ID: 392873
Sample Name: OA46809.htm
Cookbook: default.jbs
Time: 23:17:37
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

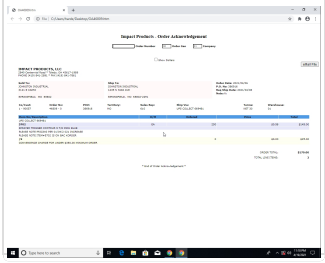
Analysis Report OA46809.htm

Overview

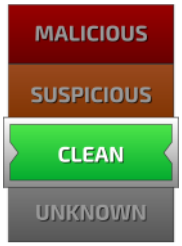
General Information

Sample Name:	OA46809.htm
Analysis ID:	392873
MD5:	170db7cf0e97b8e.
SHA1:	1f67ca780887d2c..
SHA256:	f7d6248230338ad.
Infos:	

Most interesting Screenshot:



Detection

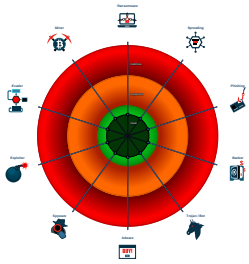


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5364 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\OA46809.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6260 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1580,3607684188885310936,9111398575048557525,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1688 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

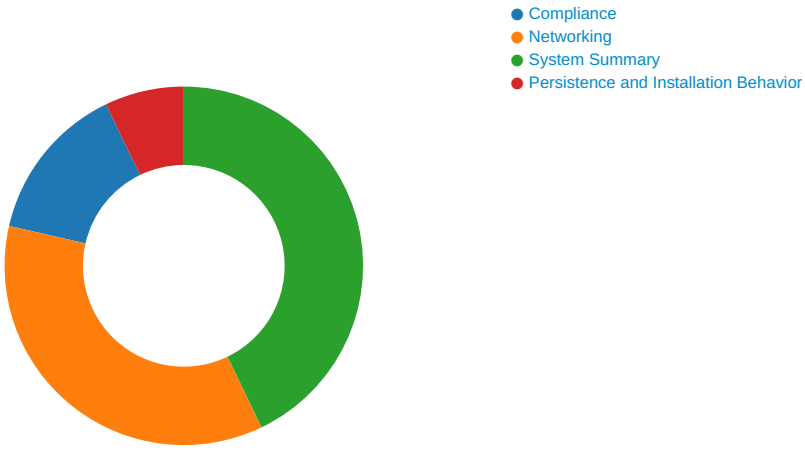
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



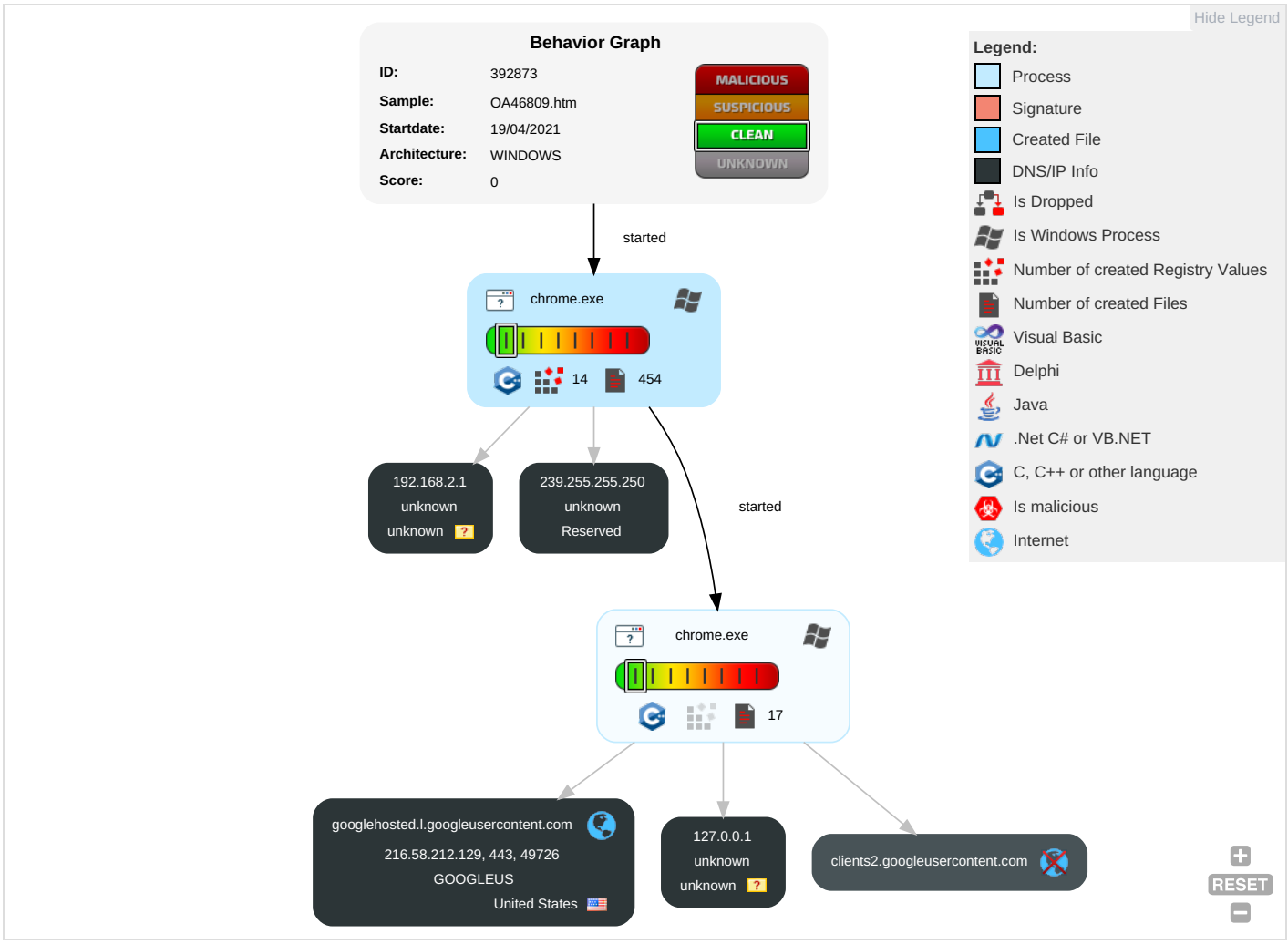
Click to jump to signature section

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

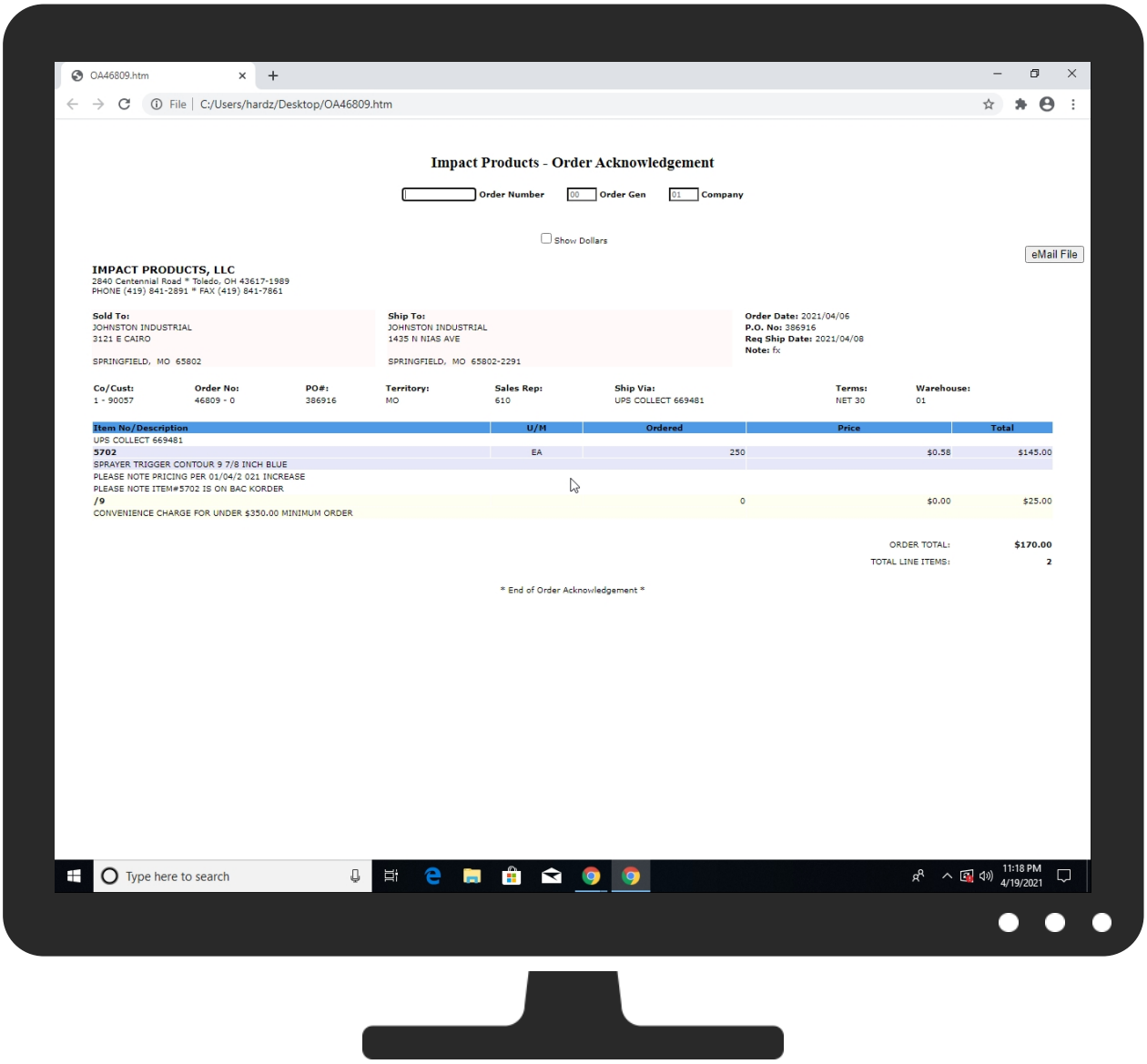
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/OA46809.htm	false		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	488ec301-c88e-4e13-8057-de7c725ac4ed.tmp.1.dr, 5dc5cbe9-51c1-414a-9182-47d0960e7cda.tmp.1.dr, 385dc898-cca1-41fe-8fc0-2b1ae56929ed.tmp.1.dr, babd0dbe-6725-43c6-8e60-70a56a1920b4.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients2.googleusercontent.com	488ec301-c88e-4e13-8057-de7c725ac4ed.tmp.1.dr, 385dc898-cca1-41fe-8fc0-2b1ae56929ed.tmp.1.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392873
Start date:	19.04.2021
Start time:	23:17:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OA46809.htm
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winHTM@35/177@1/4
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 20.82.209.183, 204.79.197.200, 13.107.21.200, 93.184.220.29, 13.88.21.125, 52.147.198.201, 2.20.86.117, 13.64.90.137, 172.217.18.110, 142.250.185.205, 142.250.185.142, 142.250.186.35, 173.194.187.138, 74.125.13.231, 142.250.185.170, 142.250.185.202, 142.250.185.234, 142.250.185.138, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 172.217.18.106, 172.217.23.106, 216.58.212.138, 142.250.185.74, 172.217.16.138, 104.42.151.234, 40.88.32.150, 168.61.161.212, 20.82.210.154, 23.57.80.111, 92.122.213.194, 92.122.213.247, 93.184.221.240, 142.250.186.131, 142.250.74.195, 173.194.164.170, 20.54.26.129, 173.194.182.200, 74.125.11.25, 20.50.102.62, 173.194.182.102, 173.194.187.70, 173.194.151.107, 74.125.173.137, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, r1---sn-4g5e6nsk.gvt1.com, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, skypedataprdcoleus15.cloudapp.net, clients2.google.com, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, r2---sn-4g5e6nzs.gvt1.com, hlb.apr-52dd2-

0.edgecastdns.net, update.googleapis.com, r3.sn-4g5e6nss.gvt1.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, www.googleapis.com, r5---sn-4g5e6nsy.gvt1.com, r4.sn-4g5edned.gvt1.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, r5---sn-4g5e6ne6.gvt1.com, clients.l.google.com, r1---sn-4g5ednld.gvt1.com, r5.sn-4g5e6ne6.gvt1.com, r3---sn-4g5ednee.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, r4.sn-4g5ednsy.gvt1.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, r4---sn-4g5edned.gvt1.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, redirector.gvt1.com, cs11.wpc.v0cdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, r5.sn-4g5e6nsy.gvt1.com, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, r3---sn-4g5e6nss.gvt1.com, r3.sn-4g5ednee.gvt1.com, r4---sn-4g5ednsy.gvt1.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, r1.sn-4g5ednld.gvt1.com, accounts.google.com, r2.sn-4g5e6nzs.gvt1.com, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, r1.sn-4g5e6nsk.gvt1.com, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
239.255.255.250	VoicePlayback (0195) for turnerrd pellamw .html	Get hash	malicious	Browse	
	Monday, April 19th, 2021, 20210419111136.68B7C9F20FAF4F3F@classactsautobody.com.htm	Get hash	malicious	Browse	
	P A Y M E N T (1).html	Get hash	malicious	Browse	
	This computer is BLOCKED.html	Get hash	malicious	Browse	
	MasterFundDistributions235.html	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	quote_Jroof166.htm	Get hash	malicious	Browse	
	Dobra-Dossin.html	Get hash	malicious	Browse	
	Cocha904.htm	Get hash	malicious	Browse	
	eFax_Sg803.htm	Get hash	malicious	Browse	
	FAKTURA.exe	Get hash	malicious	Browse	
	Play_audio_jharvison@elevate.com_file.htm	Get hash	malicious	Browse	
	File6512365134_7863_20210413.html	Get hash	malicious	Browse	
	BR-169293.htm	Get hash	malicious	Browse	
	scan_745.htm	Get hash	malicious	Browse	
	audio_christine.morris.html	Get hash	malicious	Browse	
	Mike-voip-18388.htm	Get hash	malicious	Browse	
	March Financial Reports & Statements.html	Get hash	malicious	Browse	
	setup-1.exe	Get hash	malicious	Browse	
	scan_715.htm	Get hash	malicious	Browse	
	Document8451.htm	Get hash	malicious	Browse	

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:	moderate, very likely benign file
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\26a15189-df54-4862-b04f-c739166bfb0c.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):	163250
Entropy (8bit):	6.082314245920987

C:\Users\user\AppData\Local\Google\Chrome\User Data\26a15189-df54-4862-b04f-c739166bfb0c.tmp	
Encrypted:	false
SSDEEP:	3072:zTPupswbCSU8AYeuAZFcbXafIB0u1GOJmA3iuRj:vPCDbXDAYtA3aqfIlUOoSiuRj
MD5:	349FE3395B4F9A5D5FACBF66EEC9CE8A
SHA1:	7675CCBC73B9244323E295D9FBAA389AEA5E94BE
SHA-256:	0D0590DC1F4AD7BF4B7E93436F4229F4A51395A6052F6017E40CA8A0B571E82B
SHA-512:	5DC4D3A036578F98D6264CB6E262A22D9788E1643D71E0319AAA33DDF1323F31471B37B297CFBF7A10B783C90810A630F60A78E8C6D4843531B5904C80F9F695
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":1.618899507361564e+12,"network":1.618867109e+12,"ticks":96379797.0,"uncertainty":5298239.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr 2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1 vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\2c551663-dcd2-42a4-badf-da2bbbe249b0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7436950288892343
Encrypted:	false
SSDEEP:	384:oULxKuwnlYPMyV/xO1Nyr3vm+3NmoBHMpG5wrr4aIxlMoY7rj+mP0bICuu1O8AGo:1G6lRSYtRkeDg6IMfXGiKQuCJa
MD5:	98706A8EC22B766E06BCCC99416787B5
SHA1:	7D8AC2687BBD11B6ADF31F0B5893EC91C9548EBD
SHA-256:	28EA2CABCB716CB9720E01EC126EE05A0D058A9A9536324CC723FA27C1D7DBCF
SHA-512:	BBE095EFE6F8C06876EEAFB71027C1DC166788806EAD769208C2F8AE40E6FE632E7C34328C33441E877EE6FEA7D66C07A876399335F3A16BA2114E6F6BD5BFE 6
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....78.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\32e0aa42-2568-45ce-aea4-5b523f128083.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):	154773
Entropy (8bit):	6.051709653104547
Encrypted:	false
SSDEEP:	3072:8KupswbCSU8AYeuAZFcbXafIB0u1GOJmA3iuRj:pCDbXDAYtA3aqfIlUOoSiuRj
MD5:	99D97D440790141241948684E60D1D2A
SHA1:	6F25CBCE65C0B54C816575BFB273BC073399B579
SHA-256:	45679ED9B10FECED83F011FD44DA9A766C4A970914CB9B0C6024E338F6B486CE
SHA-512:	EEDD6FED13F3EC5F6B1DCF3BF50FC28502F11FBD6682CB367B5C0C98966FF8BC5E9E7CE91592B94EE5A59F531FFC9375C63BB295F17D0F81F0E0D02A475FEE A7
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":1.618899507361564e+12,"network":1.618867109e+12,"ticks":96379797.0,"uncertainty":5298239.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr 2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1 vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016923922"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\33c9b185-af01-40c1-89c4-cfc3ebf2d01f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7432193073931415
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\33c9b185-af01-40c1-89c4-cfc3ebf2d01f.tmp	
SSDEEP:	384:WULxKuwnlMM7O1Nyr3vm+3NmoBHMpG5wrr4aIxlMoY7rj+mP0bICuu1O8AGNP1iX:D6lRSYtRkeDg6IMfXGiKQuCJE
MD5:	656BC78C5585C34F2CACE36D76866779
SHA1:	D4B3E299580DAE4BBB9EEDDB7BAC1175852D06E2
SHA-256:	749A95E267168C4243A180FBD9A945B2B7477E8F7A9000ABEFD4F3C35AE3FC16
SHA-512:	6FC3557C5A9670D63FE187F05C92FDBCEB70623A481EC90348986F6E17BD169B31AFC962E37AEE086EDC3B7F6D9DA425493F0EABA32BB857E09943C09B05C9 6
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....78.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\3828fa0d-4d2e-42a3-9a4f-92a02e9bacd7.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):	154773
Entropy (8bit):	6.051709653104547
Encrypted:	false
SSDEEP:	3072:8KupswbCSU8AYeuAZFcbXafIB0u1GOJmA3iuRj:pCDbXDAYtA3aqfIlUOoSiuRj
MD5:	99D97D4407901412419486 84E60D1D2A
SHA1:	6F25CBCE65C0B54C816575BFB273BC073399B579
SHA-256:	45679ED9B10FECED83F011FD44DA9A766C4A970914CB9B0C6024E338F6B486CE
SHA-512:	EEDD6FED13F3EC5F6B1DCF3BF50FC28502F11FBD6682CB367B5C0C98966FF8BC5E9E7CE91592B94EE5A59F531FFC9375C63BB295F17D0F81F0E0D02A475FEE A7
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":1.618899507361564e+12,"network":1.618867109e+12,"ticks":96379797.0,"uncertainty":5298239.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016923922"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\4405fd5c-4631-4bb3-b453-031bae07109c.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):	155214
Entropy (8bit):	6.053029075034281
Encrypted:	false
SSDEEP:	3072:5gupswbCSU8AYeuAZFcbXafIB0u1GOJmA3iuRj:SCDbXDAYtA3aqfIlUOoSiuRj
MD5:	9C2A76E814D0A7D9D866368FF8235016
SHA1:	ECB5A8F90905DD34910B65D675BE32C0BA889950
SHA-256:	9FBFC7DDEF843E76CF6F6FCF19A2CA0D3D17C51BEAFD6B3A1B84103332CB1221
SHA-512:	69967D79D99AAFE2D229109CBB637B37CA0DA1E60A48D1A5E3ADB78D913DA2CBD5D10126E111394403F649C12681C275E6BBF4FB7A18595C9A17767C5B7A69 8
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":1.618899507361564e+12,"network":1.618867109e+12,"ticks":96379797.0,"uncertainty":5298239.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132

C:\Users\user\AppData\Local\Google\Chrome\User Data\5388489f-446c-4927-9200-c43156313345.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):	155057
Entropy (8bit):	6.0524869513361015
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\5388489f-446c-4927-9200-c43156313345.tmp	
SSDEEP:	3072:RtupswbCSU8AYeuAZFcbXafIB0u1GOJmA3iuRj:PCDbXDAYtA3aqfIlUOoSiuRj
MD5:	01F2C691F3E232EF343FB0C8FD4EB0C2
SHA1:	BD359B065AFBFEF8BF5EF58A0904DEB650E47A3C
SHA-256:	31AE9365A4F20008E4EF86B239B035D03926C527DA736B352AD890EF1D0FDEDE
SHA-512:	8D78E46A5DA4DF872362CFA8F03F473C89FBC747944DCF8AD3394154F7BD57E9097E769E18312BC1D033FF4D1FF50EE058D59CD2E3524626A8480F18578A1416
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":1.618899507361564e+12,"network":1.618867109e+12,"ticks":96379797.0,"uncertainty":5298239.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr 2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1 vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016923922"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\5f1c721c-cd5b-44da-868c-1c42d71a89dc.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):	163250
Entropy (8bit):	6.082313914977102
Encrypted:	false
SSDEEP:	3072:dTPupswbCSU8AYeuAZFcbXafIB0u1GOJmA3iuRj:hPCDbXDAYtA3aqfIlUOoSiuRj
MD5:	2CEF5A91F79DF562D109EA3EA64BDD0D
SHA1:	2D291C4ACF4C2B4D9B83FB7A6F5C320958A6EA67
SHA-256:	6FA19F6BC537DEC2369F515E48AABCBC83048FE95D7FBA09409A8ACFB497F463
SHA-512:	E03305C2189B52C521074085A9F2954FB57E7C81A0344DECB11C0E459DBD09BF977921CC0868844674EBDFA38A57417671DCB8A428D778EF7278C08445902A06
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":1.618899507361564e+12,"network":1.618867109e+12,"ticks":96379797.0,"uncertainty":5298239.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr 2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1 vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016923922"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\385dc898-cca1-41fe-8fc0-2b1ae56929ed.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):	2042
Entropy (8bit):	4.894005990261388
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5s9Ds3TsMARLsj1jQRMs3yKsh3gYhbD:JTnOCXGDHz+qWWBQJlxhH
MD5:	F368A8B7538C4531592F380586445B0A
SHA1:	0DB2F196110A6AA2858366290A9A51791E701C28
SHA-256:	159E77E97EB6245DAA210D37375418861C5A4858DA7BC83775D2EC5A2101BC97
SHA-512:	AF0243506A20F374599C6D3464055B29F395CDDBBE0B3BB5B8723A7F40C6D061CE9D8DE7A04F2EF8282BCFD91B6AEB1D75D0809A7E70E120252D7740AC4B7C8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\385dc898-cca1-41fe-8fc0-2b1ae56929ed.tmp	
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13265965109346459","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13265965109401040","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\488ec301-c88e-4e13-8057-de7c725ac4ed.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4a68b685-09f4-48d3-95e7-d0304d8fce1a.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):	1039
Entropy (8bit):	5.5654772715314555
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvj7wU6HRUenHQ:YI6UUhVseKUewqPeUer2UeffwU6xUenw
MD5:	0D8448957C5FA042C934C6075EA3E89A
SHA1:	D843C2F152D6178E9B7FC1D1C9460AE561817B01
SHA-256:	0CA9E6B49E452F24A503FD2191BC92C29D23EFA27C464ED306CCE9C3A90DF51C
SHA-512:	3C2AC94C392C56B9C004088F587DEC187F5287D976EED1A2BAB9F1C96617E86F6BC037A1079A3EDEC560A7BF0A7777DC3E34368866DDE23525CFACE9E0BE7E39
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1650435509.401781,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1618899509.401785},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\53f9272f-b75d-44c3-add5-f4433d06503b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5b476457-4d21-4c75-876a-79d197c2ad89.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):	5424
Entropy (8bit):	5.190473767733629
Encrypted:	false
SSDEEP:	96:nQ99WFdmf9fhRaScV/ok0JCKL8tbOTQVuwn:nQeqfvRZcw4K2
MD5:	269D9C489F0D4F7204CC1BB4A4460373
SHA1:	5C607563D3260C55EB2EA5ADF411D8B7D4782DE3
SHA-256:	BE68F66D843DF3672B8778D7F7CD57F3C759176C8D4D2EC9692CA6BD13591C43
SHA-512:	4B9FC7C6F1D2950E8CF136A0D5F92AB27CF5F84F8911C4EDE254112795F716636107EC3528DD53C746EF715DD32BA928F50FA4CF1E3B9A5AAFFFB1CD69E439E A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13263373104153251","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\82ea3c9d-b15c-4a7d-ad80-65bf231147d0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535367727791804
Encrypted:	false
SSDEEP:	384:uiyPt8Ll5gXM1kXqKf/pUZNCgVLH2HfDprUPHGuynT6I549:5LlAM1kXqKf/pUZNCgVLH2Hf9rU/Guye
MD5:	DA881123607CA2D7E65BF8AB13ED86E9
SHA1:	1B66220C4E3722450E84D51F8F56FA5595473EC5
SHA-256:	817235A4A5EA5A7206944840670BAF40AA071161F3BC8F912E7DA88120F300FE
SHA-512:	AF984756F804332AE354F4C4132F623CA83BDEB2D65878A382F4845CA04D83C1A003787622289AD2536B863ADA2CB26AF573E1110408E75156D3863E9993DB76
Malicious:	false
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":"13263373103945401","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):	334
Entropy (8bit):	5.238992883454824
Encrypted:	false
SSDEEP:	6:m55Qul4q2PWXp+N23iKKdK9RXXTZIFUtpO5SOJZmwPO5SODkwOWXp+N23iKKdK9l:yBl4va5Kk7XT2FUtpCSOJ/PCSOD5f5KU
MD5:	4709EBA671B7B651C9E6DE1A8593D250
SHA1:	2D6895F8B09FCF2D350422647C8B88C4E33644A0
SHA-256:	93B61D9DEF234C41181D3227B11F8664896D3EFEF124E381C42B8E564995DEA6
SHA-512:	DC5EA0DEC1D661C1A402BF8207685C5658CBC78A02138F0503CF43DC0955344A3B136222F563F0837D584B638B889772666FF8DCCCAE523CFE88A17B179445204
Malicious:	false
Preview:	2021/04/19-23:18:27.285 1820 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/04/19-23:18:27.287 1820 Recovering log #3.2021/04/19-23:18:27.287 1820 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.203670878868281
Encrypted:	false
SSDEEP:	6:m564q2PWXp+N23iKKdKyDZIFUtpO5MlJZmwPO5MlDkwOWXp+N23iKKdKyJLJ:94va5Kk02FUtpCAJ/PCAD5f5KkWJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
MD5:	5CD1FDA2F803DBAC3E0AEF87DB1BD82D
SHA1:	A63DE14ABC8B55B226DFF204C31CA619570F7EA7
SHA-256:	DD809F841532CC3765BB9378CDBC8775C985FE1F32F2875D67F24CDDE0C80882
SHA-512:	1759FFC83AC0418970698606FC511E801B03F88F878B6CA67CBE84B74468F8E8186D5F3F452616081C1EACB48D1B25F39496807AF9EC3288B2CFC1123FAEA759
Malicious:	false
Preview:	2021/04/19-23:18:27.279 1820 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/04/19-23:18:27.280 1820 Recovering log #3.2021/04/19-23:18:27.280 1820 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\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9680152534654619
Encrypted:	false
SSDEEP:	24:MrcLgAZOZD/rqLbJLbXaFpEO5bNmISHn06Uwm8:Mr8NOZrq5LLOpEO5J/Kn7Up8
MD5:	0F169C62949D5EADF60457E4D7BD9200
SHA1:	54ECCB941DFF67A648AAEC9A23DDF6B12273C01B
SHA-256:	012B9BD7D2B13E92784EF2C7A68F61B27F433601DE2DC726901888ED18C2EF5F
SHA-512:	E7A4255DCDA78050C5FDAB4FC50A4021AC3E3B92A6D90C47788836C03AD300BE49668C81D4DBE9B78C2BFF05BE9D6C6C414EAE5BCD99C39C1C8257A2A6D0C9C
Malicious:	false
Preview:	.....C.`..... ....

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):	2507
Entropy (8bit):	3.0663182171313577
Encrypted:	false
SSDEEP:	24:34SZ2vNlrlAfKx37H0Ehl037Cc6xLYPiGblpeJlin/OIM0TM:3462vxPx3Qr3h6NYP9nexnnTM
MD5:	0621268449C565E9A4FDE9E07B786CF9
SHA1:	BEE465EF6DDCBB22252C43D7430A1EA5F21E508B
SHA-256:	904422053AA1B5D9CA01D83689F2ED707F3143B219F373E9B34377BB7DD7BB8A
SHA-512:	F2E235D4FF0C14485277B61C4A2EC3B8EBD5B512C71D4DDD1FE4EE08173ED84CB986EB4502D45378EEDA214F6B748F38537606207F95A30293E411411A71B33B
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...925ba709_f78b_4b0c_851b_ec552132a867.....4l..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....a..\.....*...file:///C:/Users/user/Desktop/OA46809.htm..... .....h.....`.....o?.ia...p?.ia.....\...*...f.i.l.e.:././.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.O.A.4.6.8.0.9...h.t.m .....8.....0.....8..... .....*...file:///C:/Users/user/Desktop/OA46809.htm.....d.s.../. .....!.....*...file:///C:/Users/user/Desktop/OA46809.htm...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
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
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):	320
Entropy (8bit):	5.269053308578411
Encrypted:	false
SSDEEP:	6:m5LWVjyq2PWXp+N23iKKdK8aPrqIFUtpOLx1ZmwPOLnRkwOWXp+N23iKKdK8amLJ:YW9yva5KkL3FUtpo7/PonR5f5KkQJ
MD5:	04224588C4FBD7E228D3110573E1A5B9
SHA1:	6D53174D84D08DE54732EEA32CC02C0B39B42D57
SHA-256:	F41AE38FD2F871F64202BBF7A1D5067AC018EB46E73B1788E6FF29D415BBF302
SHA-512:	779F96A2C8EF4F5D369FB50EFCA77682D51B04EB09E9958C82B0CE0B11B1596D327948B131A5CE3A2B3238E75DA18DCA7FACFD9D14471F3A92806BDE0E5AFB10
Malicious:	false
Preview:	2021/04/19-23:18:24.167 1850 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/04/19-23:18:24.168 1850 Recovering log #3.2021/04/19-23:18:24.168 1850 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
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
Size (bytes):	320
Entropy (8bit):	5.254140507296037
Encrypted:	false
SSDEEP:	6:m5vyq2PWXp+N23iKKdK8NIFUtpO6X1ZmwPO6BRkwOWXp+N23iKKdK8+eLJ:Ayva5KkpFUtpB/PdR5f5KkqJ
MD5:	2FAD64647D50B3EB84D8D801C4064A5C
SHA1:	99A85C1EAC96886FB16E4D44A11AA3FC2C5D9E8B
SHA-256:	953E50C6CF5F4909FF78BA2D77AB6E24E870C937F18DB0FE5D7053945411C387
SHA-512:	991AA0E5092A7067DFADDB3AF002E73E762F846BBCDA8481F6FFA86B1CA6BE53B9C07AF4C55A1B994A735A4047012EBEB1EF79F3F18B0ABFAD21D53463BAF6 10
Malicious:	false
Preview:	2021/04/19-23:18:26.548 1850 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/04/19-23:18:26.550 1850 Recovering log #3.2021/04/19-23:18:26.550 1850 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","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
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
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.265913670389889
Encrypted:	false
SSDEEP:	6:m5L/4q2PWXp+N23iKKdK25+Xqx8chI+IFUtpOkJZmwPOPNDkwOWXp+N23iKKdK2L:8/4va5KkTXfchI3FUtpPJ/PiD5f5KkTM
MD5:	4DD5ABE0455BD18C35996AF17BF34E64
SHA1:	6732E13E7A4C748206CE4BB17173F872BD44FFBC
SHA-256:	A2D2C06D4591E319A04A6A4B28756C2C1878A67CEFDDAC26A314627CAB080139
SHA-512:	A98DBAC2146D8FB5B0D1897D712AF796A60225BBDF8F446C064DFCDDF3FCC5542DA84EA2076704F3098D94BDBBEAC9BDB35227DA872D7B89480D27DF74A2594
Malicious:	false
Preview:	2021/04/19-23:18:27.272 1820 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/04/19-23:18:27.273 1820 Recovering log #3.2021/04/19-23:18:27.274 1820 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.245162300630362
Encrypted:	false
SSDEEP:	6:m53HUd/4q2PWXp+N23iKKdK25+XuoIFUtpO3cOJZmwPO3cODkwOWXp+N23iKKdKl:EUl4va5KkTXYFUtpdOJ/PdOD5f5KkTXp
MD5:	40B292E3E546863013A478CB89EB2916
SHA1:	6B808C43B6C99E3E53F3276EB9A4005967A55B4A
SHA-256:	8DBD331972FBB5AAEE88C89FCBC88FB809144F3BC025B4C8775482DC9DB11ADA
SHA-512:	24848147536B9BF7F89188719C3B8DB05452018C2C6DB4F1341FA14A430A17CA207AB31490B4072A2B9EBE39474099C4C948DA6541FC735DCA27148D379EAFFB
Malicious:	false
Preview:	2021/04/19-23:18:27.268 1820 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/04/19-23:18:27.269 1820 Recovering log #3.2021/04/19-23:18:27.269 1820 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.284503244880922
Encrypted:	false
SSDEEP:	6:m5YqN4q2PWXp+N23iKKdKWT5g1IdqIFUtpO8JZmwPO+E/DkwOWXp+N23iKKdKWTk:s4va5Kkg5gSRFUtp7J/PRE/D5f5Kkg5i
MD5:	83D46D39186EB4B9E2F4DF93757578FE
SHA1:	105C2FE397AD1B78357E84268A32584950298EBD
SHA-256:	D7264FF812E807071D9D92E2490029DF716B363E5538F50B8B2BE21E927800A1
SHA-512:	57BBECFA6219C33830A12871AAAD1E08893A881425E607DE80381E2A4788E8C763E0209C527D1246577DAC6CA6C19A625BE03A233702AC25122A9E7136A72F1E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Preview:	2021/04/19-23:18:27.254 1820 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/04/19-23:18:27.255 1820 Recovering log #3.2021/04/19-23:18:27.256 1820 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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8Efl0s3:85s
MD5:	86FA947878B47548861BF05662E6AF71
SHA1:	671F64DEB4174B081CC60F743062899E85A457E5
SHA-256:	F56EF77B8EC33BD5A5C6F3D37B751BADA76E18620AD4EB2CCE0DCDE89BBCE066
SHA-512:	7A7AA8E856E206C02F9D72D9DF68678403BBA5D009535415A811CA522AD7AD3CAD70611DD5A7ED2DCEEFF1C27F9CE6F342DFA5B009B824FC40FC3DDF9BDDA96
Malicious:	false
Preview:	.'..(.....-.../.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.1003114158689333
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvCtfYbjF1K+3CDeo+HOo/lCxthifIGCxC+/eryX/HlkMYCjF1K+:TL+A/VBeP+HNuQgGI/VG7CBl
MD5:	80F039C36750DD07F661962ECE86E22A
SHA1:	FC2479D3A764B00181240E720221C79563322601
SHA-256:	5B29C134CC1EF6DAEA4C6B9A00176AD1AB1CDCB63DC4FD808C079DB964C0E964
SHA-512:	FB8D85D59693B6023C1DD88F44B6952B29CDD3A07DC44DE7282EA70FCE193EF2DE058EB4F55DCFB09197928F769CB364BE27C0DD6D17328BACCCFC54C65AED35
Malicious:	false
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):	521
Entropy (8bit):	5.096043248302253
Encrypted:	false
SSDEEP:	12:Xiga3NcuwBhw63FBPyP1aKzweU7sk6WUdvMBk778B/xgskJnkBLbJkWin:XiBN+AcFBPU1hzM771y2Y78BJgskJkPi
MD5:	0B4873E41C13A0779A7E39ECFF954301
SHA1:	C5518706F467E8BE4865B0E1C93C27C577EB211B
SHA-256:	1AFF34372949D8F61CC4CFD168A0CDDA2909074F755EA441018682F772B71D3C
SHA-512:	BE19970EB9F22E93C599FC73667D389C9970995EFEA27CA871144EF9FA0D3588998F2B3306842AD4B4A6F61F501BB6CD11E0355C5EFBA31FA16255A8D6F2E2A9
Malicious:	false
Preview:	....."0....c..desktop..file..user..htm..oa46809..users*L.....c.....desktop.....file.....user.....htm.....oa46809.....users..2.....0.....4.....6.....8.....9.....a.....c.....d.....e.....f.....h.....i.....k.....l.....m.....o.....p.....r.....s.....t.....u.....z...:A.....BR...N..... .....**file:///C:/Users/user/Desktop/OA46809.htm2.:.....J.....'

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11642500274899595
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
SSDEEP:	6:C//Ygg9bNFlWCj/lWel3lb4/fMt76Y4QZVRtRex99pG/QqR4EZY4QZv8fOe:CIgqLBj/s63lb4nMWQA9LoBQZ8fOe
MD5:	C6940B73D263FFC206B00E087AB733DF
SHA1:	4A41C670EFB37F3DBC47146EB113C39394AE9B57
SHA-256:	E768F729363DC69B0A0D20105FBA63E673931913CAAD35D0E3CF25D0521CB6A5
SHA-512:	1A54F4AAE5F0E062A85C9FC0107D7FF240FE0D952003D79BB6F6E73798D3E4FCB23F6C2A9EDDBF5BC80005A20E347A99DAA912B4798B960CE4C1192BD82DA57
Malicious:	false
Preview:	.....O.i..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.480338657241785
Encrypted:	false
SSDEEP:	48:9X4GsA0MLa7VLMZ+8dbxVs81bQSefgGQNrS0U9RdiN9l:/a75MXdbLs81bQ5fgGYrS0/
MD5:	5672BB75E75CD63AAFB5E6E37C80FC14
SHA1:	0492B4F63C7D367C79615242ABE3D2C523D3072C
SHA-256:	E3EB88E96C4F4A73437B80DC5CB505639D030AD43865B2FABB3EF0F46CCA53A8
SHA-512:	AE717B8CCCA7E3148BA3306B95DD3764A16535CCC330F587B701078963BA58454A33385BD71850C502D082ADE41F520D80B3FF627DCFEB117DAA9A12065CFB09
Malicious:	false
Preview:	.JJ...*.....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..249762000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-04-19 23:18:31.96][INFO][mr.Init] MR instance ID: 7efbc021-49e1-4c19-8f2f-146ddfb2d905\n","[2021-04-19 23:18:31.96][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-04-19 23:18:31.96][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-04-19 23:18:31.96][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-04-19 23:18:31.96][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-04-19 23:18:31.96][INFO][mr.CastProvider] Query enabled: true\n","[2021-04-19 23:18:31.96][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.215187807362162
Encrypted:	false
SSDEEP:	6:m5uMMM+q2PWXp+N23iKKdK8a2jMGIFUtpOuZmwPOWESMVkwOWXp+N23iKKdK8a23:BQ+va5Kk8EFUtpF/PZE/V5f5Kk8bJ
MD5:	BF44E68439675A544ECD38A26B90FA2C
SHA1:	5468DB49C6E728C36A1E3AEDD50A2B1BEEE09F00
SHA-256:	80F793C614BD68A6BC0063D7F8C8F8F1D3B2E4E0CACF6497B27C6E58B86A8EC5
SHA-512:	6220A213C318EB0020F9757B9A4E4EB9D42EA5BFF942CCCAD15301E05116791DF484C561A7994F1F45F7BE01BE535427E82629E6F8A63F5E22C1B5F492E8B6FD
Malicious:	false
Preview:	2021/04/19-23:18:23.951 181c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/04/19-23:18:23.954 181c Recovering log #3.2021/04/19-23:18:23.959 181c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.23712445117803
Encrypted:	false
SSDEEP:	6:m5FY9+q2PWXp+N23iKKdKgXz4rRIFUtpOFN3JZmwPOFrS9VkwOWXp+N23iKKdKgi:l9+va5KkgXiuFUtpIJ/PSS9V5f5KkgXS
MD5:	C5E0881743DD86FCC203B835413D0EA9
SHA1:	C63623B16527CB5EF298FE65F29DA1BE39505F5D
SHA-256:	7EA9916BF07CEE3F35110D759AB989B69644B7C0C62769E30AD006EB07F9523F
SHA-512:	C516812F2A095E9840AFA23F1A6224DCFE349FD32EFBCB5A6A36D0FCCF116615A02A8926F93A6DC72A4B1A392E4E365FDD8839E9B5ECF7CC7B7B0F37DC3117C
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Preview:	2021/04/19-23:18:24.183 184c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/04/19-23:18:24.184 184c Recovering log #3.2021/04/19-23:18:24.185 184c 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):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

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):	320
Entropy (8bit):	5.186855795123462
Encrypted:	false
SSDEEP:	6:m5e7+q2PWXp+N23iKKdKrQMxIFUtpOY5ZmwPOJtVkwOWXp+N23iKKdKrQMFLJ:Qva5KkCFUtpj/PM5f5KktJ
MD5:	02BF66722EC3738CE8DF8B34F9E26ACB
SHA1:	CDCF8580F878837F89441BDF34B4DA8B25CC87F3
SHA-256:	E3A77C1962A9DCF80EBE646A1D9A27781AFFA61DC1BE5A47B1EDC2016FAC2AA0
SHA-512:	8F0235C9C9E7B4BD502033886DFC0E009E47BBEB459405B35B9E224E8BD29A706154E5C4404AE352F5E9AF7B7D4F62591A9DC263AF00BC2EB6B4CF177E44219E
Malicious:	false
Preview:	2021/04/19-23:18:24.092 1848 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/04/19-23:18:24.094 1848 Recovering log #3.2021/04/19-23:18:24.095 1848 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):	348
Entropy (8bit):	5.201749211660349
Encrypted:	false
SSDEEP:	6:m50yq2PWXp+N23iKKdK7Uh2ghZIFUtpOBSK1ZmwPOuHRkwOWXp+N23iKKdK7Uh2w:Tyva5KkIhHh2FUtp0SM/PxHR5f5KkIh9
MD5:	4DAFD2B6CD8B3772C02F979ACF0E6550
SHA1:	418578835AC64BEA12D005AF5A1F68B6DB9D3BDD
SHA-256:	F6FAF0D585D1324F6966D3FFCD0B37908D48D6AE2BEE35A85287445CB0C4B269
SHA-512:	6533E45FF3D61FCB7A75BAB3B7888C5E44768251EEF53EF04CE102F5EDA64191C9C67C11B90AE0689EA4D70DF5572EFCCA2F90E978CA10C505B8164FB278D3I9
Malicious:	false
Preview:	2021/04/19-23:18:23.944 1850 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/04/19-23:18:23.949 1850 Recovering log #3.2021/04/19-23:18:23.951 1850 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\5dc5cbe9-51c1-414a-9182-47d0960e7cda.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\5dc5cbe9-51c1-414a-9182-47d0960e7cda.tmp	
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\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
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.256085905375345
Encrypted:	false
SSDEEP:	6:m5P+B+q2PWXp+N23iKKdKusNpV/2jMGIFUtpOPNZmwPOPk3VkwOWXp+N23iKKdKK:c7va5KkFFUtpsN/PsI5f5KkOJ
MD5:	2317CEC466F1D1CEE3B699BDB08E27B8
SHA1:	E29F0F72E77BB4A16787DFB61C114F1723FBC680
SHA-256:	09CC1E76541DB13008D9DE62F76EB3FE47ED3494A680402ADE1C553CE0537E12
SHA-512:	5F44D981205C7DD424D94383804FE98F0B0958B10B7DCAA286DB47E5DD3672AE73B4EA81DAE5A7609F1435E656342FBA1F1838D8F0F44E3E47BC6202197D8FE
Malicious:	false
Preview:	2021/04/19-23:18:24.122 1848 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/04/19-23:18:24.123 1848 Recovering log #3.2021/04/19-23:18:24.124 1848 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.301737949393457
Encrypted:	false
SSDEEP:	6:m5FQL+q2PWXp+N23iKKdKusNpqz4rRIFUtpOFlFG1ZmwPOFySQLVkwOWXp+N23iM:Byva5KkmiuFUtpl/PvR5f5Kkm2J
MD5:	C71EE5C30BFBA8E1627AD0B63A7BAA42
SHA1:	A0F090B05F3458741831D6453760D1D8462DFD0F
SHA-256:	E64BB5438CDA979D9E41C145C9798CCF89E6AA3097BD1846E72AC412062CA071
SHA-512:	1856A7011F6349441F421C02C35AC9DDD9745F41BAC4D53EBBECFE7416AAE9639A120BCFACAC3748C91C99C77367EBFD9607FF9A7E575024C21CCFF69DC3837
Malicious:	false
Preview:	2021/04/19-23:18:24.178 1898 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/04/19-23:18:24.181 1898 Recovering log #3.2021/04/19-23:18:24.183 1898 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
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
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):	418
Entropy (8bit):	5.308803811536069
Encrypted:	false
SSDEEP:	6:m5gQTtS9yq2PWXp+N23iKKdKusNpZQMxIFUtpOgQo1ZmwPOgQScRkwOWXp+N23iA:DGtS9yva5KkMFUtpTD/PTncR5f5KkTJ
MD5:	0F4F41D07C2A6DF7C10E02551BBCDC22
SHA1:	226D57B9DDAA5B0AD9DBA97E6C02DEC999D7B068
SHA-256:	8BE608F4AA2956D040753EC6153A57DC9A89025B20826EEFF48CB6C194C2A5F4
SHA-512:	3B24B068B6148BC51D2B234D10E0B49484846CF47B4626620399ED2573400A239C660AA0AEDCE3B6CA13281311315 46A6F30E9960BFCEC1D95C6D7854DEF57D
Malicious:	false
Preview:	2021/04/19-23:18:40.569 1850 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/04/19-23:18:40.570 1850 Recovering log #3.2021/04/19-23:18:40.571 1850 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
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.22398635879975
Encrypted:	false
SSDEEP:	6:m5bLk+q2PWXp+N23iKKdKkGckArV/2jMGIFUtpObLEuZmwPObLBVkwOWXp+N23ik:mva5KkkGHArBFUtpY/P65f5KkkGHAryJ
MD5:	2A3AB39A8AE8F02091B87DD830DFEC07
SHA1:	3DBC517BF5FFD599BB8378FC8A8A365EE0E6A601
SHA-256:	66F4107220FC3D5822E9839936FC08C95E7D710CE8369F7CEC1F81F475DB19D1
SHA-512:	5414C30B1F81F5BB35DAD80865B68F26789906A10A576389589DA2AF845175B87455FAC755C500E357D0CA02547AB361B24550A3116D803BDBDBB5DF5E86E1B7
Malicious:	false
Preview:	2021/04/19-23:18:30.798 1848 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/04/19-23:18:30.799 1848 Recovering log #3.2021/04/19-23:18:30.803 1848 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.22050267644481
Encrypted:	false
SSDEEP:	12:Vva5KkkGHArqiuFUtplUy/PlO5f5KkkGHArq2J:5a5KkkGgCgTVYf5KkkGg7
MD5:	8923416488C7D9281CAF13C37F0C8D57
SHA1:	78793F9F1DDBA540AA771A050E791D21B54F6529
SHA-256:	C25B5AEE4E36444EC88E62918AC43539DE63AD8D0C03561C61B1012DF44DC2EF
SHA-512:	711A3727B57666807DCDCB25639AF3D16F7CB79F575E8F57BAADE65904578FE13C4B7782BA8F07DD437001530DD0C25E8445040FD419F548DAD0749C1C68D86
Malicious:	false
Preview:	2021/04/19-23:18:30.809 1844 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/04/19-23:18:30.811 1844 Recovering log #3.2021/04/19-23:18:30.812 1844 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.217216949514199
Encrypted:	false
SSDEEP:	12:Qyva5KkkGHArAFUtpnn/PDR5f5KkkGHArfJ:QYa5KkkGgkglTDf5KkkGgV
MD5:	247E6F6CD8EED6230704944A8D573F00
SHA1:	A5CA9152BC93EA29CE9D4FDC6A1DC2440EA15ED0
SHA-256:	988BB4CE1EB3C83A45D36F5B5AB93CA39E2CDF523E078524606F6D64E163E40A
SHA-512:	E142D0D555BE1C48F21EAC12C9319F1114E2643AFE74930C26320067C0A20049E2C6C37089D6531989C36EDEB5E407255415BA10EA10A8EFAED04C5F74297E7E
Malicious:	false
Preview:	2021/04/19-23:18:46.018 1898 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/04/19-23:18:46.019 1898 Recovering log #3.2021/04/19-23:18:46.020 1898 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\babd0dbe-6725-43c6-8e60-70a56a1920b4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\babd0dbe-6725-43c6-8e60-70a56a1920b4.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.277093619103952
Encrypted:	false
SSDEEP:	6:m58AVq2PWXp+N23iKKdKpIFUtpOKRNAgZmwPO64LAIkwOWXp+N23iKKdKa/WLJ:Eva5KkmFUtprRX/P94P5f5KkaUJ
MD5:	58758261D527D9AC4B46B05195AD546A
SHA1:	4E6A7DC422FFD96FAE5BB2E1530F5FA41EC4B074
SHA-256:	C315B5A862A7FC2A7004D96DA17B35DB52F7A5732EFEB2A95295FAF41E1532A5
SHA-512:	21FD25173DC0EFDDB9A4B494E1FCFA02C575FA231CC03261CEAD07ADC6A7CC61A906E2299C0F60B71428ED0EF44A0D82345F682B8051F76679BD093EF77467F
Malicious:	false
Preview:	2021/04/19-23:18:23.950 1844 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/04/19-23:18:23.954 1844 Recovering log #3.2021/04/19-23:18:23.955 1844 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.350243371595492
Encrypted:	false
SSDEEP:	6:m5Syq2PWXp+N23iKKdKks8Y5JKKhdIFUtpOC1ZmwPOURkwOWXp+N23iKKdKks8Yx:dyva5KkkOrsFUtpD/PfR5f5KkkOrzJ
MD5:	9218A225ED398BDED167A8AA0921A29C
SHA1:	A94760F8314BA1A51AAD32684F2C5BF90046CE39
SHA-256:	E36C69B21C8BA6210A22975970F06979C01D3B5D3AFAFD6A0C2F87F2A01FE843
SHA-512:	3415FE7C061008676BCBA524EDBAB881A222FAF78552F99F2413D5FB1A05A1C6E69DCAD9CF94280353C586A4F9FA3F776F25639233AF83913ADD70BF57E206C3
Malicious:	false
Preview:	2021/04/19-23:18:31.932 1850 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/04/19-23:18:31.934 1850 Recovering log #3.2021/04/19-23:18:31.934 1850 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):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:xedn:xC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
MD5:	19954008B730AA9B156D170DDF119667
SHA1:	19E169DEC1515C0B385046BBCB4EB39F54E99F6E
SHA-256:	800CEC860F78F395BA173F96205254C725C7851434C7FBE96B0B5D4E46F7F246
SHA-512:	7830BD2BB9C4CC81CCBF1022826E923740571115FDC582FC49ACDA62AEE3D8044B5F890C04303E3ADD8866FCFD70E6C60424DE7AC3D2CFA0FA18400B047310A
Malicious:	false
Preview:	.....l...x

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bd542608-73a4-43b6-bdfd-065f1daa0d53.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):	22594
Entropy (8bit):	5.5353649735068045
Encrypted:	false
SSDEEP:	384:uiyPtxLl5gXM1kXqKf/pUZNCgVLH2HfDprUPHGNynTBx54r:eLlAM1kXqKf/pUZNCgVLH2Hf9rU/GNyC
MD5:	1C4649089169FBDE6F4D16FF025906A3
SHA1:	9546DDF4679FDAB845B2D8E57EAB14748D21AF67
SHA-256:	359A68E45102CD1C4EFC9518ECDAA2C3B8204195F05445B4DB27D53711F91969
SHA-512:	DC0A8318B9B669AE886367BD890167C26DEB52EB12F1A537A14076031B9A766881824DC63B317565D05614E3C853F5E45B83E53F56E731D3387E61D70584612F
Malicious:	false
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":"13263373103945401","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
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):	4.525732464956886
Encrypted:	false
SSDEEP:	3:tUKO/cEXVNJZmwv3s/TVSQuNhAJ01V8ss/TVSQuNhAJ01WGv:m5c+VNJZmwPOyAJ0VvOyAJ0tv
MD5:	350380AEFC62D8EFDC8AD1B2B0FD8686
SHA1:	B35B6FB6C7C86BA26BFB02C7C42E9507876F188E
SHA-256:	96F32128A04B1D80D3B8F3FD106D0F35941E18555C14B8B9CF360F33F9B6A14E
SHA-512:	895D76575F7A402B2AEAE017EB074FB67B83BA1B778708B900129986236697A845FB3F34A4EEE219AD759DBF635FF034F3221DDF0789E371127CA8095A062E2B
Malicious:	false
Preview:	2021/04/19-23:18:26.996 1820 Recovering log #3.2021/04/19-23:18:27.075 1820 Delete type=0 #3.2021/04/19-23:18:27.075 1820 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Preview:	V........leveldb.BytewiseComparator...#...........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dc2f810c-4f2f-44fc-ac84-90f6f5cbf1ae.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):	5398
Entropy (8bit):	5.187778161567233
Encrypted:	false
SSDEEP:	96:nQ99WFKmf9fhRaScV/ok0JCKL8VbOTQVuwn:nQeXfvRZcw4K6
MD5:	EE4A13EC7A15C953AD14CC2DF62E51FB
SHA1:	BF55ED42E53CD7521B5AFFE6DBD77013B99B9C02
SHA-256:	DCFDE99968912A047C5948E3452FF3AF09A78D74CAEB126599CA53A21A74C476
SHA-512:	98EB463C1442478C885311057F53DC39F09A83AFF53D230CCB7D404FFC409617CD9BDC5BF2839B10E69E652BC6E9EDEDDC331DBF9E02E5C3638F1A4351937AB
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13263373104153251","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.25452086507787
Encrypted:	false
SSDEEP:	6:m5aKyq2PWXp+N23iKKdKfrzAdIFUtpOamK1ZmwPOaMRkwOWXp+N23iKKdKfrzILJ:PKyva5Kk9FUtpfmM/PfMR5f5Kk2J
MD5:	99DD6B5CD4D3D6CDC6D3EB74CE0E3168
SHA1:	C14C581C3AD276291EF53DF67C2CFADCE78FA4DB
SHA-256:	EFA2D9ADF28B93836C004227BC6D8E5D68BC19FF70D6000F55BC0CC5588D665E
SHA-512:	6C47662A2E20CBEAD7D1FDFB7005B148567E801631193BB9AF8403DB8FF62951EEE82E3EDC97C44470740DA32D7FE95156BEF99F161D9B09DEEF190B13BD92EB
Malicious:	false
Preview:	2021/04/19-23:18:27.352 1850 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/04/19-23:18:27.353 1850 Recovering log #3.2021/04/19-23:18:27.354 1850 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
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8Efl8:8z
MD5:	86CAF535CB34EC618CC81C19F006F1D2
SHA1:	4D100780313A05479B52AE8294510B71DB3D4B8C
SHA-256:	1F12DEC1C19377647099C102ABB8553AED4829DACF2B6743BFADAE0DC1B68B32
SHA-512:	87DC731B3067078A0319E5967D668ED62C13DAFD6471B18D9244AF4961EA6CD06E9F7072AB54808F1315DAFFB9C813518ED3C26B2B2CB91DF8EB9BCB49A4D4 9
Malicious:	false
Preview:	.'..(.....r.*... /.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.22.0\Indexing in Progress	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir5364_1894980434\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208920
Entropy (8bit):	4.964307261909652
Encrypted:	false
SSDEEP:	3072:gzChBJeloN++/mYWcT8WSkb1RqmYb8zpoPo/smfgbpxT0C0oUBXrvzpnuidAut:5clEHRAqggCylW1
MD5:	A96F63877D2B8648563905C60513B9F0
SHA1:	EE63F5F68E176DCEA8416C9877F09533C4E5498E
SHA-256:	B5A3D515B1673D134B197878D681C0CC8290BC476EB69D69EF27FF9669EC2E80
SHA-512:	C137035D92E4161FF55AF447D61F7F61E9FB8812EF0D32649011A6D7A07AEBA317B4197CF0205B37B755FACF7A1ABCA586507A1B825BC2FD4194E8306DB4E008
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir5364_1894980434\Ruleset Data	
Preview:	.....$...,.....C.....p.....P.....,.....geips..... n.....lgoog.....R.....ozama.....onwod.....h...(.....g.bat... ....<...@.....uotpo.....X.....ennab.....nozam.....e..l....E.....-.....l...P.....,.....\|.....h...p...H...,.....\...X...T...P.....H .....@...<...8.....d...,...(...$... .....,.....`...D.....|...x...t.....l...h...d...`.....X.....P...L...\...D. ..@...<...8...0...0..... .....`.....0.....h.....H...,.....x.....p...l...h...d...`..\...X...T...P...L...H...

C:\Users\user\AppData\Local\Google\Chrome\User Data\b6baa9a8-8122-4f6e-8eca-8cf0500d3c51.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):	155298
Entropy (8bit):	6.053182359866107
Encrypted:	false
SSDEEP:	3072:5AupswbCSU8AYeuAZFcbXafIB0u1GOJmA3iuRj:6CDbXDAYtA3aqfIlUOoSiuRj
MD5:	5664C762E3504BEAF65151B1BC6598C6
SHA1:	E64A7D64F6B540BC2B66A4F98225FB84CC50F863
SHA-256:	06D2C2FB38E311A8BFC2571B02A8E7699F1966C1BC54588C5816D62AC1FCB1DA
SHA-512:	6E0A7AC63552BF4D858FDE27575C732A6AA56F98827E2687811BA13A625CAA6E4AF34F64314D58995972C295B9058DAACA4874C420130637E0E82DB2034000DF
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.618899507361564e+12,"network":1.618867109e+12,"ticks":96379797.0,"uncertainty":5298239.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132

C:\Users\user\AppData\Local\Google\Chrome\User Data\ed676fdc-e47b-4200-ad25-9ac4189b22be.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):	163250
Entropy (8bit):	6.082314245920987
Encrypted:	false
SSDEEP:	3072:zTPupswbCSU8AYeuAZFcbXafIB0u1GOJmA3iuRj:vPCDbXDAYtA3aqfIlUOoSiuRj
MD5:	349FE3395B4F9A5D5FACBF66EEC9CE8A
SHA1:	7675CCBC73B9244323E295D9FBAA389AEA5E94BE
SHA-256:	0D0590DC1F4AD7BF4B7E93436F4229F4A51395A6052F6017E40CA8A0B571E82B
SHA-512:	5DC4D3A036578F98D6264CB6E262A22D9788E1643D71E0319AAA33DDF1323F31471B37B297CFBF7A10B783C90810A630F60A78E8C6D4843531B5904C80F9F695
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.618899507361564e+12,"network":1.618867109e+12,"ticks":96379797.0,"uncertainty":5298239.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510166076 96"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\f6959ff3-d39a-4e7c-973f-c3c616304af7.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):	154971
Entropy (8bit):	6.05231956065841
Encrypted:	false
SSDEEP:	3072:RGupswbCSU8AYeuAZFcbXafIB0u1GOJmA3iuRj:oCDbXDAYtA3aqfIlUOoSiuRj
MD5:	FBEEF0B85CBA6D91A16AD4F1FDEA7519
SHA1:	11B7F9B08A1E0F11D24600C869E6D4BD270D1173
SHA-256:	4D2E5FF5D98796D88647CDAC114A7D4016FA5DCF8F095F3C4BC0259C308BA97C
SHA-512:	9EC032A88B051CB920046303980D3DDBBAE725708896994819167906CA7564B2488016C11426FB9ADB29B3071086A97519E15FF99B6DCCCC22507CF00CFB4057
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.618899507361564e+12,"network":1.618867109e+12,"ticks":96379797.0,"uncertainty":5298239.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510169239 22"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\fdf39e1b-01b0-4ae9-93f3-c887e81cab52.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.743421577537811
Encrypted:	false
SSDEEP:	384:4ULxKuwnlYPMyV/xO1Nyr3vm+3NmoBHMpG5wrr4aIxlMoY7rj+mP7VbICuu1O8AK:FG6lRSYYRkeDg6IMfXGiKQuCJ1
MD5:	592311581129D18C94B2433B76472334
SHA1:	3D33034C12EB589BD2E4888497D2A97C3C8A179F
SHA-256:	B5E9A4B21C41598D122D638311FEAF882B109C160FFD5D7D81B77AAC6B1E30EF
SHA-512:	59B6AF99BC38F166D086BB731E908352671F22CF9F53AE1BB2D32088C888151C9D601FF75324B1F08EDCAABF4BD80DBBBFB759A9727F65DBF53F3073982CEB6
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....78.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Temp\29963d83-cd33-4e90-ba73-337ad6fabb19.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..& ..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,.. .W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6.. @?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\5364_1247938175\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9669759926795995
Encrypted:	false
SSDEEP:	3:SfvHUTa8URTTH/BXDj6:SXD3TfB36
MD5:	E3EDA33A5C956F4FC9C5BBD91FF10252
SHA1:	182B989E299A3EC306622A9DD45C3B74A4DF6077
SHA-256:	6D7A462B703F1617286B65BFE0116F267328BEFC379812BCE774D8C640289647
SHA-512:	A49FF4979FEC3512C44899840CCF8D112806330C93812C515F09953B9B6DBA6B1DAB1828382D634235CF23E093C983AEFA860B7A75FDCB5F3F98DD928D4F47D
Malicious:	false
Preview:	1.d730fdd6875bfda19ae43c639e89fe6c24e48b53ec4f466b1d7de2001f97e03c

C:\Users\user\AppData\Local\Temp\5364_1400477012\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363

C:\Users\user\AppData\Local\Temp\5364_1400477012\manifest.fingerprint	
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\5364_1411257820\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.7968821892704963
Encrypted:	false
SSDEEP:	3:Scay3wETa+bUXXAOWAU:Scx3w9XXAOe
MD5:	B911E803164F10BB690800F334384D15
SHA1:	85A5001E4ECB906157D6C41BAC1B24C20508C886
SHA-256:	6047ACD363644130633549F7C6E215E53D9E6CA127C43E122D8A53F69E3ED2DB
SHA-512:	4D37F6CB95031AA0156F85511CB5E24FDD1CCFB32D528125B2BCD541C2E466B04F635736CF2AA4BE3FFF15D7D0BF9A8F2222D5E333B45F17BD414DB48ED035C
Malicious:	false
Preview:	1.9ed6655f7339c2250e552bfa12561a5fc51574c60a22cbf36cecfd197ebb2dc1

C:\Users\user\AppData\Local\Temp\5364_1797466597\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.866533712632772
Encrypted:	false
SSDEEP:	3:SpUCQEd2dq8ebEJW2GnnHR:SXQ5Y88EJeR
MD5:	423CB83A2A3B602B0AA82B51B3DA2869
SHA1:	58BC924AF90A89CE87807919F228FE6C915AD854
SHA-256:	0047059C732D70AF8C2F407089237F745838A0FE4F75710ABF1E669B81243E9C
SHA-512:	F80E9B5D544894A667F74CFD0A4D784311299DB080CA6793AABD93B95CF1E2870F74AD38A6386D862580220047F828457240577335C565B7F38B0C6677811660
Malicious:	false
Preview:	1.ffd1d2d75a8183b0a1081bd03a7ce1d140fded7a9fb52cf3ae864cd4d408ceb4

C:\Users\user\AppData\Local\Temp\5364_1903111963\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.89429824295036
Encrypted:	false
SSDEEP:	3:SRwGXyUtz24TSXhV6DDt5WBG9EBn:SGGXyA5kDoDt5WwaBn
MD5:	7FB6C0307DFC7235990A87216D6EFE79
SHA1:	9C86024DE6EE647227E73C5905468DB9C31D8447
SHA-256:	F01B98701AE70087F82AAC256AB3ECFB736F4865B7DF915051C7D5B1C51BA78E
SHA-512:	AC7106F2503DB666C4B3A382587C9DAE424CC5692D75E555D1F6BC0E4F4B3A360B82C1C356D06E4F607EA40206699191F5F206979E67B9614F1DE2073D5B0E40
Malicious:	false
Preview:	1.4dcc255c0d82123c9c4251bb453165672ea0458f0379f3a7a534dc2a666d7c6d

C:\Users\user\AppData\Local\Temp\6adc9fdb-e31e-49c6-8a28-5eb60df84d7e.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

C:\Users\user\AppData\Local\Temp\6adc9fdb-e31e-49c6-8a28-5eb60df84d7e.tmp	
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....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.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\77ba024b-4bcc-4c36-b5df-2074aaa651e7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\a29e6c4e-09ef-4f95-a442-fd05746cc027.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\6adc9fdb-e31e-49c6-8a28-5eb60df84d7e.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
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.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\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

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\CRX_INSTALL_locales\am\messages.json	
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
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_dir5364_1379923383\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
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_dir5364_1379923383\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "155090406471082895 8": {.. "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_dir5364_1379923383\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:IPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\CRX_INSTALL_locales\bn\messages.json	
Malicious:	false
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_dir5364_1379923383\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:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE 1
Malicious:	false
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".. },.. "1522 140683318860351": {.. "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_dir5364_1379923383\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:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
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": {.. "m essage": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$ST ART_LINK$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_dir5364_1379923383\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
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_dir5364_1379923383\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
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_dir5364_1379923383\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
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_dir5364_1379923383\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
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_dir5364_1379923383\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

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\CRX_INSTALL_locales\es\messages.json	
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71EEEE
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas describe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\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:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB11202723566
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "1522140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\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

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\CRX_INSTALL_locales\fi\messages.json	
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A5261952050 21
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "152214068331886 0351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\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:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C8202343738 91BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C00 0
Malicious:	false
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_dir5364_1379923383\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51 B
Malicious:	false
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_dir5364_1379923383\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

C:\Users\user\AppData\Local\Temp\scoped_dir5364_1379923383\CRX_INSTALL_locales\gu\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.483906482724201
TrID:	
File name:	OA46809.htm
File size:	9422
MD5:	170db7cf0e97b8ef6b317541da9178c6
SHA1:	1f67ca780887d2c4905afaf625aab6f4af00be87
SHA256:	f7d6248230338ad28e623c73c5667d3d0851ee1ea1404a22a9f5e7882120318f
SHA512:	75d17d15851596d2c2a94c3a273e802c468a7cd6d4a11119d87f1c307085ea79db3bea4cf958be15637e1423f8f2718f8453af4339c69f880565efa3dd363771
SSDEEP:	96:zyBFqwb3yHhAL1ddddo9mddddCWjrIFqxbGe3zMMgN5glYOIXs+XSIKEC8HtYx9z:zyBFVl4mjrIF2BzmN5UC1Y/IK
File Content Preview:	..<SCRIPT Language=JavaScript>...// This version also passes the recipient and order information as variables.. .function saveFile(url, sTo, cNo, oNo, oGn){...var isSaved = window.document.execCommand('SaveAs', 1, '\\\\IPFS01\\Public\\Computer Department\\

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/19/21-23:18:45.251038	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution

Total Packets: 110

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:18:30.827996969 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.868652105 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.868763924 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.869010925 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.909694910 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.916846991 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.916897058 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.916934967 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.916973114 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.916973114 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.917038918 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.930700064 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.930851936 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.930958033 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.971764088 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.971807003 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.971884012 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.973303080 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.973758936 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.973800898 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.973838091 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.973861933 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.973875046 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.973889112 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.973929882 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.976568937 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.976613998 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.976665020 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.976687908 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.979448080 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.979491949 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.979538918 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.979568958 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.982415915 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.982467890 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.982589006 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.983479023 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.985110044 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.985160112 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:30.985197067 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:30.985235929 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.012636900 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.012701035 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.012770891 CEST	49726	443	192.168.2.3	216.58.212.129

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:18:31.012830019 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.013959885 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.013999939 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.014065027 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.014086962 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.016760111 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.016802073 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.016875982 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.019637108 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.019676924 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.019747019 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.022492886 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.022542000 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.022613049 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.025338888 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.025378942 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.025500059 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.028248072 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.028290033 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.028358936 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.031044960 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.031086922 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.031150103 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.033921003 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.033981085 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.034075975 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.036633015 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.036672115 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.036756992 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.039328098 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.039377928 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.039460897 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.042032003 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.042076111 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.042135000 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.044769049 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.044821978 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.044915915 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.047446966 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.047488928 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.047561884 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.053423882 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.053466082 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.053529024 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.054522991 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.054564953 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.054625034 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.056624889 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.056672096 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.056735039 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.058551073 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.058592081 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.058675051 CEST	49726	443	192.168.2.3	216.58.212.129
Apr 19, 2021 23:18:31.060368061 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.060412884 CEST	443	49726	216.58.212.129	192.168.2.3
Apr 19, 2021 23:18:31.060477972 CEST	49726	443	192.168.2.3	216.58.212.129

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:18:17.068815947 CEST	60985	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:17.133224010 CEST	53	60985	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:17.207283020 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:17.264772892 CEST	53	50200	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:18:17.372291088 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:17.421590090 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:18.738483906 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:18.787200928 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:19.830872059 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:19.879466057 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:20.183695078 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:20.245769024 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:21.160378933 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:21.217487097 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:22.474369049 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:22.525779009 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:23.616255999 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:23.664940119 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:25.227607012 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:25.279126883 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:29.062453985 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:29.063077927 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:29.066945076 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:29.124140978 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:29.127626896 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:29.131196022 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:29.138045073 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:29.200570107 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:30.017692089 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:30.086112976 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:30.086946964 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:30.133775949 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:30.146326065 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:30.201955080 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:30.757595062 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:30.824783087 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:32.252414942 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:32.312406063 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:32.498132944 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:32.551521063 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:34.455830097 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:34.504707098 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:36.285114050 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:36.333760023 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:39.556730032 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:39.606944084 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:41.069252014 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:41.122378111 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:41.896522999 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:42.911119938 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:43.938783884 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:43.950737000 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:45.202142000 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:45.250936985 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:45.984038115 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:46.044025898 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:46.953555107 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:47.002278090 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:47.846076965 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:47.904937983 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:48.914354086 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:48.963402033 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:50.344939947 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:50.397241116 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:51.821661949 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:51.871952057 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 19, 2021 23:18:53.694552898 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:53.743860960 CEST	53	59420	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:18:55.334343910 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:18:55.395503044 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 19, 2021 23:19:03.262264013 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:19:03.321315050 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 19, 2021 23:19:12.622383118 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:19:12.673073053 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 19, 2021 23:19:24.717787981 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:19:24.787086964 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 19, 2021 23:19:25.666093111 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:19:25.727612019 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 19, 2021 23:19:25.822021961 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:19:25.879110098 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 19, 2021 23:19:25.881786108 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:19:25.947932005 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 19, 2021 23:19:26.433007002 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:19:26.497849941 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 19, 2021 23:19:35.254831076 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:19:35.303622007 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 19, 2021 23:19:44.761763096 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:19:44.822488070 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 19, 2021 23:19:57.988540888 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:19:58.061727047 CEST	53	53279	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:06.364310980 CEST	56881	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:06.431488991 CEST	53	56881	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:06.556555033 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:06.617522955 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:06.705471039 CEST	55667	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:06.773559093 CEST	53	55667	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:13.950093031 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:14.157938957 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:14.618527889 CEST	62476	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:14.683285952 CEST	53	62476	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:14.812062979 CEST	49705	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:14.860790968 CEST	53	49705	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:15.280250072 CEST	61477	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:15.347948074 CEST	53	61477	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:27.017040014 CEST	61633	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:27.081986904 CEST	53	61633	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:27.226026058 CEST	55949	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:27.283508062 CEST	53	55949	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:43.611167908 CEST	57601	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:43.676491022 CEST	53	57601	8.8.8.8	192.168.2.3
Apr 19, 2021 23:20:43.836226940 CEST	49342	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:20:43.898113012 CEST	53	49342	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:04.263745070 CEST	56253	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:04.330914974 CEST	53	56253	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:04.481256008 CEST	49667	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:04.541150093 CEST	53	49667	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:11.776585102 CEST	55439	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:11.857338905 CEST	53	55439	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:12.315515995 CEST	57069	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:12.375307083 CEST	53	57069	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:13.008260012 CEST	57659	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:13.102334023 CEST	53	57659	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:13.467278957 CEST	54717	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:13.555152893 CEST	53	54717	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:13.992959976 CEST	63975	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:14.055195093 CEST	53	63975	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:14.507966042 CEST	56639	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:14.567553997 CEST	53	56639	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:14.940208912 CEST	51856	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:14.997174978 CEST	53	51856	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:15.548171997 CEST	56546	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:15.609868050 CEST	53	56546	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:21:16.399861097 CEST	62152	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:16.459841967 CEST	53	62152	8.8.8.8	192.168.2.3
Apr 19, 2021 23:21:16.884247065 CEST	53470	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:21:16.941318035 CEST	53	53470	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Apr 19, 2021 23:18:45.251038074 CEST	192.168.2.3	8.8.8.8	d077	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 19, 2021 23:18:30.757595062 CEST	192.168.2.3	8.8.8.8	0xbbee	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)

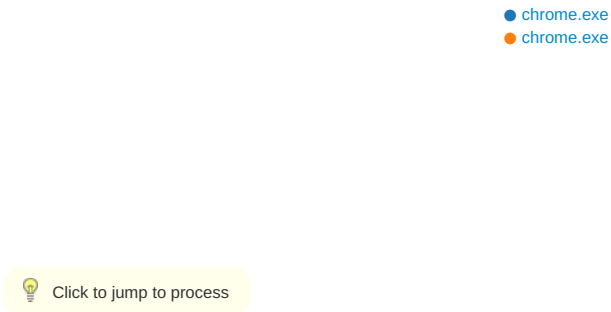
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 19, 2021 23:18:30.824783087 CEST	8.8.8.8	192.168.2.3	0xbbee	No error (0)	clients2.google.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 19, 2021 23:18:30.824783087 CEST	8.8.8.8	192.168.2.3	0xbbee	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5364 Parent PID: 2124

General

Start time:	23:18:22
Start date:	19/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\OA46809.htm'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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: 6260 Parent PID: 5364

General

Start time:	23:18:24
Start date:	19/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1580,3607684188885310936,9111398575048557525,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1688 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly