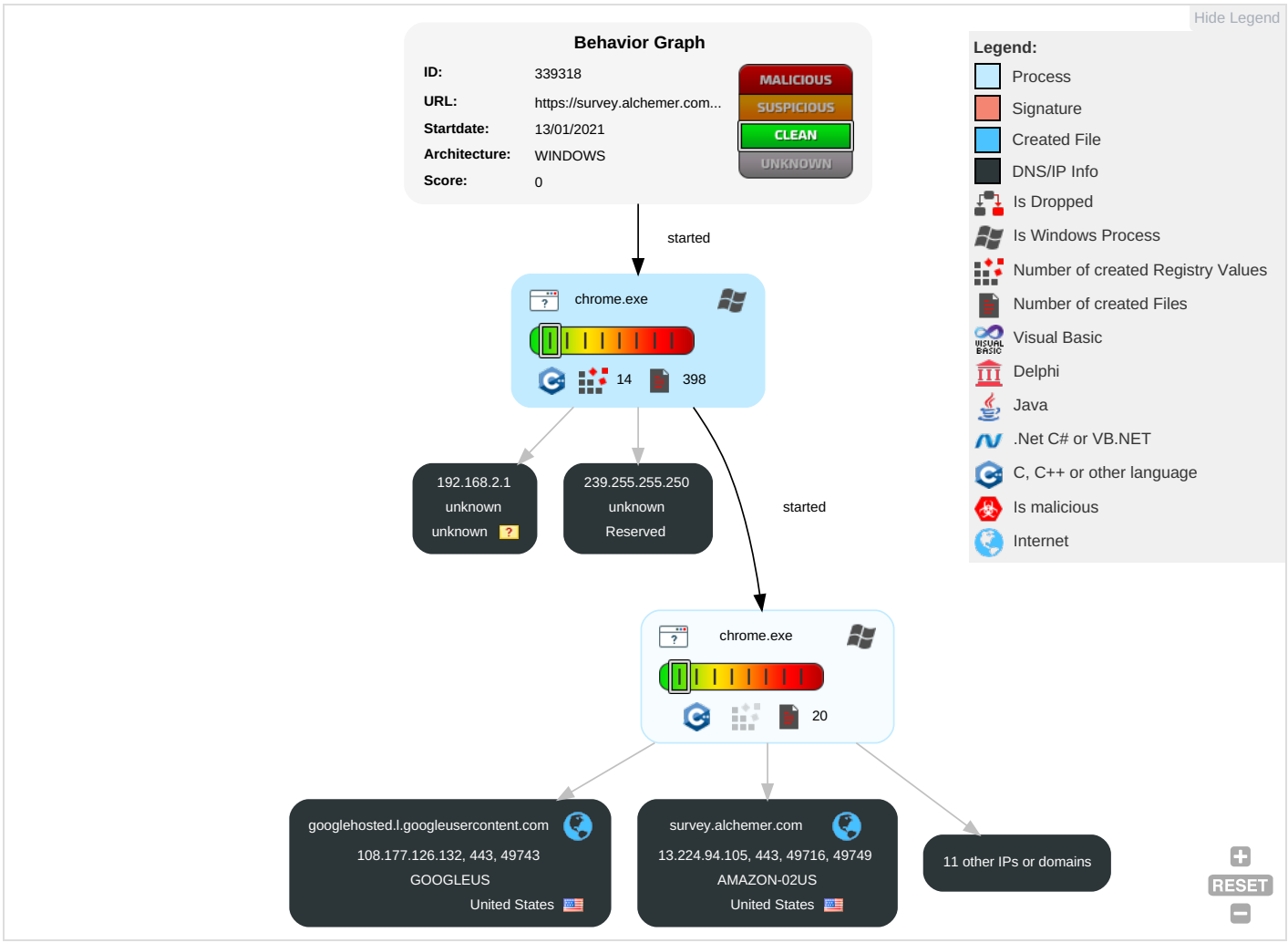
Click to jump to signature section

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	Impact
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	Modify System Partitior
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

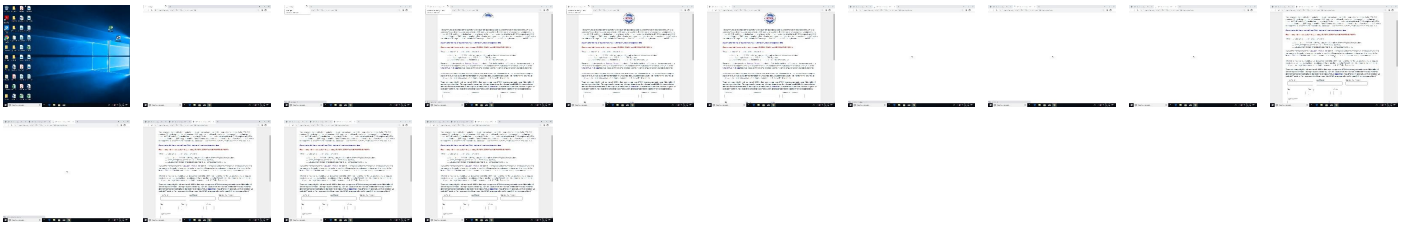
Behavior Graph

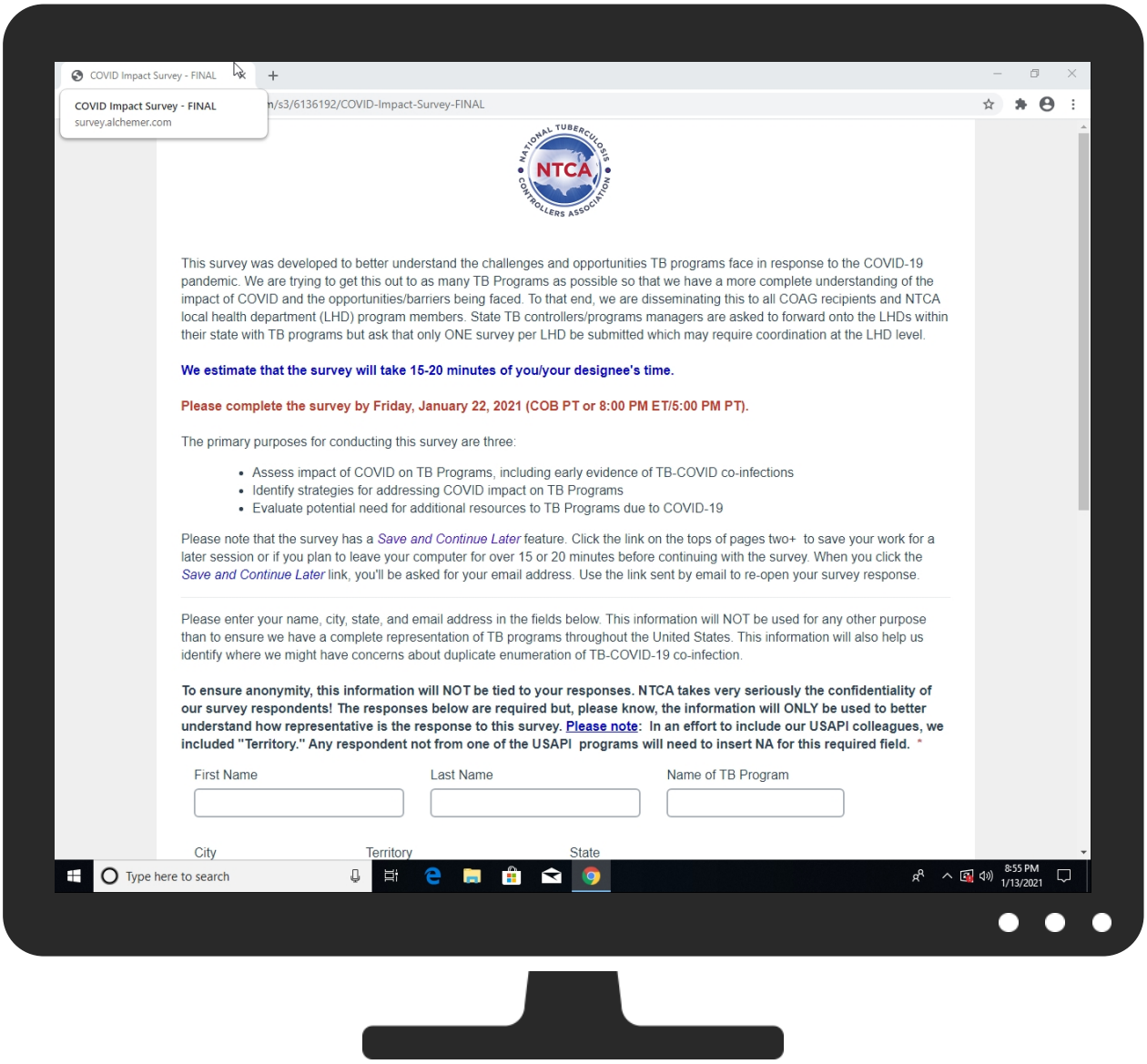


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
survey.alchemer.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL#sg-skipnav-target_	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL#sg-skipnav-targetCOVID	0%	Avira URL Cloud	safe	
http://https://alchemer.com/	0%	Avira URL Cloud	safe	
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINALCOVID	0%	Avira URL Cloud	safe	
http://https://survey.alchemer.com	0%	Avira URL Cloud	safe	
http://https://survey.alchemer.com/	0%	Avira URL Cloud	safe	
http://https://alchemer.com/P	0%	Avira URL Cloud	safe	
http://https://www.alchemer.com	0%	Avira URL Cloud	safe	
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s3-1-w.amazonaws.com	52.217.0.180	true	false		high
d3gvv5iecquak.cloudfront.net	13.224.94.66	true	false		high
survey.alchemer.com	13.224.94.105	true	false	• 2%, Virustotal, Browse	unknown
cluster96-elbwpeel-u8fat1y76lys-241867217.us-east-2.elb.amazonaws.com	18.221.77.186	true	false		high
googlehosted.l.googleusercontent.com	108.177.126.132	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
www.surveygizmo.com	unknown	unknown	false		high
surveygizmolibrary.s3.amazonaws.com	unknown	unknown	false		high
www.alchemer.com	unknown	unknown	false		unknown

Contacted URLs

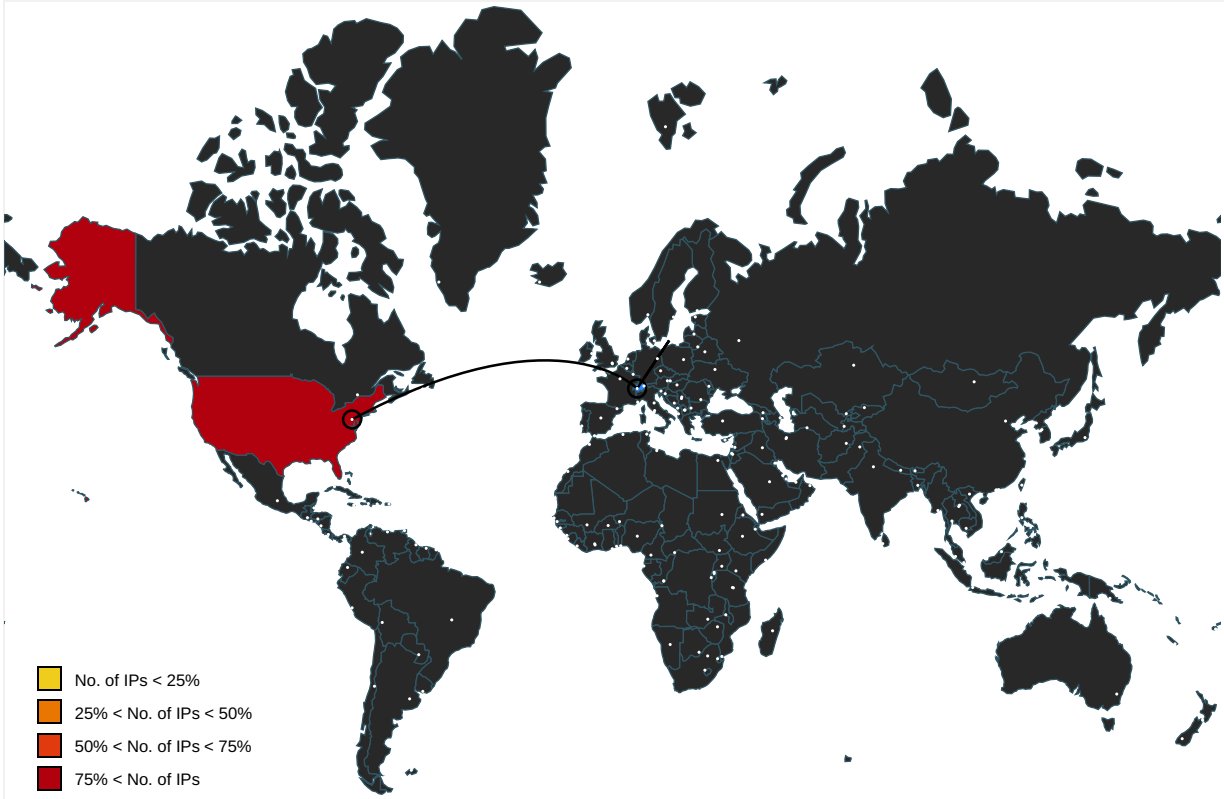
Name	Malicious	Antivirus Detection	Reputation
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL	false		unknown
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL#sg-skipnav-target	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL#sg-skipnav-target_	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	d452acba-5d11-483f-8d58-b71a6434702e.tmp.2.dr, 11f12588-057a-4850-b68d-fdb446f94a80.tmp.2.dr, bdad2fd6-408b-4556-8bae-461793d5ebe2.tmp.2.dr, 982f410b-f4e1-4dd5-a547-84de14331441.tmp.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL	Current Session.0.dr, History.0.dr	false		unknown
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL#sg-skipnav-targetCOVID	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://alchemer.com/	433ff0fc5a6cc6f8_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINALCOVID	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://survey.alchemer.com	d452acba-5d11-483f-8d58-b71a6434702e.tmp.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://survey.alchemer.com/	000003.log0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://alchemer.com/P	433ff0fc5a6cc6f8_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.surveygizmo.com/	Network Action Predictor.0.dr	false		high
http://https://www.surveygizmo.com/2021.01.12.01/runtimejs/dist/survey/js/survey.js	433ff0fc5a6cc6f8_0.0.dr	false		high
http://https://clients2.googleusercontent.com	d452acba-5d11-483f-8d58-b71a6434702e.tmp.2.dr, 11f12588-057a-4850-b68d-fdb446f94a80.tmp.2.dr	false		high
http://https://www.alchemer.com	d452acba-5d11-483f-8d58-b71a6434702e.tmp.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL#sg-skipnav-target	Current Session.0.dr	false		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.221.77.186	unknown	United States		16509	AMAZON-02US	false
52.217.0.180	unknown	United States		16509	AMAZON-02US	false
13.224.94.105	unknown	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
13.224.94.66	unknown	United States		16509	AMAZON-02US	false
108.177.126.132	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.255
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339318
Start date:	13.01.2021
Start time:	20:55:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Sample URL:	http://https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@31/171@5/9
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL#sg-skipnav-target • Browse: https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL#sg-skipnav-target

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, SgrmBroker.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 13.88.21.125, 108.177.119.102, 108.177.119.100, 108.177.119.138, 108.177.119.139, 108.177.119.113, 108.177.119.101, 173.194.69.84, 172.217.218.101, 172.217.218.102, 172.217.218.113, 172.217.218.139, 172.217.218.138, 172.217.218.100, 74.125.104.87, 173.194.188.234, 108.177.126.95, 216.58.208.35, 108.177.119.94, 173.194.79.95, 108.177.127.95, 104.42.151.234, 23.210.248.85, 84.53.167.113, 51.104.139.180, 51.103.5.159, 92.122.213.247, 92.122.213.194, 108.177.126.94, 173.194.188.38, 20.54.26.129 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e15275.g.akamaiedge.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, par02p.wns.notify.windows.com.akadns.net, clients2.google.com, redirector.gvt1.com, r1.sn-4g5ednle.gvt1.com, wildcard.weather.microsoft.com.edgekey.net, emea1.notify.windows.com.akadns.net, update.googleapis.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, r1.sn-4g5ednse.gvt1.com, prod.fs.microsoft.com.akadns.net, r5.sn-4g5ednsk.gvt1.com, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, client.wns.windows.com, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, fonts.gstatic.com, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, www.googleapis.com, r5---sn-4g5ednsk.gvt1.com, ris.api.iris.microsoft.com, r1---sn-4g5ednle.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, r1---sn-4g5ednse.gvt1.com, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.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 GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\54ba5a32-b56d-4095-87d6-bf779a5cd7ed.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):	354272
Entropy (8bit):	6.015576996195932
Encrypted:	false
SSDEEP:	6144:8mS5B8+wcw1fph3A8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBc:hAdrw53VxzurRDn9nfNxF4ijZVtilBc
MD5:	E9D2082D026B490778738D17AFE87BD5
SHA1:	24C3313AE4CBFDEBC626161EF0EFB0D1EB00F464
SHA-256:	7D419D68F80F5418F0324B2B60E208220FF2E482B67E86322A36C6DAF058B553
SHA-512:	529722B829377D82FEC24CCE448C7443FE970E1C702CD2D2A3A3110F3741405A98EC9AB9C03A7533991FFD48E81F1B8D9DC8F82207723B5E9FE36A46D89D137
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":1.610600157026458e+12,"network":1.610567758e+12,"ticks":110979301.0,"uncertainty":4391482.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMlXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13255073753779

C:\Users\user\AppData\Local\Google\Chrome\User Data\6ef6c54b-5bfa-4f76-b7eb-0b68f1d7c41e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7447116375264002
Encrypted:	false
SSDEEP:	384:XbW5dDcW7j8F4NNr+vRb36djiHz+GuRr8/h9xiXPfOrMBmMv87V5FGOjjZNo1tsW:6S9tKPaOUePVb70PrGTKBvNJ+
MD5:	0FB986AC24C43D7F44A8520161DC23BF
SHA1:	32ADFEF2430E7D899BB4FD8EE679DBCEB8CF1DFC
SHA-256:	3715BE4C0D9D07571674E6D60E059288F32CDDDEF3CA6247C9F2B97FED7451C0
SHA-512:	AA3C2ED4FE85151A7C6851CD66FA17AD62D91F88CAF9F671A6508144E1A41750D0A96B01B5CB04EBA8643B7E5A233919D8620C8CF73533B9E0F349C56FA8C2E0
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n.....8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\77bc9d13-f253-4882-886f-dc0333c9394b.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):	357847
Entropy (8bit):	6.028219166851776
Encrypted:	false
SSDEEP:	6144:pmS5B8+wcw1fph3A8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBc:IAdrw53VxzurRDn9nfNxF4ijZVtilBc
MD5:	A1534DA010EFFE46DF2A456D073B5456
SHA1:	C9AC59653013A6822C688F898AAA98B1EEA58FF5
SHA-256:	6BC6573DC5C42139724396EB733FAB6C54E33AD8D3C4C024088AF74F44624C9C
SHA-512:	DDF99D1FBA6D0F94ED973A560F776F8DD2F9F418D6F7365DA6920BD6F3FF2B17AF4B6824FE592A8015476A935C5C781B39E63678B5DA8E02CF28D0017006B6B
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":1.610600157026458e+12,"network":1.610567758e+12,"ticks":110979301.0,"uncertainty":4391482.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075927485"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\79e843ea-38b7-4fd7-b32e-5ab1ce9c8f08.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):	354272
Entropy (8bit):	6.015577328632948
Encrypted:	false
SSDEEP:	6144:5mS5B8+wcw1fph3A8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBc:4Adrw53VxzurRDn9nfNxF4ijZVtilBc
MD5:	FEF95393A53735DC6B9C4200460DD256
SHA1:	3D2C1A699984D83090EDBF54E1A26502176E10FA
SHA-256:	15F069FE642451A04F1BA405D034668C294ACB42E5A2FF6A62AA2D8DB580263C
SHA-512:	803032647694EDB3A7A873E0E3B1E9739A3D6648A34C100D5F81D9DC72F7F59F25D9965C03C097670F62769177724F71EA72C17F72C2229F39CF4AA8D3DD9016
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":1.610600157026458e+12,"network":1.610567758e+12,"ticks":110979301.0,"uncertainty":4391482.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13255073753779

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC....................8...?E."..N_.sdPC....................8...?E."..N_.sdPC....................8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\09fb53a5-e6fb-4cc5-b785-bd8386918ecb.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):	22613
Entropy (8bit):	5.535611858154587
Encrypted:	false
SSDEEP:	384:29DtBLlv4XN1kXqKf/pUZNCgVLH2HfDLTrUXHGonTKGatCgxj4Q:eLlKN1kXqKf/pUZNCgVLH2HfzrU3GonE
MD5:	0A41905C3ED237B57F0526BC0693E9AF
SHA1:	2E66A49FD689AE4418E2B80E5C87221511EA329F
SHA-256:	EC3D9966B31C5BB3C7BC0EDE6F1573ADE25FE8365A30A97B457466001157DF26
SHA-512:	5331A146457352562B67AA1AB2366D94E674475017CAC07D6134A2FC3A570BEDE28D0F68267DBB8B119CABE676D6135334AE5960BBC0732FC154CD3722D195C
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":"13255073753891350","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\0a0b8d48-5221-4e5d-ab9f-5e3dcb50bd68.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):	5021
Entropy (8bit):	4.96352986582791
Encrypted:	false
SSDEEP:	96:n4nrFEr4pSVZIk0JCKL8Hkd11dbOTQVuwn:n4nro4pSLC4Kekd1
MD5:	491FAD8622B86BCCC325E7AD367A85B5
SHA1:	156D00952905636CCD3AB4CF50450F8B9BB22D95
SHA-256:	160EE889A9B91E247B7D3D03A29CE6B661DE92B6FEE9E43ED61B1CDECB783FAA
SHA-512:	DB43F133D9306B675B28B388507FB278F6ADCA65ADB57627ED2EAC5D2CD27C2B8978EDA8FFAC39331767A3A9FFBBC8D5FEB688A7DC4C98DD083773FAB97282E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13255073754188032","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","1538886"],"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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\11f12588-057a-4850-b68d-fdb446f94a80.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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\11f12588-057a-4850-b68d-fdb446f94a80.tmp	
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2670eaaf-e65c-4824-8c76-7e1bee35d01c.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):	5617
Entropy (8bit):	5.187678607611437
Encrypted:	false
SSDEEP:	96:n4nrFIr4Cg3XZSVaIk0JCKL8Hkd11dbOTQVuwn:n4nrI4CgZSAC4Kekd1
MD5:	E1C0A3B74111ADE57EA94DE1B5DEDAE5
SHA1:	29D1F0CCF7BE4FBC0A006D8156DBB2E72B95EB1F
SHA-256:	E2AD72979869529BF9DCAE2CA180029EFB11006922B12CF1E106A9BE12D4EF78
SHA-512:	70DD8AB086819C5693120516935079DCE9C200DC7F21C4B57F2A798F0750B0077F26ACCAB550E861C3E0EFC37AA0779A002B63D8E0FA6FE6B6667A2AFA6D07E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13255073754188032","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","1538886"],"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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3ad169a6-c911-4ec0-adc9-3423dc1fc4e3.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41e5646b-2a7a-4636-9e9e-a84d6863a06e.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):	874
Entropy (8bit):	5.553914401044261
Encrypted:	false
SSDEEP:	24:YT6H0UhHu05G1KU3aUeCeqb7wUckBRUeIQ:YT6UUhmKUKUeCRwUFUeh
MD5:	D445E7AEA979BAA016445DD36E6B2A25
SHA1:	72361980D8CF65778F2B0FA76C1D2CA7A80960D1
SHA-256:	4DE335F04C3FD0C6377CA00C409021FAB3B936AB80D366D9E508BB6618630722
SHA-512:	4F149F2166AB1AEC0091A856080825D45AFE60F0FCC761FA1D973E562A1585467EF2AEEF1AC4DFECD72CFFBD1A609832AB5D7C75B1934BA0650B6FA0E0CD8AC2
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41e5646b-2a7a-4636-9e9e-a84d6863a06e.tmp	
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1642136157.870461,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1610600157.870464},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1642136156.952818,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1610600156.952822},{"expiry":1633013028.952627,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.95263}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\70780d05-9cee-48fb-81f6-b18db0dcaed0.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):	5707
Entropy (8bit):	5.188978604034113
Encrypted:	false
SSDEEP:	96:n4nrFzr4Cg3XZSVbIk0JCKL87k60SMHofxzbOTQVuwn:n4nrZ4CgZSJC4KGkEPH
MD5:	C29140F3B1DD1D961AD6C2B810F95E1A
SHA1:	FED647DC9E029DCF4F0B07B5200A31269F59E601
SHA-256:	92F0FF5881C62CDFB1D0E6C79EA53489CAE1ECAC31418730D0D3117E9BA36029
SHA-512:	A16C661C6B91C030F51970BE8EEB0A6B00F11A18792CAB91765AABF72FBA912B1E79AEF8C56ECF483C9223C40000CDC9ED3FC707D90103FC2D2B83DA324EE6 52
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13255073754188032","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","0","0","1538886"],"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","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b54cf1a-7317-4087-b1de-e3a97615fe2a.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):	19025
Entropy (8bit):	5.567079092991649
Encrypted:	false
SSDEEP:	384:29DtMLlv4XN1kXqKf/pUZNCgVLH2HfDLTrUXHG5kGatYgxj4L:VLlKN1kXqKf/pUZNCgVLH2HfzrU3G5ko
MD5:	9DF9198919274E8144C09439EF28D791
SHA1:	624CBF6136D85730BC3D6A58DD5EE4E38B7AFF52
SHA-256:	684D53AB5B83023FC94BB9DDC2E32EFCBD81BAE3A96A12B1DCF1DEDAA6B88D60
SHA-512:	7A5ED7D2BB11D34BA438C2FE9F9774030F4719C20CC12124750EC83FC7963794978BF449EAF7EFCEF3509F31D85A5427A0F24E035DC987F880640E0AD2CB59A
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":"13255073753891350","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\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.210810469710418
Encrypted:	false
SSDEEP:	6:miXqL+q2P923iKKdK9RXXTZIFUtpDCUEL1ZmwPDCUEdLVkwO923iKKdK9RXX5LJ:7qL+v45Kk7XT2FUtp+dB/P+ddLV5L5KU
MD5:	FC54654CF572B6211AC688D204E6B25F
SHA1:	F68666608268889969B0C48ECE98EAB034BFD3C6
SHA-256:	DBF0BB1C9DFB33FE1ED7119593F12CC28662AA6DE0C467094E857560C0D39BDE
SHA-512:	14C15BDDAEFA7DEDDF01F95825BD650BFB718DD7BECB91901A18E552E390864E59A68314968895BF7741F0915E892AA13F8670FAD337D396FDD4A3966CC82FE 1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2021/01/13-20:56:02.469 1a7c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/01/13-20:56:02.487 1a7c Recovering log #3.2021/01/13-20:56:02.487 1a7c 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):	320
Entropy (8bit):	5.114673021291832
Encrypted:	false
SSDEEP:	6:mi0qL+q2P923iKKdKyDZIFUtpDaZ1ZmwPD/jLVkwO923iKKdKyJLJ:YqL+v45Kk02FUtpWT/P7jLV5L5KkWJ
MD5:	C9729724C3FCE9F558D20B2931718BA7
SHA1:	07E758E2BDAE7B8007752DD6C9C35DE5D267DAEB
SHA-256:	1BE583637D0E158EC5B3B3435DF024ACDF958778B94A62E78EBF84E5688ED95C
SHA-512:	ADBEC1571AC63654ABFE5F1012579DEEFCC4EB6E6815B063AB1D1BA3E6407176A6AE462CA45BD9355F2C55FF928E75A038E42BB014E90C6FC434AF6E829DE3ED
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:56:02.000 1a7c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/01/13-20:56:02.003 1a7c Recovering log #3.2021/01/13-20:56:02.004 1a7c 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\433ff0fc5a6cc6f8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	705
Entropy (8bit):	5.5320424152747965
Encrypted:	false
SSDEEP:	6:mtaYGLXOrYksil3tSglLaGhdS1Z41QK6tWtaYGLXOrYksiP1CglLaGhdS1Z4oDKn:hkn/61Z/zknA1Z51zknuqC1ZgH/T
MD5:	BC8834E9723B9940105569D29F0A85F5
SHA1:	24D8A7546D0DC625AC4FC0FC90106CB2C22C8C9D
SHA-256:	1F4F22FC67FF21BF353367D091F582B95C4AB0A21041FCA17D57A018379B1D8A
SHA-512:	2D6F806DC8A721F441447D7C0211780537C5BE0C7BA93F3E7E29127EB82A1717771140847325D281622ECD33D66EF7D73BCC15DFC41D890D867F1B95343FEEA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...].Wy...._keyhttps://www.surveygizmo.com/2021.01.12.01/runtimejs/dist/survey/js/survey.js .https://alchemer.com/*..Zk./.....5.Y..5..?..L%aoyD?.D5V.....A..Eo....._.....A..Eo.....0\r..m.....g...].Wy...._keyhttps://www.surveygizmo.com/2021.01.12.01/runtimejs/dist/survey/js/survey.js .https://alchemer.com/..V[k./.....\.....5.Y..5..?..L%aoyD?.D5V.....A..Eo.....15.....A..Eo.....0\r..m.....g...].Wy...._keyhttps://www.surveygizmo.com/2021.01.12.01/runtimejs/dist/survey/js/survey.js .https://alchemer.com/P.%\k./.....5.Y..5..?..L%aoyD?.D5V.....A..Eo.....]_J$.....A..Eo.....

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):	120
Entropy (8bit):	4.047157300429571
Encrypted:	false
SSDEEP:	3:f+bi094l4YHl67U4KL/lllhuBQ6qKqlMBObn:2bbulXrqBQ6YMBOb
MD5:	26B01FC30E1A31BE6260895B2C26063A
SHA1:	DB7FFE2B86B33ACB5E98C007445D5C3E7DFFE7C8
SHA-256:	786EA8220B2906354ACC9794727F85A4811C318CE7D8B49F0F71C9DB4B3323E7
SHA-512:	7A0838F82A27924B4292BC38DCAA8476A0D603C9C6FAD78283AC3C3DB1F34581A6D2EAB91A6F740A2FAFD1F761F2CF5A5FE1C64B6057BA9206A5B2F4097901A5
Malicious:	false
Reputation:	low
Preview:	p...:pq.oy retne.....lZ..?C.. \k./...../...3...5../.....^}.Np.....5../.....!.*\k./.

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):	8192

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Entropy (8bit):	1.3525350041890412
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwIn4rtEy8i:TekLLOpEO5J/Kn7ULix
MD5:	50C279FDAA6EC0A5033A860FF4D676A6
SHA1:	F0BCCA90A1DCF3B24886705402C1464461CEFE13
SHA-256:	81659C4AC15FBBF57F043BC1843C76DB58DFDFDE7C9621C916EED7D233E9F69C
SHA-512:	796980B60E6CB40A81483FC4C0CCAE0F269A122F9A531EC99D3A906E028967076E000DDCDBFAF12CC9584443AB1E6599A55AE6E857C4C7B1E150AC6752572A1B
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):	8732
Entropy (8bit):	1.3148716760385069
Encrypted:	false
SSDEEP:	24:EIL4rtEy81qLbJLbXaFpEO5bNmISHn06Uwi9:EI+oq5LLOpEO5J/Kn7Up9
MD5:	8E4E3F1316461033C5F60605132FDA81
SHA1:	A6D38BAEC1814AF3B0C2827CE5124F96BBA4C3F3
SHA-256:	CDF833526ADDF442DE550E04D5C122D3599F4B599002E61E897EEFC1B0346437
SHA-512:	71C65E5186A2622BED434A9626F1EFC759410E52BA437F313A8D58DF9536B63564B0D50DA33332494ABF8B7C4013F931C4DE570D6A9D7375EC63C9D75EDA851
Malicious:	false
Reputation:	low
Preview:	.....`2..... ....

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):	15970
Entropy (8bit):	2.9153806782300853
Encrypted:	false
SSDEEP:	96:34j0k4kuyTILUB4vvvvoGzjYg6Kgvf8KI40uFYvvvvH9s9gh+gKfhIW/mbvvvvo+:3wP4ktqUBHGSBh0uF4fM1/mkE3
MD5:	F3945F36818D58B0B566BAC44D06B1BB
SHA1:	E64F1B0CA87D2EEEFD2A4742929143FA5F33938E
SHA-256:	E9A5AA752C5B52736007D9B275909079F430D991C51F611EA634C94781E62570
SHA-512:	05C2CA99E0FCEA460219DECC2A498DFEC240CBC0ADAB77CE50CB0E366D49FA38958D7386D1CA472F59E90336B2A21D679FF503FB989ED888419767A8AAA10716
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...bb154784_e4a4_4605_b662_b478a49dece5.....Rq..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....@...https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL....C.O.V.I.D. .I.m.p.a.c.t. .S.u.r.v.e.y. .-. .F.I.N.A.L...|...x.....p.....h.....`.....C.....C..... .....@...h.t.t.p.s.:././.s.u.r.v.e.y...a.l.c.h.e.m.e.r...c.o.m./.s.3./.6.1.3.6.1.9.2./.C.O.V.I.D.-.I.m.p.a.c.t.-.S.u.r.v.e.y.-.F.I.N.A.L.....8...F...0..... ...x..... .....8.....P.....@.....X.....p.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
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):	319
Entropy (8bit):	5.1379396399032595
Encrypted:	false
SSDEEP:	6:m8S9yq2P923iKKdK8aPrqIFUtpMI1ZmwPkRkwO923iKKdK8amLJ:eyv45KkL3FUtpMG/PkR5L5KkQJ
MD5:	7C3A182F46CCDA84EE4324219FB07C86
SHA1:	00EF5AB76DE9FD88ADB353D0D8F9F39F8ABF53BE
SHA-256:	21A054DDF987F7D15E3C86D8FCE022D46404AFDB392B7C2DBEB808B49CE2D18A
SHA-512:	F4BB8A1023F3B133AC914655BBF15211235CBA0B75AAE5376487A618827D46920300C28810DBA16FFC6430E8F149E37C215CAE230BFB69B2082E62CF73533A4B
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:55:54.241 e70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/01/13-20:55:54.242 e70 Recovering log #3.2021/01/13-20:55:54.243 e70 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Size (bytes):	319
Entropy (8bit):	5.157234210025608
Encrypted:	false
SSDEEP:	6:mm31yq2P923iKKdK8NIFUtpJr1ZmwPJ9RkwO923iKKdK8+eLJ:Tlyv45KkpFUtpL/PXR5L5KkqJ
MD5:	30248B789E6D9B829A3996B4CB2A599D
SHA1:	845022E263A434E83F0DF303B2D07165E058612C
SHA-256:	B59975D2762CB0DFE8FD79EB03389117E82835D9CEFA32B70BE7065A54A131F8
SHA-512:	C75F3DC079CBCF9348864098972553751B4B0A0C60613B1CD08BE43014D04D6CFAAE19A065E3E8F497903D496D66DA0B3909F7A1CBD6BCAF2E3E1CC9FD09624
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:55:56.536 e70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/01/13-20:55:56.538 e70 Recovering log #3.2021/01/13-20:55:56.538 e70 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\1.0.0.5_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
Size (bytes):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49C
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2l/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

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
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":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+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=","hqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
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):	374
Entropy (8bit):	5.187486475640888
Encrypted:	false
SSDEEP:	6:mHTm+L+q2P923iKKdK25+Xqx8chI+IFUtp8Rf1ZmwP8MLVkwO923iKKdK25+Xqx7:h+L+v45KkTXfchI3FUtpCd/P1LV5L5KN
MD5:	82F2ED4BA9CC14948E055778002C3477
SHA1:	362E9451E7F800048E39636C02A49B6594225595
SHA-256:	5A0211210A3F3402193282D2E33C439455166A315BDE83D06F90FFFA954DB306
SHA-512:	0467F5CB1E1F62D2DEFB4C4FBE9CC7A68ECAEE166C3C00ACA6E3ED20F66D8537D4C027F0343711C4C355EAB8F98470D5C46FE05C4C006ACDDCA572CFEA61289
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:56:01.370 1a7c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/01/13-20:56:01.372 1a7c Recovering log #3.2021/01/13-20:56:01.373 1a7c 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):	360
Entropy (8bit):	5.166148851598679
Encrypted:	false
SSDEEP:	6:mHVEdL+q2P923iKKdK25+XuoIFUtp8R1ZmwP8ijLVkwO923iKKdK25+XuxWLJ:uqL+v45KkTXYFUtpS/P3LV5L5KkTXHJ
MD5:	46DBBEB2E159F6DAD36B2197257BE76D
SHA1:	95FFA3E23BAD2FEFC6FABD364BA3D2E53BF1F002
SHA-256:	DD94079F9657F6FC2A70121C1C0EF1EDA37247648942D61B5666EC69DA5AD43F
SHA-512:	F30A31ABD7F8046C6523AA8F3AFA0C7B9589C9EE23E8A3959B26F7BE7E00330E5E2309427E9DB577B65EEF8355ADCE6BAC9A5079B51898219AE1CF34EF0BC6AB
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:56:01.364 1a7c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/01/13-20:56:01.365 1a7c Recovering log #3.2021/01/13-20:56:01.366 1a7c 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):	332
Entropy (8bit):	5.157986435760614
Encrypted:	false
SSDEEP:	6:mHuL+q2P923iKKdKWT5g1IdqIFUtp8Jo1ZmwP8RS+LVkwO923iKKdKWT5g1I3ULJ:bL+v45Kkg5gSRFUtpx/PeLV5L5Kkg5gZ
MD5:	52714E9F44F16814566A5EC4F3FBA768
SHA1:	20AF0E3945021AA039E319F645E1F22749F8F904
SHA-256:	18BD53FFF317A5F30C96324DB36C41D81377449FB93D3D08AEA1E9DF9384AC77
SHA-512:	711580A53B299B7C543A4C8C36F2A2D89802C50059EA8CDAFD26B9A8DB2ADD7CBD311D63F9704FEA4ABF7F102BA21444E54245A08E495365A5D3822AC4E7494
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Reputation:	low
Preview:	2021/01/13-20:56:01.270 1a7c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/01/13-20:56:01.272 1a7c Recovering log #3.2021/01/13-20:56:01.273 1a7c 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):	53248
Entropy (8bit):	0.24281083605339834
Encrypted:	false
SSDEEP:	24:TLBkdDDxUdjDIcQAMnNv6dQ9dBdDDdadjD7jjKZt:TUU0cQAMnNvpxczjKZt
MD5:	CE7E9FE608FFA95CFBFCA5297568E88B
SHA1:	FB5CBE8A2BF054AB50B15BD16BB40F4385877555
SHA-256:	8665F83EEED671F7E1C52D3CAFB3EDC3A219D8C7FDA0EBCAD5FB4C14DBC8FFE0
SHA-512:	7600EC52DBF85383306FABFD682BF2D9D3D1B9C167709F87D925764BAD80E7F4F3743895DB488A605612666A43133F0205F17F7EB725E09869B3D80CA3AFCBF9
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):	664
Entropy (8bit):	5.391451319909734
Encrypted:	false
SSDEEP:	12:MbCGemX/HYSmLjMwJGg3+HMpaDrB2lIvWKBk778B/xgskZBa2jI86BU/QDihDtks:+G+q9EBOIY78BJgskfaH1dkDWANN
MD5:	701CEC0ED50331D80088858944AFB2E7
SHA1:	9D9BA1FAAB87116CA570F35AA2C80968B3277880
SHA-256:	C28FC84DF9CF4F7532E34CDAA90C5782E2F02546712319EEE1745CAB723851B9
SHA-512:	67A4D73216A2F9D3086D07EB9A63F2D1A22A2EE76788E1918D3BDC1791A2A4CD8D4C248E3A0CCC1BEAA72464B1E8877656ECC06E1027DF91F422310FDE7B317
Malicious:	false
Reputation:	low
Preview:	....."C....6136192..alchemer..com..covid..final..https..impact..s3..survey*g.....6136192.....alchemer.....com.....covid.....final.....https.....impact.....s3.....survey..2.....1.....2.....3.....6.....9.....a.....c.....d.....e.....f.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....y...:S..... .....B..... .....*@https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL2.COVID Impact Survey - FINAL:..... J.....'-4;.....

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):	63120
Entropy (8bit):	0.14804602501974223
Encrypted:	false
SSDEEP:	24:6m946R3c3pqLiUqt37cdDDxUdjDGMLAAGtjt56F5fwjNO:hwqu37+UqMLAACjtgb4O
MD5:	BFB4318F61603560766B4E190F1F9133
SHA1:	4125C91C71257DF683478F3C798B9F91CC056FBE
SHA-256:	8140729835A5B7CA44BA59DB80ECE1C9B94C5C5A094A5208504797CA8F48742F
SHA-512:	579E8A29675CC72DF21E9ED52CD62E0F93958E806A5DD1F53FF9691690E6AF565314B7A0A543D8626088361F71E4D5017AC691810FAC0D2E4AAE36FB9313CB35
Malicious:	false
Reputation:	low
Preview:	.....j..`..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.461449326552079
Encrypted:	false
SSDEEP:	48:4Dz34GYtV3AH3P3La763LMW78db+eGe2/+isbQSefgGMNrS0U9RdiN9Htc:o3I3W3P3La763LMWIdb+eGe2/+3bQ5ff
MD5:	F2810B35BF7E2B6E8668ABD36A6F87B3
SHA1:	DB6C4CFA5639B154AEA124E572A92503BF56D120
SHA-256:	099BD7561171803168CC0188B143ECBE970B138C7B69FFA72E823F7721FDBCD7
SHA-512:	093DBA70C907C6E65789CB88AB2C7726A9560B5E7D2134FB88BAEF7FE2B0AE466A4A6556CBF6A1BD5BEAA1998E189920E00126E223BCE28BAA743B2814527265
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..883639000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-01-13 20:56:05.10][INFO][mr.Init] MR instance ID: 21d4a3f0-1c44-4574-aec6-106a831f58e4\n","[2021-01-13 20:56:05.10][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-01-13 20:56:05.10][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-01-13 20:56:05.10][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-01-13 20:56:05.10][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-01-13 20:56:05.11][INFO][mr.CastProvider] Query enabled: true\n","[2021-01-13 20:56:05.11][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):	334
Entropy (8bit):	5.179166644921527
Encrypted:	false
SSDEEP:	6:m7HFN+q2P923iKKdK8a2jMGIFUtp0ZXZmwP0wVkwO923iKKdK8a2jMmLJ:iIv45Kk8EFUtpU/Pf5L5Kk8bJ
MD5:	5E83502C4E66E20F7CC5FC3BDCE81B7F
SHA1:	AC9EAC904A0E1F5E45783FAE756CA339D7EA0027
SHA-256:	6A0730133BB15B940F3968D7C5EDC595F6438DE0406C9DB77364C8A5BD423F5E
SHA-512:	DC397F4A4BB357E8B48F579AE14DFEFBF9E3DD768291FA059335CEF9AF7692B7A2BECAFA7606DC4DED0C67971EE96B2646D2D4EC5B96EE5F1BBF4356F70D6052
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:55:53.938 1708 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/01/13-20:55:53.954 1708 Recovering log #3.2021/01/13-20:55:53.975 1708 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\Network Action Predictor	
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):	24576
Entropy (8bit):	1.1616223728511506
Encrypted:	false
SSDEEP:	48:Trw/qALihje9kqL42WOT/RPbw/qALihje9kqL42WOT/PWo6:vOqAuhjspnWO5OqAuhjspnWOqo6
MD5:	980C8E5C728B41C010864423FC4C5053
SHA1:	3783FDF92863776B675792A161691AAC3B693524
SHA-256:	165DE4EBDCDCA74149000DEA0EBF35E4B7F848D73F670EC924A90CFD38A7D8CF
SHA-512:	CFDF5686216B14EE79A587449ACF65EE60A82B6A73E2723456D4F96D0601A8245E34FA2A305EC5EF5288CEE5146E806F686B3132DDCC9CB12A2D39D7763D75D
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>...,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.0210628640620847
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
SSDEEP:	48:C0q7w/qALihje9kqL42WOT/Px1qrw/qALihje9kqL42WOT/K8:C0UOqAuhjspnWON1kOqAuhjspnWOl
MD5:	11F0D15D7B9A777837BB2E023E9D5868
SHA1:	ABBAB7515AEB7269468805C8BFFD73C745058D7B
SHA-256:	6647E845CC3BEC902AFACD54914E95403565B29E3B16908F86869C6347B2048E
SHA-512:	1FA0C64F056DBD6C01BF8D799E5397AA36F7082053978D12ECAB602F3B289AD859D48F964D4BF69C20268AFBBE9D3C2ED2EF3832963F5F85A6BFA8C371D8E2F
Malicious:	false
Reputation:	low
Preview:	....

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):	333
Entropy (8bit):	5.1698769346278795
Encrypted:	false
SSDEEP:	6:muHyq2P923iKKdKgXz4rRIFUtpj1ZmwP+k1RkwO923iKKdKgXz4q8LJ:Ryv45KkgXiuFUtpJ/P+eR5L5KkgX2J
MD5:	AFE07BE6A9B29554D257AC5C9874E782
SHA1:	D7CEADF26B6B308F2A35D6DA46F5D39CBB255EE7
SHA-256:	7384C9D736E60D5C67238CA74059E398979471B8BA715009C947A5050DFBDBF5
SHA-512:	E540CF0EC2F935DDDDAFC263C540EA8840B9E8F05553139BF9C649F952B57216623C6BA5B09202BC3A099D648AE1D267B0DB7085A70BDCA68AE70BC1C7F1CA1E
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:55:54.277 e70 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/01/13-20:55:54.282 e70 Recovering log #3.2021/01/13-20:55:54.284 e70 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\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	453
Entropy (8bit):	5.029741706061513
Encrypted:	false
SSDEEP:	12:5lYhUqXn8+CPXj+AP9A/XmPXQDthknd5h/:7qUYn8rPXj+CqXm/Athknd7/
MD5:	1FEAEFC1053C47EEC7BF5D1DF9306B78
SHA1:	BBCBA4794C00FF5D3B97217D2B704158141614E2
SHA-256:	A4FC313D81C0410726F4532F675C8888422A8F7D2405DE68F51201E1FC496E74
SHA-512:	2246424E602599E3D11B15F267948D8467CE9D5DAC093875F0E125ABEC937C545536F74CCD7C5230C43812E007357356F772724B0F35F485F2B46595B6768304
Malicious:	false
Reputation:	low
Preview:	..&f.....j.....next-map-id.1.Knamespace-bb154784_e4a4_4605_b662_b478a49dece5-https://survey.alchemer.com/.0V.e.....V.e.....V.e..... .....W..j.....next-map-id.2.Knamespace-a798e7fb_1a7c_46a9_a01a_190f96616dcb-https://survey.alchemer.com/.1. .....m...j.....next-map-id.3.Knamespace-9dcf6f53_d020_4b57_a213_71f87c1197f9-https://survey.alchemer.com/.2.R.....

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):	322
Entropy (8bit):	5.150067686470471
Encrypted:	false
SSDEEP:	6:mO3+q2P923iKKdKrQMxIFUtpkJZmwP9VkwO923iKKdKrQMFLJ:Kv45KkCFUtpc/PD5L5KktJ
MD5:	D82DCAB1FD7124B182E104CA647D16F6
SHA1:	FAFBBB09F49B4523AF485F94EFF73099BA88C4E6
SHA-256:	1CC50AB4F05E274E0BC83E7AC0B743CAEABC34E9CAFB7E68072AB9FCD10F2892
SHA-512:	34AFCD7F9939A8FDA232921FDB28B1E2C1D3A85C5A560973F3FD5A8F770BC86D78401C600A4A35D6CA9F1648F0506D7EECE4A5D82C4E30102F8DF6D6B8A6C0E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Preview:	2021/01/13-20:55:54.174 1708 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/01/13-20:55:54.175 1708 Recovering log #3.2021/01/13-20:55:54.176 1708 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/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
Category:	dropped
Size (bytes):	347
Entropy (8bit):	5.1397720367411885
Encrypted:	false
SSDEEP:	6:m7siFlq2P923iKKdK7Uh2ghZIFUtp06XZmwP0Sm7kwO923iKKdK7Uh2gnLJ:QIv45KkIhHh2FUtpZ/PPm75L5KkIhHLJ
MD5:	9E0A817EAC1105736FCC804C97473F90
SHA1:	A7101855B0B6F73A2BCD3352179A4C3E56E85907
SHA-256:	232FB6E26104E8524BD212D129DCE476CBBFDD491F4EB5CE0B1D0C672DD1313F
SHA-512:	AE21DF06217E15D8FB2B6ADD87936A64F2A94FD3E74918B2E47502132083FEF81B5C9481B8FC50D25C40310EF24414C86484EEA2CC27C9A30D3093E609978B0
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:55:53.870 920 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/01/13-20:55:53.871 920 Recovering log #3.2021/01/13-20:55:53.872 920 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\982f410b-f4e1-4dd5-a547-84de14331441.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	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):	432
Entropy (8bit):	5.240342422180261
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
SSDEEP:	6:mMt+q2P923iKKdKusNpV/2jMGIFUtpIqXZmwPEnVkwO923iKKdKusNpV/2jMmLJ:4v45KkFFUtpPX/PA5L5KkOJ
MD5:	BC632EA8A5A925B1F30F22FD46F43FF2
SHA1:	259C2575976EE9E8F07FBD1573812055AC10C306
SHA-256:	BD168C46AA23E37E59AB653CB1862857E81A6EF4B910D7AF94CE0C208BE863FE
SHA-512:	A20882EC8DCDB93334BE8AC56DC976DD5CCB7D1F30A7EC6C4EB513ECA1BE903D6A678711FF4911E612EDDF1A1EE8F34EDD76233B199B6F29AEA7A7F73755F EF4
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:55:54.222 1708 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/01/13-20:55:54.224 1708 Recovering log #3.2021/01/13-20:55:54.225 1708 Reusing old log C:\Users\user\A ppData\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):	434
Entropy (8bit):	5.287251793181886
Encrypted:	false
SSDEEP:	6:m+L+q2P923iKKdKusNpqz4rRIFUtpPZmwPPVkwO923iKKdKusNpqz4q8LJ:Lyv45KkmiuFUtpP/Pd5L5Kkm2J
MD5:	1E57034CF9CD3F2415E996B79E057534
SHA1:	9BD49B133E0539AD6FCC3D2748FF52131987B658
SHA-256:	27270BAADBC66C16DA425F92C2C5EF3AE5F8A7C814DEB43D0FFE5C4429854534
SHA-512:	290616426469BAF2B90EFC0896B982FC936102E07A3C9579FD78F0D41463FB4BB2A6C80F34E27425E3EE64C9BF0CBEF926C3365F11AC7607847FF1F0CADA97F5
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:55:54.278 16d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/01/13-20:55:54.281 16d8 Recovering log #3.2021/01/13-20:55:54.281 16d8 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):	420
Entropy (8bit):	5.238551355234884
Encrypted:	false
SSDEEP:	6:mA+q2P923iKKdKusNpZQMxIFUtp7EZmwP7kVkwO923iKKdKusNpZQMFLJ:Mv45KkMFUtp7E/P7k5L5KkTJ
MD5:	693201E2FF770E42FA634A28C7CF2474
SHA1:	1E984DFFB40C2A5952A7606AEE3810F66DC47838
SHA-256:	0299428B8CCEC2F291F87F18B44EDED70B3FB55DC82109789B98B407D5CC0525
SHA-512:	2A0F6D08BD58F9A811887FC791AF11FA3F85C6C10E491DB98DC7FF074FFD7DB4D837F71C70DE8E6853AC1554012E91C01A6249EC4BD95D56B3C53A7EC80B55 A
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:56:10.761 16d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/01/13-20:56:10.762 16d8 Recovering log #3.2021/01/13-20:56:10.762 16d8 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\nmmhkkegccagdldgiimedpiccmgmieda\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\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.171453609488469
Encrypted:	false
SSDEEP:	12:rv45KkkGHArBFUtp3XZ/P65L5KkkGHAryJ:r45KkkGgPgdXqL5KkkGga
MD5:	75657AE00DE86DBA05F644780519B257
SHA1:	E12B3755EC8C185950E765E78260ED0D89679A0D
SHA-256:	1835E27CAE12845B6A66BA4CA27DAC8DF77ECC0E6E3E0CAFBDE1CA0B60FDBC43
SHA-512:	E4AC50E80315AA1CF3562BBFDFBF928DD117DB430DF73C2CF0F83D9AF1E6B5240AF7208901174F6CDB348BDBF53A501E2AE8AEC7EDC5A692587F84D854AA2E EB
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:56:02.515 1708 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/01/13-20:56:02.518 1708 Recovering log #3.2021/01/13-20:56:02.520 1708 Reusing old log C:\Users\user\A ppData\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):	434
Entropy (8bit):	5.153016508305734
Encrypted:	false
SSDEEP:	12:NB+v45KkkGHArqiuFUtpaW/PaHNV5L5KkkGHArq2J:N245KkkGgCgsL5KkkGg7
MD5:	7150F8DA7A9022134E9F09E0AA4ADF39
SHA1:	3E0A6C3CAB4A2E9E2F787CFC670A663F87F1C2D3
SHA-256:	7EA04571BC7C05F17AE58E3104919301B1CB8BAC51994A6F31E9747E46CD78AF
SHA-512:	950A9FB882BD0885397A3489F646A6D9669C03D808634CA02058EDC036F50E1031BD3E82308020AED20725270EB76D592DEF01C3D1FE3769DF4D2B9262EB474E
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:56:02.517 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/01/13-20:56:02.520 16cc Recovering log #3.2021/01/13-20:56:02.521 16cc Reusing old log C:\Users\user\AppData\Lo cal\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
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):	420
Entropy (8bit):	5.2021920853169155
Encrypted:	false
SSDEEP:	6:mM+q2P923iKKdKkGckArZQMxIFUtptdHZmwPINVkwO923iKKdKkGckArZQMFLJ:gv45KkkGHArAFUtpL/P05L5KkkGHArfJ
MD5:	295736AF4197A1DA2BA8237E24477D0C
SHA1:	990C0CC1B756742FA564ADCDAD8A288B31BA32AC
SHA-256:	56FEC67B6A38562531C15968D561F889D0C2DE9D389E0D97418268568DAD4592
SHA-512:	41F3BC354639B097FD566589F77328AB5191DAAA63D8444D47B794B3821D874B0E2A70D72E005344819F4A8D5AFF677F2F139D1B729BA761FADB676C2B2E90EC
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:56:18.339 1708 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/01/13-20:56:18.342 1708 Recovering log #3.2021/01/13-20:56:18.343 1708 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\bdad2fd6-408b-4556-8bae-461793d5ebe2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FB 27
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isol ation":[],"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:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Size (bytes):	323
Entropy (8bit):	5.177031961655166
Encrypted:	false
SSDEEP:	6:m7hq2P923iKKdKpIFUtp0tZZmwP0tzkwO923iKKdKa/WLJ:6v45KkmFUtpQ/PY5L5KkaUJ
MD5:	CC375C7D41D290928C97669288FB9006
SHA1:	6D13DB4AD7A8C2BF7FD5EB65C7B9907ED435C690
SHA-256:	8F6A25916A12B7E0EA9654F3EE39B0C20934ECCC9E94CB2D3C379B4CFC246300
SHA-512:	2AE01F021CA509E1B87FA538BAFEFBF62C1C4AFB05B80F0062E6DC97277B1F52B1A6B63AE6923A2B41D6FFF9AA3B1EFB7342DCD744807802DDF6EED4D3B5C8E9
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:55:53.891 920 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/01/13-20:55:53.892 920 Recovering log #3.2021/01/13-20:55:53.892 920 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):	404
Entropy (8bit):	5.273841198337458
Encrypted:	false
SSDEEP:	6:mDgb2+q2P923iKKdKks8Y5JKKhdIFUtp4gwaZmwP4gAVkwO923iKKdKks8Y5JKKp:v3v45KkkOrsFUtp7/PE5L5KkkOrzJ
MD5:	7E8F7996DFB8440C82A638809809D4AB
SHA1:	D7F4FB3CFF7F83E5A958437E39B932EBAB96C930
SHA-256:	ABEBACA16D7CD59334D246067DA9543B18A41C228395470578DBD7D018FE454F
SHA-512:	27D9610577ECEE24A925548E2CA8BB5F04EFD6FEE9A90720C3FDFAC367FBD7250CDB7F1AC50373CD9B99FED89D8146E4A31B94E76AF517AA90E1E3B57628B5EC
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:56:05.105 1708 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/01/13-20:56:05.106 1708 Recovering log #3.2021/01/13-20:56:05.107 1708 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):	3.855388542207535
Encrypted:	false
SSDEEP:	3:O81ntM:B1nK
MD5:	EF39FEA966ADAB6256EF573F8A915647
SHA1:	1C0774CB183E2D7660B068C25BE76DB799D59480
SHA-256:	6ED30F39FFB8467C10807E9AB28FE802E530513CB45B388566F1FAD51EDDD846
SHA-512:	E64BAEA4CE6D03A8D134991B4D774F4336A901BCCF2907C1A4A0BBC881FE711C62934CCA3C94C7DC3558D26E85B59B83DEC545C3BB3D3D34A0E96B18B4702FC
Malicious:	false
Reputation:	low
Preview:	....*J.].OBA....W...<.'

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c994d97f-ccd6-473e-afd1-746cf7dc7884.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):	5617
Entropy (8bit):	5.187699637233347
Encrypted:	false
SSDEEP:	96:n4nrFlr4Cg3XZSVbIk0JCKL8gkXjrXbOTQVuwn:n4nrl4CgZSJC4KFkX7
MD5:	DBA666C7D7E8C74F481D16A97093C594
SHA1:	D48A3412B350310558366AF4E1C2A9F5CD7E3F93
SHA-256:	76736F920B48BCE971C472C2B087C184E523326C101E974505FAD6F0A9A8B5DD
SHA-512:	1BF4E1840F611EC660EAE67B8657A6EB0CD1D9FD8308A83598FD594496E359D045514CD45A34AC56E5AB3EDCC1088452BECA0FF9B9E5AB2EC5C7949F7F617DC1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c994d97f-ccd6-473e-afd1-746cf7dc7884.tmp	
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13255073754188032","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","0","0","0","0","1538886"],"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","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d2e21dc1-f53e-4f3e-ace5-de2189d12ee8.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):	22614
Entropy (8bit):	5.5355381994738915
Encrypted:	false
SSDEEP:	384:29DtBLlv4XN1kXqKf/pUZNCgVLH2HfDLTrUXHG1nTKGacPAUgxj4B:eLlKN1kXqKf/pUZNCgVLH2HfzrU3G1nb
MD5:	D6D4BDAF08BF4AC2E484446DC923A981
SHA1:	9068FD913350F4675C870A7B416EA1ADE7C413CC
SHA-256:	1E0F71DFC644E8255951C4F2EE6EAE94C2809EC59D91779F555612F5990ABF0C
SHA-512:	A4E171AC783D2048AE012D28D20A1D4B6840B49C5C216967DB424668B8585F517C235EB1335497319E402A46F56B7ECDEEF0DE52C66D0F1477C5BBA881AADF
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":"13255073753891350","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\d452acba-5d11-483f-8d58-b71a6434702e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2588
Entropy (8bit):	4.894451450042645
Encrypted:	false
SSDEEP:	48:Y2ntwTXDHz5sCRLsGTsBTA2JYsryKs13q7shtkqzs9MH3swMHygYhbxD:JnOTXDHzZFt2VMa+tjUGhGKhVD
MD5:	77AD69263AC4DC6C586842D6C16F8763
SHA1:	89BECBD912900ACBF40BE22610A6052640A8ACB1
SHA-256:	C7CB01A77340D6253DA29B5CE2346D7E74070FCC09D5C8BCCBF6B076EBB5B378
SHA-512:	2273885B8CA5C5693BB4D7289745719FE7915A103B3FAEA7E3CCB599332AA0DDA4F2B0565CA9E54B7EB4670845645D6F6B19F3E9068F70361D1AAD366F8DA7D
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13257665756952729","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13257665756991759","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13257665757327362","port":443,"protocol_str":"quic"},{"advertised_

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
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):	4.270365519653835
Encrypted:	false
SSDEEP:	3:tUKqJHUjhZmwv3sJDUHeJ01V8ssJZNHVkJ01WGv:mHHUjhZmwP8DUHW0Vv8ZVW0tv
MD5:	4CFECDF83267A25A4735F04141BB06D5
SHA1:	2EBCD9D8F99CE070A2D68F10623D36AA6B154865
SHA-256:	377D758D7D6A44C4E548AEBA18318FF556E69AB3B47D3E506EC89B94A2E050DC
SHA-512:	6284641DA87AB57381819AC746E8EB6D29164E688DA55C95CF2DF8A4EAD80A6A3AC627D3FD47A3BA1224D66F38E00A665EAE03F25EBCCD5FFF299621B226A57
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:56:01.041 11b0 Recovering log #3.2021/01/13-20:56:01.102 11b0 Delete type=0 #3.2021/01/13-20:56:01.103 11b0 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/vxQRDKlVmt+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\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.214038381821327
Encrypted:	false
SSDEEP:	6:mIY2+q2P923iKKdKfrzAdIFUtpVy+ZZmwPVKVkwO923iKKdKfrzILJ:FY3v45Kk9FUtpVy+Z/PVi5L5Kk2J
MD5:	D4F46509225DEDBBCE5C259268F18FFC
SHA1:	8DF72F2CE8D6E27E4969E5D37BEF723675A384E0
SHA-256:	32A6DFA62A37C480826466D9F8E96BD37B9BDC968F2AC1AC98628052892CC485
SHA-512:	E190D7791AB67DE3C73171F9DCE7B61C0AE45F28B133D7F726D7DDC5BBF96E1978DAC511F6C2065666F6F40850962BD93089220643E00E79D8D50A5BFF35165
Malicious:	false
Reputation:	low
Preview:	2021/01/13-20:56:04.242 1708 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/01/13-20:56:04.248 1708 Recovering log #3.2021/01/13-20:56:04.249 1708 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:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\b095727c-fd78-4874-ab0d-3441cbd83c2f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7455121716213378
Encrypted:	false
SSDEEP:	384:pbW5dDcWPEjbVYeF4NNr+vRb36djiHz+GuRr8/h9xiXPfOrMBmMv87V5FGOjjZNU:ZaS9tKPaOUePVb70PrGTKBvNJ4
MD5:	0CC60B82BF07A60AC00F94B3383F4283
SHA1:	A8B55F9044BF3A0AB3388191DF9828FFA833BFBF
SHA-256:	683E37F6F4DF3063AEEE41B082628E2FFD15C60D13991BF61783024B8E3900ED
SHA-512:	3686AB0FAD57FCC90B1BE77C5EAAF40ED3A6D4B5E9A6BFF493B09633F94CC31FADD255F1CF5F8C315CF9E513835F22121AC1554E799FCA71F6F56F8A06F75CD2
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n.....8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\b66f082d-c598-46eb-bc01-327c092ba43c.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):	354272
Entropy (8bit):	6.015577811203153
Encrypted:	false
SSDEEP:	6144:DmS5B8+wcw1fph3A8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBc:KAdrw53VxzurRDn9nfNxF4ijZVtilBc
MD5:	E1B330AEEEB84915C168BCF00BA253F8
SHA1:	5F7430478EFC1B2FF9A1566A51EA4C455E7BF864
SHA-256:	E0A5346F9FB0361F4629172584276E85EC39117580B9EFB6E45A565A954FE883
SHA-512:	93D4C738FA3A8210BEF033F6FD671575A2A247BA3A608728589C77B9F540178FAFB1F365AE2049CD766DBE66C257B4797F16364A8B87F82777DA0A4C3BE37363
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\b66f082d-c598-46eb-bc01-327c092ba43c.tmp	
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":1.610600157026458e+12,"network":1.610567758e+12,"ticks":110979301.0,"uncertainty":4391482.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13255073753779

C:\Users\user\AppData\Local\Google\Chrome\User Data\cf87303f-5fec-41d2-9a2e-8fa0829ce26c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	95428
Entropy (8bit):	3.7451199805219293
Encrypted:	false
SSDEEP:	384:ZbW5dDcWPEjbVYeF4NNr+vRb36djiHz+GuRr8/h9xiXPfOrMBmMYK87V5FGOjjZi:paS9tKP0OUePVb70PrGTKBvNJU
MD5:	EC0A00F1455D42FD3442E821EC7F48B6
SHA1:	FF58EB1162B38FF5D3F3E5B49851F96BA1A3BBA9
SHA-256:	31E5C544FB3715458DE0AC5F8E80B61343B1FED99513F88737CABC5430C74EB8
SHA-512:	03177C2D595DC7AF38E7C822A16ADCC168E52F83923F0DD390ADF9978CD721BC82E1B9881AC1AAC184966997A9CE8C4C99E8CBDDA04EBBFC57FBD047C44F24B
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n.....8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\d38facbe-5961-42ee-b798-419492f19c7d.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):	354272
Entropy (8bit):	6.015577704055423
Encrypted:	false
SSDEEP:	6144:omS5B8+wcw1fph3A8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBc:VAdrw53VxzurRDn9nfNxF4ijZVtilBc
MD5:	A315DAB58CDA97F4734B1E93FC1D0932
SHA1:	7344E8CF5B61F972B4804707CAC16FD4A9A65197
SHA-256:	5B021BB3CAA51B873441D8C74061513C0C0F274E0E3D4F48F9793D0B0332A2BE
SHA-512:	9F8B61393F139997F3E21B436333D23C9D683D1FD9E40FB8DC84408DE1ED15FCEC857E3F16955B1F6DBE01412F43CDD8C6ADF3588FD93B08441CEBC231727F
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":1.610600157026458e+12,"network":1.610567758e+12,"ticks":110979301.0,"uncertainty":4391482.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075927485"},"policy":{"last_statistics_update":"13255073753779

C:\Users\user\AppData\Local\Temp\0f2d04d3-4475-49e5-b1ac-96a96beff08d.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

C:\Users\user\AppData\Local\Temp\0f2d04d3-4475-49e5-b1ac-96a96beff08d.tmp	
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\240e5f93-2001-466c-99ae-667c915ed273.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	300953
Entropy (8bit):	7.973503294353402
Encrypted:	false
SSDEEP:	6144:0sb1v/4nxPbqqBbWbFsw+wh3bC5NFv++S/hup0XcaxlnJ9:7l/4nxPZbOFsw+y3d+S6WnX
MD5:	1FE8E0AEB768437A23CEEAE6053E5822
SHA1:	5529A275644B729009E22035F6125879450F4ABB
SHA-256:	25A2F515CEC98CF2ACF11B34C59723D76820A4B5734E223D7EBEA55E5A851468
SHA-512:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA56812320
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.....L.18..Y.~..%...~._.....O\..p,...eY.0=.!..+.SoZA7...:t.G...VZ<..d....MN.....T..{1\.T...P,...i...NrD...e.2..u....5.....1.n.Zu.E...!..XR..j.:.E.gUw.-s7:T.c_...(.i..iU.).M=yF<..`.....F...@)..IK.. b.4.o..mC'...N.*@OtT...`.&|.8.M;.....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.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....RI.G.,2.....[..T'.....".ct.).s#.(/.D..C..4..RKf.W....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...H0F.!...L..\.j.1.d.....==v.....-

C:\Users\user\AppData\Local\Temp\2a3906bb-2838-47a7-8284-5e92ea94bebc.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\f3aee009-0c6e-477d-a739-8473eb6f0250.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_dir3272_125736234\0f2d04d3-4475-49e5-b1ac-96a96beff08d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\0f2d04d3-4475-49e5-b1ac-96a96beff08d.tmp	
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.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\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:	{.. "1018984561488520517": {.. "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_dir3272_125736234\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
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_dir3272_125736234\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

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\CRX_INSTALL_locales\bg\messages.json	
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 Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\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:lPswlWtoK8xfG6uml
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_dir3272_125736234\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
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_dir3272_125736234\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

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\CRX_INSTALL_locales\cs\messages.json	
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_dir3272_125736234\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".. },.. "152214068331 8860351": {.. "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_dir3272_125736234\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
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_dir3272_125736234\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

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\CRX_INSTALL_locales\el\messages.json	
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_dir3272_125736234\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:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+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_dir3272_125736234\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
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas descr ibe 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_dir3272_125736234\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 6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\CRX_INSTALL_locales\et\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": "Hangub".. },.. "12139579827238759 20": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "12827687646031907 5": {.. "message": "Seadme tuvastamine".. },.. "14284488690781267 31": {.. "message": "Video sujuvus".. },.. "152 21406833188603 51": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "15509040647108289 58": {.. "message": ".htlane".. },.. "163668674768 7494376": {.. "message": "T.iuslik".. },.. "18027627465894571 77": {.. "message": "Helitugevus".. },.. "18503975003120203 88": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "conte nt": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\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:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF371 95
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".... ... .".. },.. "12139579827238759 20": {.. "message": ".... .. ..".. },.. "128 27687646031907 5": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "....".. },.. "16366867476874963 76": {.. "message": "....".. },.. "18027627465894571 77": {.. "message": "..... ...".. },.. "18503975003120203 88": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPA N$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\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:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A5261952050 21
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Pys.htyy".. },.. "12139579827238759 20": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "12827687646031907 5": {.. "message": "Laitteiden tunnistaminen".. },.. "14284488690781267 31": {.. "message": "Videon tasaisuus".. },.. "15221406833188 60351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "15509040647108289 58": {.. "message": "Tasainen".. },.. "16366867476874963 76": {.. "message": "T.ydellinen".. },.. "18027627465894571 77": {.. "message": "..nenvoimakkuus".. },.. "18503975003120203 88": {.. "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_dir3272_125736234\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

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\CRX_INSTALL_locales\fil\messages.json	
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-smooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "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_dir3272_125736234\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:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51B
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".. },.. "1636686747687494376": {.. "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_dir3272_125736234\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
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\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:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\CRX_INSTALL_locales\hr\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):	15507
Entropy (8bit):	5.290847699527565
Encrypted:	false
SSDEEP:	192:Pdapr6h85tRwVQgkvJryLkla5Kfndg/V6c8TEKdl:Arwot2Q7BryVce/V6uml
MD5:	3ED90E66789927D80B42346BB431431E
SHA1:	2B061E3271DF4255B1FFC47BDB207CDEC0D9724F
SHA-256:	0B41E3C42414F72C9A12C05F8772597F9685115366A774C66018467AD4B71A74
SHA-512:	92BE43F1FFC8EFBF5BBC50573AC4C65F6104416A5B6CD04404C3A9854CA3DCF2A43A4044C168590CDF83887D234495843572331ADCD5B020D2E48A3956F3C16
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Zamrzavanje".. },.. "1213957982723875920": {.. "message": "Koje od sljede.eg najbolje opisuje va.u mre.u?".. },.. "128276876460319075": {.. "message": "Otkrivanje ure.aja".. },.. "1428448869078126731": {.. "message": "Ujedna.enost videoreprodukcije".. },.. "1522140683318860351": {.. "message": "Povezivanje nije uspjelo. Poku.ajte ponovo.".. },.. "1550904064710828958": {.. "message": "Glatko".. },.. "1636686747687494376": {.. "message": "Savr.ena".. },.. "1802762746589457177": {.. "message": "Glasno.a".. },.. "1850397500312020388": {.. "message": "Vidite li svoj Chromecast u $START_LINK$aplikaciji 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_dir3272_125736234\CRX_INSTALL_locales\hu\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):	15682
Entropy (8bit):	5.354505633120392
Encrypted:	false
SSDEEP:	192:CCEAproS9fZv+JwkDMrC2NSxoSgbV6c8TEKdl:5r5VZv+RDMrazoV6uml
MD5:	8E9FF7E49473C5734A2F6F0812E12EB3
SHA1:	A4F10DDD1580582533D5EB59EDF6D8048F887C81
SHA-256:	6CDD2FB39ADECE00E88B989E464B05ED1414092D0492F6D0AE58D549BFD1A46A
SHA-512:	E9A4AF31B1A276F395599BB620A3164CABF3459F3C102DD3F57DFEA734510BD985DE65CB409E1975559ACCC615075439A08E1DEBE22C90A0ABCAA3CAFEE79AC7
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Lefagy".. },.. "1213957982723875920": {.. "message": "Az al.bbiak k.z.l melyik jellemzi legjobban h.l.zat.t?".. },.. "128276876460319075": {.. "message": "Eszk.zfelfedez.s".. },.. "1428448869078126731": {.. "message": "Vide. folyamatoss.ga".. },.. "1522140683318860351": {.. "message": "Sikertelen kapcsol.d.s. K.rj.k, pr.b.lja .jra.".. },.. "1550904064710828958": {.. "message": "Folyamatos".. },.. "1636686747687494376": {.. "message": "T.k.letes".. },.. "1802762746589457177": {.. "message": "Hanger.".. },.. "1850397500312020388": {.. "message": "L.tja a Chromecastot a $START_LINK$Google Home alkalmaz.sbanEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\CRX_INSTALL_locales\id\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):	15070
Entropy (8bit):	5.190057470347349
Encrypted:	false
SSDEEP:	192:GsprMtChjkWfrEWL0KRCnEOWV6c8TEKdl:9rtAEr3LTRuWV6uml
MD5:	7ADF9F2048944821F93879336EB61A78
SHA1:	C3DA74FB544684D5B250767BB0CB66FFB7C58963
SHA-256:	3630947E1075E3663AD3E4824D0BE42CB47C0D615D8053E83B9595047C8BA9BE
SHA-512:	1F28BB80E1839C5581106BEA3AE2501C7618249D7E3115819F5A9A87771D59F5DE346C1B9C87F7FFC390604D5B9888CE738E25F2F04A094002A0FB3B22CBEC95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Membeku".. },.. "1213957982723875920": {.. "message": "Dari berikut ini, manakah yang paling mendeskripsikan jaringan Anda?".. },.. "128276876460319075": {.. "message": "Penemuan Perangkat".. },.. "1428448869078126731": {.. "message": "Kelancaran Video".. },.. "1522140683318860351": {.. "message": "Sambungan gagal. Coba lagi.".. },.. "1550904064710828958": {.. "message": "Lancar".. },.. "1636686747687494376": {.. "message": "Sempurna".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Bisakah Anda melihat Chromecast di $START_LINK$aplikasi 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_dir3272_125736234\CRX_INSTALL_locales\it\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

C:\Users\user\AppData\Local\Temp\scoped_dir3272_125736234\CRX_INSTALL_locales\it\messages.json	
Size (bytes):	15256
Entropy (8bit):	5.210663765771143
Encrypted:	false
SSDEEP:	192:lYprk52dAaykVza8rE0QWBKD9+vq0hKEV6c8TEKdl:qrlA8r6DalV6uml
MD5:	BB3041A2B485B900F623E57459AE698A
SHA1:	502F5EA89F9FB0287E864B240EA39889D72053A4
SHA-256:	025737EF8FA06706B3F26D0F52B4844244A6D33DAE1D82FEF2931A14C003D57E
SHA-512:	BA51784073BEF82F3A116B33DA406FDB10EC823B9EE74375C46036DAD8BDCB4141F60845DE141ABE42CEEF9251572F6AB287CA5FC7669C60E4F68071D5AB8CD
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Si blocca".. },.. "1213957982723875920": {.. "message": "Quale delle seguenti definizioni descrive meglio la tua rete?".. },.. "128276876460319075": {.. "message": "Rilevamento dispositivi".. },.. "1428448869078126731": {.. "message": "Uniformit. video".. },.. "1522140683318860351": {.. "message": "Connessione non riuscita. Riprova.".. },.. "1550904064710828958": {.. "message": "Fluido".. },.. "1636686747687494376": {.. "message": "Perfetta".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Riesci a vedere il tuo dispositivo Chromecast nell'$START_LINK$app 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_dir3272_125736234\CRX_INSTALL_locales\ja\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):	16519
Entropy (8bit):	5.675556017051063
Encrypted:	false
SSDEEP:	192:nkprPhQdxkRWrZe1wYpMR5wnAV6c8TEKdl:YrLRWri65wAV6uml
MD5:	6F2CC1A6B258DF45F519BA24149FABDC
SHA1:	8A58C7880C6D22765DCBB6BCE22A192C1B109AE1
SHA-256:	42ECFEE727CFC4F2845FEFDACE5EDC2E0A40AFAD69973A3B950CE653A7633342
SHA-512:	F7454F0E14301C59CC54361ACC0A1C6D072EF9BDF5DEA60646FB90B1CE47612785938C784A4CF1DE3E62648A14420374933B5F5DA43907BC00D3799FF163A3D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "...".. },.. "1213957982723875920": {.. "message": "..............".. },.. "128276876460319075": {.. "message": "......".. },.. "1428448869078126731": {.. "message": ".......".. },.. "1522140683318860351": {.. "message": "..........".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..".. },.. "1850397500312020388": {.. "message": "$START_LINK$Google Home ...END_LINK. Chromecast .....$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 70

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:55:56.865417957 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:56.910986900 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:56.914350986 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:56.914386034 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:56.960834026 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:56.964667082 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:56.964685917 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:56.964764118 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:56.964762926 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:56.967715979 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:56.967792034 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:56.967833042 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.039886951 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.272386074 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.272660017 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.273478985 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.317560911 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.317780018 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.317811012 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.318496943 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.320297003 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.368164062 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.870825052 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.870874882 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.870939016 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.870991945 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.871031046 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.871113062 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.872239113 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.872307062 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.872379065 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.873579025 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.873686075 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.873783112 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.874937057 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.874978065 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.875034094 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.876377106 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.876422882 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.876475096 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.877702951 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.877752066 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.877810955 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.879075050 CET	443	49716	13.224.94.105	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:55:57.879116058 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.879209042 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.880439043 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.880477905 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.880534887 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.881820917 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.881867886 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.881922960 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.883130074 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.883161068 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.883224010 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.884562016 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.884613991 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.884670019 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.885891914 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.938497066 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.955202103 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.955228090 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.955307007 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.955884933 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.955910921 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.955986977 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.957267046 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.957289934 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.957366943 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.958765030 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.958853960 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.958935022 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.960022926 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.960047007 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.960133076 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.961358070 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.961397886 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.961466074 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.962819099 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.962882996 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.962939978 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.964128971 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.964168072 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.964246988 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.965475082 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.965516090 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.965579033 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.966820955 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.966856956 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.966922045 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.968214989 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.968244076 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.968290091 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.969546080 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.969577074 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.969645023 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.970937014 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.970966101 CET	443	49716	13.224.94.105	192.168.2.5
Jan 13, 2021 20:55:57.971026897 CET	49716	443	192.168.2.5	13.224.94.105
Jan 13, 2021 20:55:57.972291946 CET	443	49716	13.224.94.105	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:55:51.416373014 CET	59596	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:51.464235067 CET	53	59596	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:52.794713020 CET	65296	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:52.845540047 CET	53	65296	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:55:54.832036972 CET	63183	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:54.880525112 CET	53	63183	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:56.795655966 CET	55161	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:56.797029972 CET	54757	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:56.800446987 CET	49992	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:56.801455021 CET	60075	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:56.859059095 CET	53	54757	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:56.862952948 CET	53	55161	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:56.867229939 CET	53	49992	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:56.868662119 CET	53	60075	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:57.388778925 CET	55016	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:57.445533037 CET	53	55016	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:57.599886894 CET	64345	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:57.658449888 CET	53	64345	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:57.951277018 CET	54791	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:57.952179909 CET	50463	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:58.009948969 CET	53	54791	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:58.011219025 CET	53	50463	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:58.269102097 CET	50394	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:58.269807100 CET	58530	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:58.316868067 CET	53	50394	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:58.334175110 CET	53	58530	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:58.746040106 CET	53813	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:58.750673056 CET	63732	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:58.814841986 CET	53	63732	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:58.815296888 CET	53	53813	8.8.8.8	192.168.2.5
Jan 13, 2021 20:55:59.397150993 CET	57344	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:55:59.473103046 CET	53	57344	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:01.604039907 CET	59413	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:01.673612118 CET	53	59413	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:05.262548923 CET	65086	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:05.319055080 CET	53	65086	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:13.578809023 CET	52929	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:13.626662970 CET	53	52929	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:14.802814007 CET	64317	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:14.859282017 CET	53	64317	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:15.365431070 CET	61004	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:15.421689987 CET	53	61004	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:25.598354101 CET	56895	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:25.646361113 CET	53	56895	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:30.388475895 CET	62372	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:30.436461926 CET	53	62372	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:31.735219955 CET	61515	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:31.791493893 CET	53	61515	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:36.290435076 CET	56675	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:36.341281891 CET	53	56675	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:37.168318033 CET	57172	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:37.216274977 CET	53	57172	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:41.196103096 CET	50969	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:41.254501104 CET	53	50969	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:46.222822905 CET	64362	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:46.272562027 CET	53	64362	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:55.213690042 CET	54766	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:55.272732973 CET	53	54766	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:55.790580034 CET	57515	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:55.851315975 CET	53	57515	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:55.921040058 CET	58199	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:55.977623940 CET	53	58199	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:56.153187990 CET	65221	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:56.217775106 CET	53	65221	8.8.8.8	192.168.2.5
Jan 13, 2021 20:56:56.342304945 CET	61573	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:56:56.401688099 CET	53	61573	8.8.8.8	192.168.2.5
Jan 13, 2021 20:57:10.367698908 CET	56562	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:57:10.438997984 CET	53	56562	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 20:55:56.797029972 CET	192.168.2.5	8.8.8.8	0x8717	Standard query (0)	survey.alchemer.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:57.951277018 CET	192.168.2.5	8.8.8.8	0xb83c	Standard query (0)	www.surveygizmo.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:58.269807100 CET	192.168.2.5	8.8.8.8	0xd540	Standard query (0)	surveygizmolibrary.s3.amazonaws.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:59.397150993 CET	192.168.2.5	8.8.8.8	0xf2d6	Standard query (0)	www.alchemer.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:56:01.604039907 CET	192.168.2.5	8.8.8.8	0xe462	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
Jan 13, 2021 20:55:56.859059095 CET	8.8.8.8	192.168.2.5	0x8717	No error (0)	survey.alchemer.com		13.224.94.105	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:56.859059095 CET	8.8.8.8	192.168.2.5	0x8717	No error (0)	survey.alchemer.com		13.224.94.15	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:56.859059095 CET	8.8.8.8	192.168.2.5	0x8717	No error (0)	survey.alchemer.com		13.224.94.11	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:56.859059095 CET	8.8.8.8	192.168.2.5	0x8717	No error (0)	survey.alchemer.com		13.224.94.69	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:58.009948969 CET	8.8.8.8	192.168.2.5	0xb83c	No error (0)	www.surveygizmo.com	d3gvv5iecquak.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:55:58.009948969 CET	8.8.8.8	192.168.2.5	0xb83c	No error (0)	d3gvv5iecquak.cloudfront.net		13.224.94.66	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:58.009948969 CET	8.8.8.8	192.168.2.5	0xb83c	No error (0)	d3gvv5iecquak.cloudfront.net		13.224.94.43	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:58.009948969 CET	8.8.8.8	192.168.2.5	0xb83c	No error (0)	d3gvv5iecquak.cloudfront.net		13.224.94.112	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:58.009948969 CET	8.8.8.8	192.168.2.5	0xb83c	No error (0)	d3gvv5iecquak.cloudfront.net		13.224.94.106	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:58.334175110 CET	8.8.8.8	192.168.2.5	0xd540	No error (0)	surveygizmolibrary.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:55:58.334175110 CET	8.8.8.8	192.168.2.5	0xd540	No error (0)	s3-1-w.amazonaws.com		52.217.0.180	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:59.473103046 CET	8.8.8.8	192.168.2.5	0xf2d6	No error (0)	www.alchemer.com	alchemer.wpengine.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:55:59.473103046 CET	8.8.8.8	192.168.2.5	0xf2d6	No error (0)	alchemer.wpengine.com	lbmaster-96142.wpengine.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:55:59.473103046 CET	8.8.8.8	192.168.2.5	0xf2d6	No error (0)	lbmaster-96142.wpengine.com	cluster96-elbwpeel-u8fat1y76lys-241867217.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:55:59.473103046 CET	8.8.8.8	192.168.2.5	0xf2d6	No error (0)	cluster96-elbwpeel-u8fat1y76lys-241867217.us-east-2.elb.amazonaws.com		18.221.77.186	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:59.473103046 CET	8.8.8.8	192.168.2.5	0xf2d6	No error (0)	cluster96-elbwpeel-u8fat1y76lys-241867217.us-east-2.elb.amazonaws.com		3.21.157.39	A (IP address)	IN (0x0001)
Jan 13, 2021 20:56:01.673612118 CET	8.8.8.8	192.168.2.5	0xe462	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 20:56:01.673612118 CET	8.8.8.8	192.168.2.5	0xe462	No error (0)	googlehosted.l.googleusercontent.com		108.177.126.132	A (IP address)	IN (0x0001)

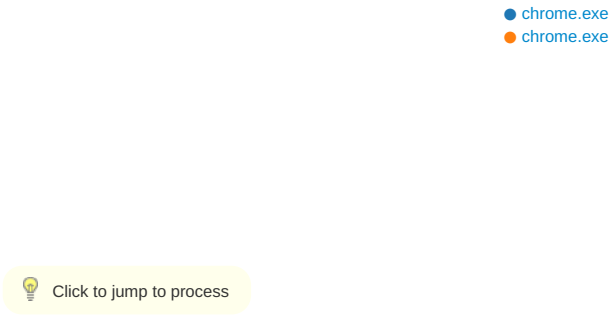
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 13, 2021 20:55:58.592039108 CET	52.217.0.180	443	192.168.2.5	49731	CN=*.s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Nov 09 01:00:00 CET 2019 Tue Dec 08 13:05:07 CET 2015	Fri Mar 12 13:00:00 CET 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 3272 Parent PID: 2940

General

Start time:	20:55:53
Start date:	13/01/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://survey.alchemer.com/s3/6136192/COVID-Impact-Survey-FINAL'
Imagebase:	0x7ff677c70000
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: 5912 Parent PID: 3272

General

Start time:	20:55:54
Start date:	13/01/2021
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=1556,552184152371578541934561775035776713 3,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1692 /prefetch:8
Imagebase:	0x7ff677c70000
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	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly