ID: 452248
Cookbook: browseurl.jbs
Time: 01:40:48
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

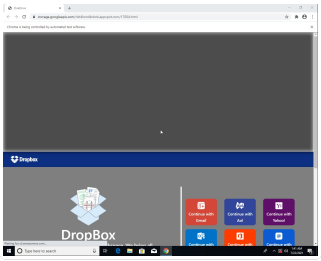
Windows Analysis Report https://bit.ly/36R4geg

Overview

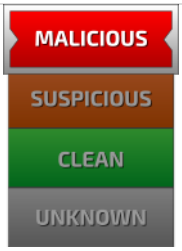
General Information

Sample URL:	http://https://bit.ly/36R4geg
Analysis ID:	452248
Infos:	

Most interesting Screenshot:



Detection



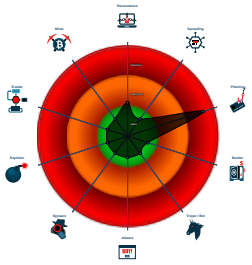
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Yara detected HtmlPhish20
- Yara detected HtmlPhish7
- HTML body contains low number of …
- HTML title does not match URL

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 768 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://bit.ly/36R4geg' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2968 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,13602693734026748389,18434443092193835822,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1720 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6672 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1544,13602693734026748389,18434443092193835822,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=4720 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Copyright Joe Security LLC 2021

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Yara detected HtmlPhish10

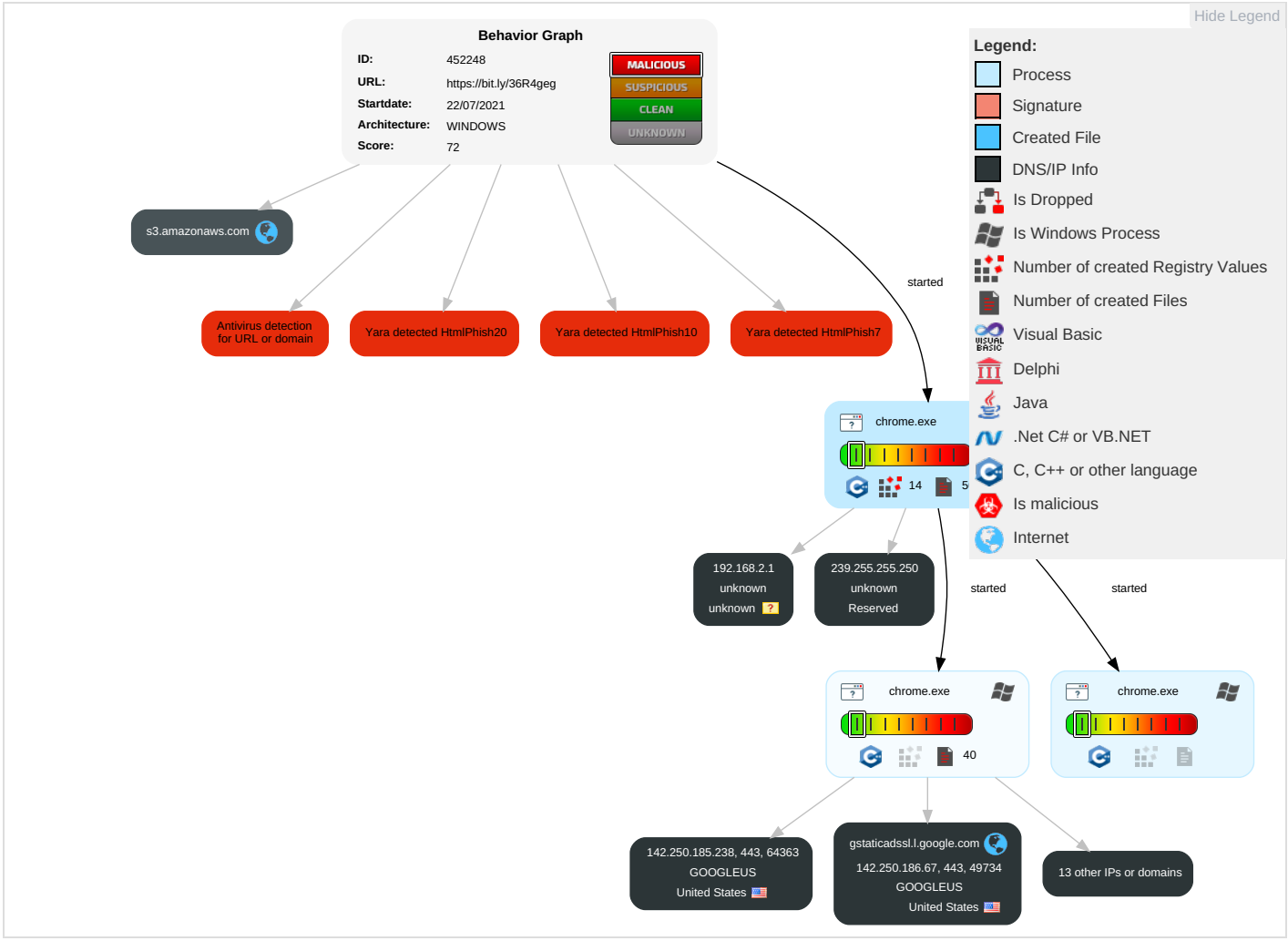
Yara detected HtmlPhish20

Yara detected HtmlPhish7

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

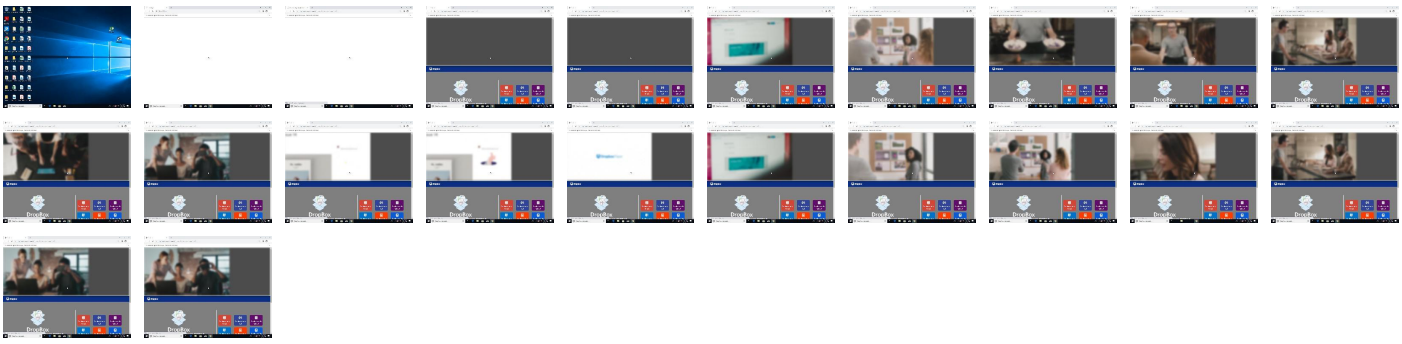
Behavior Graph

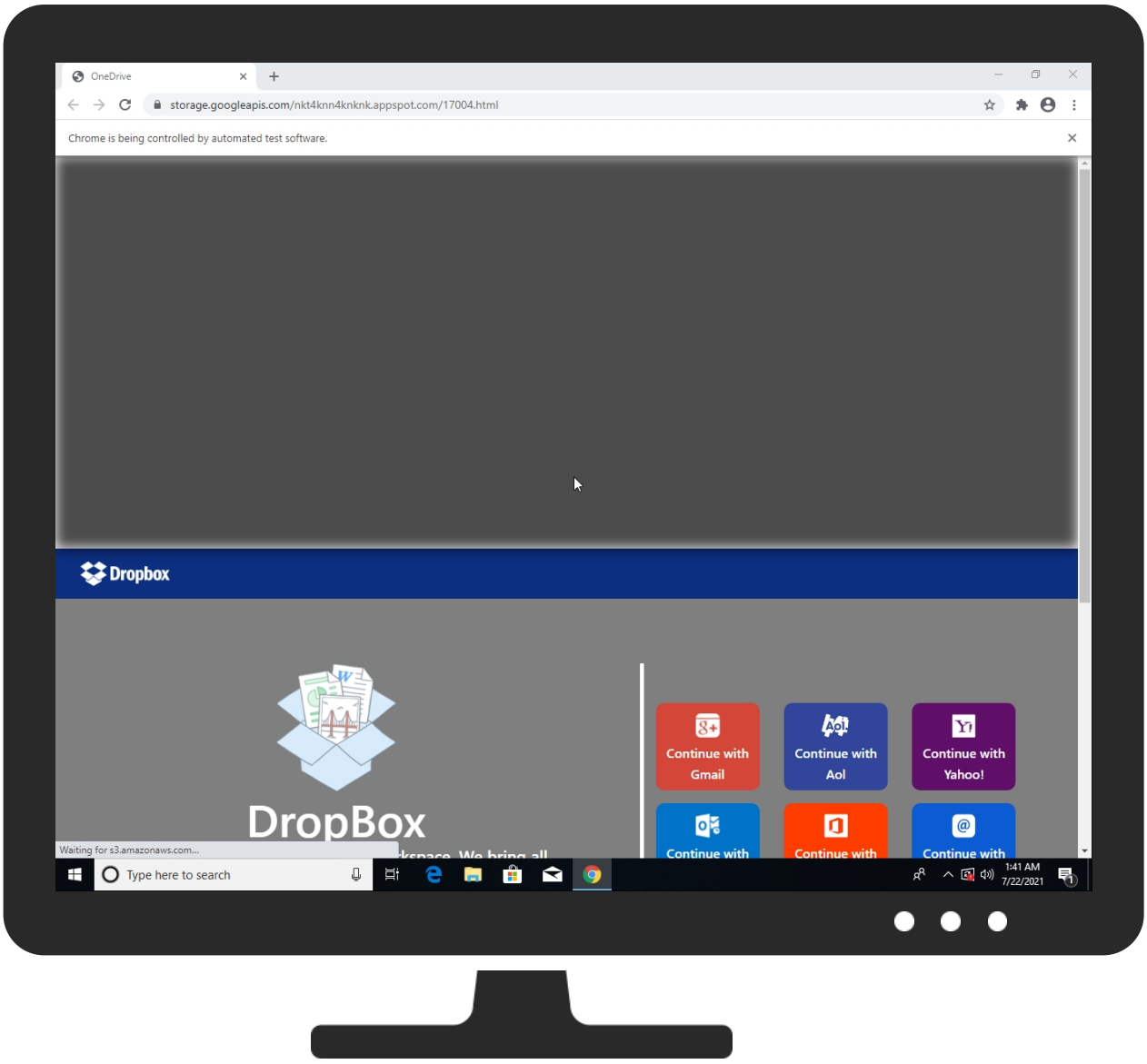


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://bit.ly/36R4geg	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://storage.googleapis.com/nkt4knn4knknk.appspot.com/17004.html	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://dns.google	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

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://www.google.com;	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.186.67	true	false		high
stackpath.bootstrapcdn.com	104.18.11.207	true	false		high
s3.amazonaws.com	52.217.134.120	true	false		high
accounts.google.com	172.217.168.45	true	false		high
bit.ly	67.199.248.11	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
use.fontawesome.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.67	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.185.238	unknown	United States		15169	GOOGLEUS	false
104.18.11.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
52.217.134.120	s3.amazonaws.com	United States		16509	AMAZON-02US	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved	?	unknown	unknown	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
67.199.248.11	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452248
Start date:	22.07.2021

Start time:	01:40:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://bit.ly/36R4geg
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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@35/229@12/12
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
01:41:41	API Interceptor	3x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\4D1ED785E3365DE6C966A82E99CCE8EA_216A6C169356295AB09C26D4D7D32E06	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.11947574613158
Encrypted:	false
SSDEEP:	12:JKtfOX5BWm+fPyiozHdhMWX0LOXedDJ6W8xTx847:JiuS/PyT7sWTX86W4847
MD5:	8B1982D1CA9C2158D88DB163FB05EB8D
SHA1:	2F049E51DE43BDDD076B8A9CB93A50F1E24F451B
SHA-256:	085F373E587049D94A0EDB0459DD6F613B3AB2F46EA797BBD89F83203C5E245C
SHA-512:	3D2E6B157BDA0DFB4DDFB55031444EBDCA04F0830FD933C8F428FE8EB19A9D063BC1BBEB0BA6A7129715D8A21C2A4A9013FD9EF294CCCE11000FD4B6CFD12D5E
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....=.P.....J`.e.!.....20210720222438Z0s0q0I0...+.....I.....v....@-h;qj....=.P.....J`.e.!.....H.!.. .E....x.....20210720220900Z....20210727212400Z0...*.H.....#....6^s..O...)./'..G.....9Q...t..4r.\A....._.@c^.V..U.....}j.....1+....C8...)....{_.3.e.G..z%..,...DR.kE;.3.l...`..>_(}.+ei.u....'B.I..* .7M.)w..z>h3...)..c.....?..8fn.).1....._u)...\.0.$.7.ej![.....7..[.....@.@d.R..J.....By..T..Q.r

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{..,."':o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.`=*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)...*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.195209092049282
Encrypted:	false
SSDEEP:	6:J0MlY0a/c5o78tjTZnDV7hLo/YpUd/tEnJFDxLvuoRy0n9qjZyXNK+a8NQW1HtSq:JY0H5FZJ9RgsyjX+aA1HHUoRn
MD5:	182151EFA6B59D28A8648FE4AB524759
SHA1:	EA0E7092DCF13F7975AC240531D4041EE4E034B6
SHA-256:	1B7F76696C158F687AD52CCBD5702F153A5135043AAA82228758F14DC446CD98
SHA-512:	6F9B87B1FDB3FD43BFD003E86E0E672110303ECE858960682D70ABB3F7D2EBAD57BE0A4F3297DF4CD28C3EA1EA9EB90013E85F33B2C62FA098F2DC14C3CAA 18
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....>.i...G..&....cd+...20210720215359Z0s0q0I0...+.....(..A..B..G@B.X....>.i...G..&....cd+....y.D.... .a_.k.....20210720215359Z....2021 0727215359Z0...*.H.....9zLm...;...i..8T#y.....IE..+..2_g9.*.....=.U.5..Q..=(./.&..f..o.%Y:f....3..EnD.g..k..%..../.D6....R++.k...'..`k>.=....h.`.Fb..$.eV.?....E#.r.....]?j ..q.5.I`b....K.;...sam.j.x.....hs.v.(..shp~...%..g....Z g..G.#..n.{.....Q..b.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\4D1ED785E3365DE6C966A82E99CCE8EA_216A6C169356295AB09C26D4D7D32E06	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	852
Entropy (8bit):	3.796357292414923
Encrypted:	false
SSDEEP:	12:UkO/DmxMiv8sFq3lCvM710z0Mqhz/fC3/DmxMiv8sFq3lCvM710z0MqhS:UkObmxxvm4vw1VhzXC3bmxxvm4vw1VhS
MD5:	146164975B69F375EBA349E2E1EFED5B
SHA1:	3FFE13175260A97101D4FF0B0F770A9620382077
SHA-256:	80C46904DA16E2C9695E5BA00140E1791FB6231B839264B156400364773F1755
SHA-512:	20AC3CCE76A32E3C3F472571CBD525D718E2291B2A54EFCC48C5A8FC52F7060EABCFF9867B3B00D8C5C49DAD72B15B0A936526C5BC7E5694AF2D7E03E0B62 5F
Malicious:	false
Reputation:	low
Preview:	p..... ....|..d.~..(..... ....W...}...U.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g. M.C.G.g.U.A.B.B.R.J.9.L.2.K.G.L.9.2.B.p.j.F.3.k.A.t.a.D.t.x.a.u.T.m.h.g.Q.U.P.d.N.Q.p.d.a.g.r.e.7.z.S.m.A.K.Z.d.M.h.1.P.j.4.1.g.8.C.E.A.t.I.g.y.H.h.z.C.A.g.f.0.W.o.j.6.G. g.e.O.A.%.3.D...".6.0.f.7.4.d.2.6.-.1.d.7."...p..... ....|..d.~..(.....}...."..-.....".-... ....W...}...U.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T. z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.R.J.9.L.2.K.G.L.9.2.B.p.j.F.3.k.A.t.a.D.t.x.a.u.T.m.h.g.Q.U.P.d.N.Q.p.d.a.g.r.e.7.z.S.m.A.K.Z.d.M.h.1.P.j.4.1.g.8.C.E.A. t.I.g.y.H.h.z.C.A.g.f.0.W.o.j.6.G.g.e.O.A.%.3.D...".6.0.f.7.4.d.2.6.-.1.d.7."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.139205445116624
Encrypted:	false
SSDEEP:	6:kK4wbqdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:Qwy5kPlE99SNxAhUe0et
MD5:	62451D49E48DB6511F74BBD99C819B37
SHA1:	897CB7C9092FC23777D72B184516C0C890A5FD3B
SHA-256:	62087C6CE4502BFF11CAE64AE09E001EF02E55EE71622EF3C32BC5D335D0F2F3
SHA-512:	22063C81DE9E685818196222EAC5348336F7ECB531FC3357760A764698504705EC237735ED0DE32B12504BC04AA1F70B8A5AE1AF8329BF9C3A0CF69BAEDAEAE
Malicious:	false
Reputation:	low
Preview:	p..... ....ZC...~..(..... .....T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.8398940478017183
Encrypted:	false
SSDEEP:	12:pCmxMiv8sF1JbqDkwJr0yruXmZZ1CmxMiv8sF1JbqDkwJr0yruXi:pCmxxvnFqYwJOXmZZ1CmxxvnFqYwJOXi
MD5:	1EA3336DD57DBD0A2A8DBAE39C697A77

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
SHA1:	F8394A9327B6D79D5BDFE0BF6C850BC4B7A67CD4
SHA-256:	59813CB64CB001C02960F8F7D5CDA202E62438F5FB75D757FB7B61924670CDF1
SHA-512:	D439A476A871236D6B995EA7E34001E267825835C4515D35FBB505F684F140038EB726435A9536B5F03AAF27046518C5884BC51F4A1788BE92C4D452AE9BDF59
Malicious:	false
Reputation:	low
Preview:	p..... .....J.d.~..(..... ....."..}...j.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.x.5.q.U.S.w.j.B.G.V.I.J.J.h.X.%.2.B.J.r.H.Y.M.%.3.D...".6.0.f.7.6.7.f.3.-.1.d.7."...p..... .....J.d.~..(.....5...}...ul.1.....ul.1... ....."..}...j.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.x.5.q.U.S.w.j.B.G.V.I.J.J.h.X.%.2.B.J.r.H.Y.M.%.3.D...".6.0.f.7.6.7.f.3.-.1.d.7."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\22aa6b85-49c4-41d8-adb9-aff7f356cec8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7487569476484826
Encrypted:	false
SSDEEP:	384:DrQP/FyoZp+zqNLrAvn93Yn54HhUGMrrGRPHxA5FFUruDmeJSdDvjIO5JHN21byB:4q1VqlowUeDLFJUXb+9Kj9/xf
MD5:	8F3EB994FCA213E215C84F4C835AB1CA
SHA1:	DFEED727DE634012CEFB924CE73E29522C3386BF
SHA-256:	4EDBBA9558FBCAF69EB95B901A7335166A133A77B3E506F21AE9498BAFA7E1D6
SHA-512:	26A6BB497A260E166A82E9B3BF9B3845E1AEA46E367D264F7C4D809610312F6C18CAB35B39FE6CF47F8FF29933FFE499E72E8F929110D80E91984F1882676564
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...h@.8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\551b1c1a-8aae-48f5-9ae7-e6259eb1f1ab.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):	365373
Entropy (8bit):	6.015126847994528
Encrypted:	false
SSDEEP:	6144:8ExzgRx37iWYFW8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBI:8izgRAxzurRDn9nfNxF4ijZVtilBI
MD5:	8BC230DBA0DF1657B497012977812CD1
SHA1:	D76819531047575E607A4C08103F0E74496B8235
SHA-256:	D1D9B9B352E06A3BEE82390AE7FCDB443DC57DFB55A1DF8D902FD437C947DF5C
SHA-512:	ACDC7607137D633D52300DA7790483EDD22EDC52F4A3731652C290CBE5EFDB6B9F77CBB9397EE6C2E29DD14BDA3D9DF77D1A7F98130A2C4505B576F3D8255C
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":1.626943300553179e+12,"network":1.626910902e+12,"ticks":6945920597.0,"uncertainty":3795734.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1Qfj oKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP0 5zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327141689766

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):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC.....................8...?E."..N_.sdPC.....................8...?E."..N_.sdPC.....................8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0284cf25-2b73-469a-a29d-a9acea714ebd.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):	5708
Entropy (8bit):	5.175693057941546
Encrypted:	false
SSDEEP:	96:nnr4GNyM9ZOqISKISoIk0JCKL8cM7bk/S97zEbOTQVuwn:nnrDyM9QqISfC4KpqkqU
MD5:	3D2913D4C20DD85E1437E5564CF47ABC
SHA1:	136AB7497FD5CF5253420D89BEA55AA9070C62C8
SHA-256:	F222AE952D51FA85FBC67A0CA5D8AAA2E92081FA48329B70BA4CD2CC94F1C181
SHA-512:	D61493CCCB65CF008AE534062DAA56ACEF8EDE1EEB26E546244936191430B7AA01EC8503EC8B4678F30CDE6D9BB079BF05EFC0BB8F50AA339E48E09AE4DA4A6A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271416898048991","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\14b44e13-d048-4924-b6fa-8c63dc0a1883.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\177d27af-e0c3-44ae-b962-7f5571fdcaab.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):	1873
Entropy (8bit):	4.874739631954309
Encrypted:	false
SSDEEP:	48:Y2n6qtwTCXDHyvzM3zs6CDs6STs6Wo5RSRsHi+YbxD:JnxOTCXDH+zM0sN50L+YVD
MD5:	C9D021D70FCE67CE58A495D31768EDA3
SHA1:	9A1D9EFAA515A65BC6CB06A4E63059E626E54477
SHA-256:	8B0EE51E8A9871652BA17E04C9EA7576FE938B5CC46EB77080B87ACC29A2C7A1
SHA-512:	05B8CF86DF3405F19B3BF19D59725C97D5078273AF35741D9A549D630EC38113DCA1940C7C96823953F39877F23B6CF82C743BA3F45A7F27E7C9999ACD6CB160
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\177d27af-e0c3-44ae-b962-7f5571fdcaab.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.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://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274008901291034","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternati

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3223eaa3-461d-4757-904e-22fde9e1a660.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.5771102128290195
Encrypted:	false
SSDEEP:	384:le9tkLll4X31kXqKf/pUZNCgVLH2HfDdrUO9FVv4A:GLlc31kXqKf/pUZNCgVLH2Hf5rUOfVvT
MD5:	D659C69065E7315E6AFE6E1212620EA2
SHA1:	5E2172AC6294F8347B8E36916F00E2A9E057FB87
SHA-256:	88550B5D7CF9773A19BA3D6EAF593F8525C3D28F18A22162E208A0757D18DFBF
SHA-512:	6081A6A71CCFC270265457F9E34AC86E9B21256DEB8FDA3F02E16EA4310CA654B07E87704573F98FB2B87D7DC2ABA1B72F833F53D696E273B6625D56B3BC82F
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13271416897739838","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\34f2408d-ac14-4430-9cc0-655396d7fb40.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):	1376
Entropy (8bit):	5.579442200090718
Encrypted:	false
SSDEEP:	24:YvIRqqeUn0xEnWswU+v6H0UhHIG1KU+9aUeCJ7wU+pBYxYUnKHRUeIQ:YQcRUnrVwU+v6UUh3KU+AUeCRwU+HsYd
MD5:	0760C2B2D16444CF9CCAA95998DADFFC
SHA1:	9F3DDB5E9C45D4CDBEF4E018E417DED37025E91B
SHA-256:	C836435B09998D4651F3729D510A65E2DBC084DB0829C60AD696CEB20A6E0283
SHA-512:	42BBD5AFA5AA954B4E4BBF7193AA9B78CF36B6649C3C3873D948A42F35EE3297F945C34725C0E0AD2A1D6022EEAC03256399CA0F007079DA02DC183FD836EE3
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658479392.790198,"host":"AKBA0EXj1W1QmJumkxUOTpibibkAwoUEp1CDrh5UFWY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626943392.790206},{"expiry":1642723392.795056,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626943392.795061},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1658479362.165411,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626943362.165416},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1658479301.337317,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\71b58166-4da6-4464-a53a-72f2fadab6c4.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):	24055
Entropy (8bit):	5.533424486015188
Encrypted:	false
SSDEEP:	384:le9tJLll4X31kXqKf/pUZNCgVLH2HfDdrU2HGTHGnnTA9Uv4p:bLlc31kXqKf/pUZNCgVLH2Hf5rUWGzGE
MD5:	99E0292E9ED32978872C9B32AB912553
SHA1:	1E1A6D065F60861FF2A18E9588A57D9351278DFC
SHA-256:	07E71E13777B1BC7F8D82B41B8420F8F68E374812C42DF1B7F856B84065F9E14
SHA-512:	9BA8C6925FED362C72C200406DA8E61EDB1982A536747819AD59F542409BBA0FAEBB7EA4505C3C389DCB44E173EFB1A02B028FCFE89EBEFF5FAAB92180ED5595
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\71b58166-4da6-4464-a53a-72f2fadab6c4.tmp	
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":"13271416897739838","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8a55a602-c4ff-4a48-a33e-cd5e818465f5.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):	1041
Entropy (8bit):	5.568161173634765
Encrypted:	false
SSDEEP:	24:YT6H0UhHIG1KU+9aUeCJ7wU+pUNYxYUnSRUeIQ:YT6UUh3KU+AUeCRwU+IsYUnyUeh
MD5:	2755A07895864D5BFC9BB331C3985067
SHA1:	76C7DC1A11BEAAE38487B33A4A197068D1EC9016
SHA-256:	60F3B0F6579FC389C0864A2E06E87E7F97FCD1DE417F67AE6561CC2068A25FAD
SHA-512:	A0034E55B626C1BF28BA69F00271333D52C1CE4863DDC6239186146CB083D8C900161D4EF43187AB284F10F8A62BCD8A4C7EAD3DF098AB429CF13E4D6C2A00E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1658479362.165411,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626943362.165416},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1658479301.337317,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626943301.337322},{"expiry":1658479362.113788,"host":"9UvCn9o1ynqURDIUGaQxoozSUYPXtPT9FELAxBKoxh8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626943362.113793},{"expiry":1633013028.952627,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.201323810410295
Encrypted:	false
SSDEEP:	6:mlbq2P923iKKdK9RXXTZlFUtpu7NZmwPu3BFkwO923iKKdK9RXX5LJ:Qv45Kk7XT2FUtpG/PKF5L5Kk7XVJ
MD5:	067E1AA6288C219C9412DA6D9D3BF435
SHA1:	0E552012EAE50FB6BFD2CC096D5664D790F64DE1
SHA-256:	5AC793495309337FAE23F85F1DFADC1B7A7CAC2693F38041001520544F1E9BC5
SHA-512:	77C10C3C0DCFAE7AF31ED1A5096A1940C34DDDFF79744E8138B4A07824C16610942339DD877816D3578C990499A4911483170D6BA66B2B4B0FE50E9777D86522
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:55.814 1b30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/22-01:41:55.815 1b30 Recovering log #3.2021/07/22-01:41:55.819 1b30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.192406197826885
Encrypted:	false
SSDEEP:	6:mlFJAq2P923iKKdKyDZlFUtpufUHSXZmwPur+kwO923iKKdKyJLJ:+Cv45Kk02FUtppyX/PP5L5KkWJ
MD5:	919F92C226567D304100DDE1E7E1FE11
SHA1:	80A3112F27DF2F76522919B348372BA15CE3327C
SHA-256:	DD5CC50118A7756CC1B936B110B99159F0D8E770CDA77B6835FB76EB909983C7
SHA-512:	B634FC28EC67235CB844686ED14EF03459D51B6024AE8B5817FBE918B7E0E3B49BAD8DBD72E57BE261258C6E21D027A61C490914B87E5FCEC0813C3CD380108
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:55.745 1b30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/22-01:41:55.747 1b30 Recovering log #3.2021/07/22-01:41:55.748 1b30 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\BudgetDatabase\LOG	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4b604237260d4090_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	365
Entropy (8bit):	5.833429572644498
Encrypted:	false
SSDEEP:	6:mm9/VYSHT8NWQAlKPUQynMLZHyUgG4UrYtRK6tWFH2WcPiZgjKQMmUrH7p:9/7z8NWQCUUxMLZcUEFkFH2Viu5FU
MD5:	267375BDBF056C5BBA09E2E20BF1A1A7
SHA1:	C974A3CFB285F3EAD75213801D6541283019F3C3
SHA-256:	B68A9939C454B639E04D24A63A31D37629743528CD60A6D82B28DDE42EE89636
SHA-512:	0BEE785DAF7D7A4DE45638BBF793C160ECD70890C5E581E71AF5F5D6D9C71012D84F44FB190AADC565D559B22ABB0D787B50797E8808A6FE20955B2C6393A6E 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...`[....._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://storage.googleapis.com/...H&/.....;.....P..../.6...F..G...a.....A..Eo.... ..^K8.....A..Eo.....H&/.Po..863278F93A116EA647408AF174977AF4D4B3F702E13DEE4C994D68FD9AC76867..P..../.6...F..G...a.....A..Eo.....".L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5fcb4d810f618d50_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	5.493076320163636
Encrypted:	false
SSDEEP:	6:muPYET08NaYWbVOqZkMLZHqtgMza6mxLI/PRK6t:zg8NaY8ZkMLZKpLr
MD5:	93613EDD1531200788FA911BE577BC68
SHA1:	1149A67ADD19BA05CBE9680134937F41A7441C50
SHA-256:	C82F70BB58A7D3B5C40EEA9A17E1D6F2B834969CA8C50118DA1CA0ACB2FC9E0F
SHA-512:	6A6F7B41BA58D96F623D0ED56EC028FB118D6133E2368889F7C5FA2B6DB666A2CAD38A3D519D6B9D6423ECBA933BC934D713B0BCD4A6452FF162790987EFB2 B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n...o.0....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://storage.googleapis.com/.T..H&/.....3.....Z.e.Q.....$..o|.. ....x.P...A..Eo.....H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\738dbc06345f3eb5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.482118946974692
Encrypted:	false
SSDEEP:	3:m+lipH8RzYP2FycyGYWCULLuFvDHMECYKKhmH+cjl1t/lHCULkcRowTjZcPFFGZc:mF6YerCU8MLZHRLtgSiwTjWL99K6t
MD5:	DDD971A4F29CC611D10951611D6D80A2
SHA1:	76DDAB15E89243A49AB6390482E3C3F29D99DD6B
SHA-256:	44822CAAEF983BB97FBFB1D7E2779D93C828B6B3D226915E56B1D18EECE98838
SHA-512:	38C2D71B49E672364BE578E72323FCEC4E3B3D1B014361CDBED69D5DC562B85731F9C1D2690E43197B87051D088A77FACB5EF2F426E6F7D673C807DB058571D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U.....:]...._keyhttps://code.jquery.com/jquery-3.2.1.slim.min.js .https://storage.googleapis.com/....H&/.....1.....rg)J.&[.-..:..j..T.....T.....KE.A..Eo..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a616bab70880d4b1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.434694249411338
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a616bab70880d4b1_0	
SSDEEP:	6:mUA/VYkb8E9xEvAErkMLZH5MvtgOl72JLjMEkX/DZK6t:pANv4OMLZZMvP0liLT
MD5:	2FA75F7D01DC1995AF8270E91376A190
SHA1:	436A7D5AED0916E021A36FF86342F11269764B83
SHA-256:	4CABF3426147945D51654682BD761442A8141FFB6E6BE181F322CD520B420174
SHA-512:	B2BC780881ACE9A84F4AD815DD9D6E418821C3363A8B262037D268313116AB9036A03A104DB633271D5AAB72026C4384509F837E504FF6C1F0621D474B041077
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...;%.b...._keyhttps://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js .https://storage.googleapis.com/.=..H&/.....H.....WI...LA_...Q.KF.E.{.` ...V.^.....A..Eo.....NVg.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bcd50c0593d29b4f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.352477989682076
Encrypted:	false
SSDEEP:	6:mqyEY68E9xEEUgLErkMLZHaxugfwlWWjL2eK6t:zxYgrMLZ6xDWvp
MD5:	8C8CE8424ADE9DB9786D934C96BA6FC2
SHA1:	F51A0CB076552AC0D8E261BE89F594829BF15BDE
SHA-256:	EDD1DC42E0219C5C5CB13754B896267BD1983CE59FA18F7AFFB52A6F23ED57DC
SHA-512:	7E4798F44347293E59A8E1B5AAB42A422A044FECBB7440E59251E6194E7CFDF6F80C22B7ED429BE2258583532462B37672E40DE2594E213535C0424095ACC887
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://storage.googleapis.com/Z ..H&/.....:.....%.f..Dv-...Ai.bH...._.vUn ...u.A..Eo.....^.c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bd8ed83d42d2a190_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94200
Entropy (8bit):	5.77175294708169
Encrypted:	false
SSDEEP:	1536:LFpeE3j2A622Yqk8VjMZzZEjS8kaRZsM94WpxSz2oDnYpnro/Ci9G1qvSPB:BNj2l2FBLWkOZsMDSz2knuCS1qW
MD5:	123AA8683698C928741FB2EACB2EA796
SHA1:	0C0C51A4168BC9B96DA70754A718D61D651E26D9
SHA-256:	0AC906CC03FBE2F6D250219DC71BFF2AE7774A671E48894D7DCB891E784682DB
SHA-512:	39AE8528AFE80F88130E82DA1F40AC9DA834AF1C8191929DC0F65A25BD4021B770BB83BE3A0071B0BC800554A42B8FE59DD9BCBB904EA2E5873ABB80670B428 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....863278F93A116EA647408AF174977AF4D4B3F702E13DEE4C994D68FD9AC76867.....'.JN....O ....n..a..S.....!..... .....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@...P....module....Q.@BAZ.....exports...Qc...g ....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.2.4 /jquery.min.jsa.....D`....D`....D`.....`z...&...&..!.&....&.(S....!..`.C.....q.L`.....Rc@.....M.....Qbz.y.....d.....Qb.....e.....Qb.C.....f.....Qb.....h.....S...Qb._.....j.. ...Qb. .z....k.....Qb..&D....I.....Qb~.....n.....Qb..=.....o.....Qb.J.....p.....QbJ.lZ....q.....Qb...R....r.....Qb.P.....s.....R....Qb...-....v.....Qbvh.....w.....Qbj.....x.....Qb.M.....y....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	4.711713313484802
Encrypted:	false
SSDEEP:	3:DrSR0s/f/lFl44DgAtiHMnD+LtdC1x+HtkMHQAl6ID+HNuinI7U4KL/lllhuBQ6N:vy3/lvbt/DEMD1AlDJohrqBQ6YNti
MD5:	E46483C096090DA49315A473BD39E53C
SHA1:	74FE57ABBC1F07394919679AF6B16579D74B263E
SHA-256:	F19973EA55E550F0659069D0316B6FAC89B735B88FE6E48BCE50350015C3BDC3
SHA-512:	2C77938A5EEF2AF6029D47C8372A39B7F926E66EC8B2EA2F59EDB4F70916ED31A622B2AED6E397C35A7C39A4DE38579E72F4A498FEBF3EAF91891487A3A3844 8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Preview:	......Mnoy retne....._+.H&/.....B=..._+.H&/..q.....O....._+.H&/.....P.a..M._._+.H&/.....>_4...s._+.H&/.....@.&7B`K....H&/...../...3...5../..... .....^}.Np.....5../.....H&/.

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):	0.821519747940552
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwadyZsZ3zwGOS/sf:TLyqJLbXaFpEO5bNmISHn06Uwi3zwGA
MD5:	7EE9F8BFF31CE8A58F1E24407825470E
SHA1:	ABC4D39D6E13CC1AAFC7018241E29E7ABE4D2CE7
SHA-256:	331A234D44F102641B7100DB9F31C3C790A9C28136C6232D0905D77690850B72
SHA-512:	F6FB7D55A084CDA2B820B8E0019FB79F706A4DADFB9A224277CDA613846354FEA88048A9DF22B6C8D202A6653E335E8B8E2F9B5615A827B5A7D4FFCD9EC45E C
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9690311575450492
Encrypted:	false
SSDEEP:	24:/IL4rtEy8ezpqLbJLbXaFpEO5bNmISHn06Uw38:/I+Dpq5LLOpEO5J/Kn7UA8
MD5:	ABEC05CFAA4A130A82E3808894F66C17
SHA1:	C3397BA4D6992ADCAB87831BEC62E711FA37E7D8
SHA-256:	33A4B015285C6636D9CAF551F637FF8BA3E8C00105A929314DF886588C0F5F4A
SHA-512:	8D5B264CE4ACED18CD55D1EE550B4056FF7FB28E4E0A842B59BAF9076A59A8EF8FB4DFAC7906A4D1AE7B6385333CBB617FAC1074CB7C85A82EE992B2296C0 CF3
Malicious:	false
Reputation:	low
Preview:	.....&N..... ....

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):	1569
Entropy (8bit):	3.2016566719171875
Encrypted:	false
SSDEEP:	24:34ScR+lrlCJc0kRcMzErtschYH1wgzUvZLcgjexG8lLlL:34vaxec0kaMortschYH1AchG0RL
MD5:	6B1CF87877ABEEAE9367CFCDAC3DFF1B
SHA1:	940B9D9085CE735D10D6BB22F56751870C24E34C
SHA-256:	37F27E662A31A8DC61B86FA011AA6119C9F55113F9DBDAAC82FEE3609CD3CF18
SHA-512:	ECB92CBD2DE978EF029E5C3E3561F6AAD780F1AB1A92DA9EA5CC555FB4898F2AB14514E91474677BDF0AA25FC925CA4C6CFEBFA4EFABBD92182EE7E93F30 C513
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...6eb07a97_ec30_4d7d_8218_0c0fe9aa9fa3.....<..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....C...https://storage.googleapis.com/nkt4knn4knknk.appspot.com/17004.html .....O.n.e.D.r.i.v.e.....h.....`.....A.....A...(.....@.....C...h.t.t.p.s.:././.s.t.o.r.a.g.e...g.o.o.g.l.e .a.p.i.s...c.o.m./.n.k.t.4.k.n.n.4.k.n.k.n.k...a.p.p.s.p.o.t...c.o.m./.1.7.0.0.4...h.t.m.l.....P.....H..... .....@.....X.....x.....h...0.. .....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....0..... .[.c.h.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....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):	322
Entropy (8bit):	5.165746761107407
Encrypted:	false
SSDEEP:	6:mnq2P923iKKdK8aPrqIFUtpAFZZmwPTPkwO923iKKdK8amLJ:ev45KkL3FUtpM/PT5L5KkQJ
MD5:	A30451590799BA176AABBD90EBA08AFD
SHA1:	1FDC638AC89C6C2098DF0C6784FBD3731206E21A
SHA-256:	48E92284567797F8BC687513A86FAD52BB5F2420A6A9C4FE9788A486653D4152
SHA-512:	57F3235A7159FA62E9A13E1E65C6F8FA68556CF3A69355B60C20359A81C337F1EE9C1710FBE3E5BB7FC18841C511CD3265C4EE7B470FEBB014B55CC255337C1
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:38.052 15a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/22-01:41:38.053 15a4 Recovering log #3.2021/07/22-01:41:38.054 15a4 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):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4C
Malicious:	false
Reputation:	low

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................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5................f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.148326996487229
Encrypted:	false
SSDEEP:	6:mncjWM+q2P923iKKdK8NIFUtpqz1ZmwP8lWMVkwO923iKKdK8+eLJ:NL+v45KkpFUtpqZ/P8lLV5L5KkqJ
MD5:	1C31B6919BAF63782867069C4937F4F7
SHA1:	B164B7BBBAC0014BC1F640711D365083D248B0C6
SHA-256:	0FED3717A3C82439A69C2D969E47E73A6461BE76E24311D31966C968E3D06D1E
SHA-512:	7FFBEF2791176013931E62B1E450270692E939D02A3E38AA5477B56710EC13038E8B46ACD68D2E942A1367E0B6991201C8985A0F1E99E9D3EC4314CB36352CAB
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:40.774 161c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/22-01:41:40.775 161c Recovering log #3.2021/07/22-01:41:40.777 161c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","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\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_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):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","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
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+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
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.242768201993027
Encrypted:	false
SSDEEP:	6:mlJq2P923iKKdK25+Xqx8chI+IFUtpuMhZmwPuE27kwO923iKKdK25+Xqx8ch+/o:yv45KkTXfchI3FUtpf/PZ+5L5KkTXfcF
MD5:	C38D01FDF816B15BB265742B45BD8667
SHA1:	EB1813045DE70D90B49DC82BB359A54A7254B408
SHA-256:	3343C861E55342B63471E6A3FF89EC5B3214932560A4EA834C1A0BA7F6504B9C
SHA-512:	D7C8E614E90941743516320FCC33D658C89A7D4D276B38418C9DE6ED0D32F391B3F72EC2322532144F340AD3A59F4575A2CF020BCCD508EACF3BEF2C12B1B7AE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/07/22-01:41:55.579 1b30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/22-01:41:55.580 1b30 Recovering log #3.2021/07/22-01:41:55.581 1b30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.223678210799751
Encrypted:	false
SSDEEP:	6:mlhCq2P923iKKdK25+XuoIFUtpu7eSXZmwPuG7kwO923iKKdK25+XuxWLJ:Dv45KkTXYFUtpgeSX/PT75L5KkTXHJ
MD5:	AB54624BB253D686F358C59CBA5099E5
SHA1:	EE59EBDD7F2AEED0D1EB4B365543F3B5EBECC25A
SHA-256:	CEB40C12CB42F9DB2C925A21ADB5127D75788C17960D011C7C869837D954CA23
SHA-512:	F01AEDE19EB0C3F7BA918A4A5261274D0C300B8F7F18936DF1E6771FCE0253A3F69D1DC41B7FF6FC9A104673C641011EDDAEEAAB81DD0A34232399495040A6A6
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:55.565 1b30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/22-01:41:55.567 1b30 Recovering log #3.2021/07/22-01:41:55.568 1b30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.172789802647814
Encrypted:	false
SSDEEP:	6:mlNWyq2P923iKKdKWT5g1IdqIFUtpuj1ZmwPuP+jRkwO923iKKdKWT5g1I3ULJ:3yv45Kkg5gSRFUtpO/PG+jR5L5Kkg5gZ
MD5:	2A36549C89F93E0D604ACACA50E75C65
SHA1:	9AAC37822C658E82619EA15E56FA53C4BEE00D8D
SHA-256:	DA8851A22ECB69262B8DFE1BC9C373AFB2AE97F9CD55D07489208DF2FAD46E15
SHA-512:	F28DE45FB988B8FB0701771109C8C9E6AE17A0F0D770AF63396BF79FBD1B3C4726EF463A947093D56182F63C7E827E846C12036DB54C616280008CC760ACC440
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:55.215 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/22-01:41:55.216 1570 Recovering log #3.2021/07/22-01:41:55.217 1570 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.17513333451213736
Encrypted:	false
SSDEEP:	12:TLBj/Yd46fZqcfGJZ6fkMLZqJgEGGJJG2MBRs2eMLZqJgEGSC:TLBg4wq6G7HMzEHnG2MAhMzENC
MD5:	07666E7C0B8B689616DE19949984104F
SHA1:	7E0A692DCE2064DCE3B9DFA192FC75060803E2A7
SHA-256:	C3F84BD96F533EA61C69F719B515FCE479AF00C87B900D6FBE8CCF538FEB0A23
SHA-512:	762745A5DEF8D0BCF27BB8122B3AA341A3F510132603617BED79ACD1D3650FE5FDEC99796F769481926FFEAD6837E32E2B76E0EDD0435F4DC364E0451CA3EE82
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Size (bytes):	868
Entropy (8bit):	5.439623850734085
Encrypted:	false
SSDEEP:	24:NduTC8TN8VTQAabqX3mTunJdAN0TNyT+MzEu1:NsTC8T+V8Aa+cjNzT+Mou1
MD5:	CCC56C77401AA6AAFE279EC799040DA3
SHA1:	EC9E7D7CAC6095B9091447372DFB765616C62E12
SHA-256:	8A996820C511BF9C63E4AB7A56E366D64C936F26B89994FB26A396C5695F21F2
SHA-512:	4F1DB1D26F9CCF71527C4CDA5A2F1E73206F31DCBC85FC19744E5A2F40F561878D959D5328DFF8D89073234CA55CFE2AE1295675FA5C9F529C15CD2F34127B4
Malicious:	false
Reputation:	low
Preview:	....."d....36r4geg..bit..https..ly..onedrive..17004..appspot..com..googleapis..html..nkt4knn4knknk..storage*.....17004.....36r4geg.....appspot.....bit.....com.....go ogleapis.....html.....https.....ly.....nkt4knn4knknk.....onedrive.....storage..2.....0.....1.....3.....4.....6.....7.....a.....b.....c.....d.....e.....g.....h..... ..i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....v.....y...:p.....B.....B..... ....*.https://bit.ly/36R4geg2.OneDrive:.....t..... .....*Chttps://storage.googleapis.com/nkt4knn4knknk.appspot.com/17004.html2.OneDrive:.....J!..... .....-59?...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33356
Entropy (8bit):	0.0470437731080601
Encrypted:	false
SSDEEP:	3:A8lwn3llu/fllg8l2Nllg8lv/fllg8lHNllg8lGFllg8lv/fllg8l8Fllg8lkpMi:ApVAC/Qn1u5KMg9bNFlEwtCS/lRl3n
MD5:	290658E2D190DB48692177016962F35E
SHA1:	B85D937E06535B9B0EB87B8B2207F935EA76A75D
SHA-256:	6FCFD017E2EFE6C8F9EE712A814C73637C3B9FC8BF1376A10A3CD92CE21B6595
SHA-512:	9580EE71DAD7C8030CD3CF05E32B4DF0389C8204153144EFE86AC527A46115D7EA05765BFA0ADA87182BE05837DB81365F8F7D394FB9DEA369CD9D0FD9CEC7E
Malicious:	false
Reputation:	low
Preview:	....

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):	5.470699229996011
Encrypted:	false
SSDEEP:	48:25GGu1D+lHZa7qZMO48dbWP+1uaBbQSefgGucNrS0U9RdiN9dI:71Qa7QM4dbW4bBbQ5fgGu8rS0PI
MD5:	23A33F09EB295E11BE1E6DBC67BB6BA3
SHA1:	9A45F4170469DC8D8D9C3A1263D05DA50AC272B6
SHA-256:	0606EF63A643E8CD3EA63EE68599C9A68FF62CB0A64050BE37F351764257E571
SHA-512:	A579CB608C37F7FE35DAC06550E84F55E5079EB1039B4CCA9D972589449E1EA5F308493931120DE5025D3793B5590A0767438CC8C854584B739DB06301B2FA2E
Malicious:	false
Reputation:	low
Preview:	.2=...*.....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..167397000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-22 01:41:57.50][INFO][mr.Init] MR instance ID: 0d5a593b-4a24-48c2-a5cd-49e1039d8c39\n","[2021-07-22 01:41:57.50][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-22 01:41:57.50][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-07-22 01:41:57.50][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-22 01:41:57.50][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-07-22 01:41:57.50][INFO][mr.CastProvider] Query enabled: true\n","[2021-07-22 01:41:57.50][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):	331
Entropy (8bit):	5.1486654698389085
Encrypted:	false
SSDEEP:	6:m13Wi+q2P923iKKdK8a2jMGIFUtp6amWZmwP6FF39VkwO923iKKdK8a2jMmLJ:8R+v45Kk8EFUtpgW/Pg39V5L5Kk8bJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
MD5:	E344FBB2BD09F5FC27F7D614553B3A0C
SHA1:	954A8AABA84C59F597754AE201E9915DDD8DE5B0
SHA-256:	AB732217E07E609796640ECAE3DABF0A0CBF7E585C41397AAE29F78C8AD2CFEC
SHA-512:	11A9A3FF96F682EAAD210C99060B100C1BECFF9C4AA4E68EA0B28A225383662993A9D7B2F24F25D8CD54CD558795D0B3778EE481C014309B90423CF4FFDCB27A
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:37.783 2cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/22-01:41:37.788 2cc Recovering log #3.2021/07/22-01:41:37.790 2cc 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):	333
Entropy (8bit):	5.142797580958026
Encrypted:	false
SSDEEP:	6:moyq2P923iKKdKgXz4rRIFUtpB7ZmwPBRkwO923iKKdKgXz4q8LJ:zyv45KkgXiuFUtpJ/PD5L5KkgX2J
MD5:	E6A7A8B5E31D6462F4A8DDF50EFAB56C
SHA1:	5BB8C79CD8875F820B320FA3A55E59190128F308
SHA-256:	1643E71DCCE88922890A8D7B49FA5659075769A30AF0F427AE8AA5FF6D887D8C
SHA-512:	A60FBBE7581E28016187E63B8552A61A60CA70668F7B0075B0ED21D5FCB7EE8332680C86CCCFBFD040DF5604180449D5D3063EC243D7B95F5939DC41C6A49A3
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:38.080 d80 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/22-01:41:38.082 d80 Recovering log #3.2021/07/22-01:41:38.082 d80 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	1.084936335405922
Encrypted:	false
SSDEEP:	192:wIElwQF8mpcSAIElwQF8mpcSKBgIElwQF8mpcS2jsij6siv:KBhR6Z
MD5:	FABA76174B1CDE0D09B3AF9CAD5DA17A
SHA1:	04BB77567A23DD5503C8FE6B503B5B8DD73DFBE8
SHA-256:	D8EF9A8DC9D57137527E6DE854BFEA253D5D73F982FD05F17C32A328217D6329
SHA-512:	804FA0567E094B8F0341372864BB99117F3BB0B1243643AB880EC1FAB0C81F294207562EC181CB2352D5440B9571BEFB73E4177033A32E9C732AAD65D2029032
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	79548
Entropy (8bit):	0.872582745164219
Encrypted:	false
SSDEEP:	192:vhIElwQF8mpcSpZxIElwQF8mpcSMx0BIElwQF8mpcSO:vP0x0G
MD5:	20DEED9E58C01C18DF6BE92C09CD2C01
SHA1:	460072E6C09C77FB4637DC8DDE6291376429A945
SHA-256:	CA24927DC9378BFFB5A990430A9C9257C08030B150F45BA43B8A5D671BFEA6B8
SHA-512:	84F63B439DE553767C403E8071C59C7D72A378C757A426D853D873D1F09DE1A1320D00502EA9A6A0477CF6167DDF528F3DDC3B26E7B925287D5D4DC0379E4FB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Preview:	.....q.B..... ....

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
Reputation:	low
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):	322
Entropy (8bit):	5.15714433760527
Encrypted:	false
SSDEEP:	6:m1wuQpq2P923iKKdKrQMxIFUtp6ycZmwP6yckwO923iKKdKrQMFLJ:Fpv45KkCFUtprc/Prc5L5KktJ
MD5:	19CA676B2161685F708DD7364425AE65
SHA1:	827CBB9827F99AE785866B2991CFD15163CB0D14
SHA-256:	B7526EB354F7DEF3B4F0A85FE5C6048A521D369F82062E9B1B2B07AC6C781697
SHA-512:	E58703756EC721C4D9FEEBA40E8E10821DA1EFD92A8B5E7A6A427EDC13D9B1174D4D7DB9C012B599C036AE710F6EB4CC29330AAC66EF34C47C8983857E63692
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:37.980 15a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/22-01:41:37.982 15a4 Recovering log #3.2021/07/22-01:41:37.982 15a4 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):	350
Entropy (8bit):	5.133679035010149
Encrypted:	false
SSDEEP:	6:m1Wdlq2P923iKKdK7Uh2ghZIFUtp65ZmwP6Q9kwO923iKKdK7Uh2gnLJ:j2v45KkIhHh2FUtpO/P/5L5KkIhHLJ
MD5:	2135050AB61E4E0726C5A92D4D06AE43
SHA1:	D0393162E703BCC005D73D9C42DE6944250982E4
SHA-256:	C0185996249476A2FAE8E6631D7A0610766554A6AC359FBA8F81441681E749A4
SHA-512:	F15EA572184A9DB882B810F4989BC815311C83CB7625B31D7DFE95CE8038DE899CDC6CC61A62F658AF0964A26B61C10F0C5050272156A54729EDABEFF3DD642
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:37.753 17b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/07/22-01:41:37.754 17b0 Recovering log #3.2021/07/22-01:41:37.755 17b0 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\19773482-ac05-4b09-bb32-a94b97d13bef.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\19773482-ac05-4b09-bb32-a94b97d13bef.tmp	
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.2408781012425445
Encrypted:	false
SSDEEP:	6:mScjWM+q2P923iKKdKusNpV/2jMGIFUtpsURz1ZmwPHuY+WMVkwO923iKKdKusNA:mjL+v45KkFFUtp1RZ/PHl+LV5L5KkOJ
MD5:	66EB6821E06D8CD6E4B4E2EBB1878752
SHA1:	E7C2C1AED19BE55C4F4D97CCEC55FC184633EB07
SHA-256:	6D58D9B02999652546A6B19CD0182DA34AD6D5C07EE6432116BFC1193277D10A
SHA-512:	D13C8706F0749632A1F20E223FEBB1BD842D9359B14D84C90463DFCEA98AC7966B6EC5E526FF5036EDD73CF32E51E89DE6C8E0E8CDAA290B806F4DF52571308
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:38.024 161c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-01:41:38.025 161c Recovering log #3.2021/07/22-01:41:38.026 161c 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):	434
Entropy (8bit):	5.264344643937454
Encrypted:	false
SSDEEP:	6:miKRFIq2P923iKKdKusNpqz4rRIFUtp/ZmwPtGkwO923iKKdKusNpqz4q8LJ:uMv45KkmiuFUtp//PtG5L5Kkm2J
MD5:	A66AD964FA73D0E3CF2BF0FCAA229117
SHA1:	8BB789E0FB08F076320894D14D410D8191512E09
SHA-256:	93079488875AD842EFA5E6D459753585C78C2459858B3C874E035B5102B58F59
SHA-512:	AEFC8AC964B756EA4C09CD6C118A433818FC27D0747255C0180C8C2046FFE28EFD6DE7EC13558A034993A3E792DE2480D9DA1B5DF32BD6DEF991D64D905E85B
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Reputation:	low
Preview:	2021/07/22-01:41:38.073 15a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/07/22-01:41:38.074 15a4 Recovering log #3.2021/07/22-01:41:38.075 15a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	417
Entropy (8bit):	5.251072539873028
Encrypted:	false
SSDEEP:	6:mE+q2P923iKKdKusNpZQMxIFUtp1WZmwPP9VkwO923iKKdKusNpZQMFLJ:/+v45KkMFUtp1W/PVV5L5KkTJ
MD5:	6C33ADCECAE1E84A7E9BAC6E03AF86CA
SHA1:	35EB8515EB83B581EF19CBB5373C44D0E98E046A
SHA-256:	92A39DAA2A360CF05C8B35FD7BB3975124AC94D69EA41BE241F0B2008A707F99
SHA-512:	A8DF343D7749F0E9607B4C81CD4B25CA964A802BF206205BDCA41BEBDBECE4E7771ED29F966C40FFB2FBD5EB578E05A398B46418FF07F58E641AB0D9307FD8E9
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:54.763 2cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/07/22-01:41:54.764 2cc Recovering log #3.2021/07/22-01:41:54.765 2cc 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\678ba568-9573-46ef-8f00-5dab3911804e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FB27
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.188577293948883
Encrypted:	false
SSDEEP:	12:3Iv45KkkGHArBFUtpW/PKuV5L5KkkGHAryJ:3645KkkGgPggHL5KkkGga
MD5:	3BE3BF8FEF9839A5CC3B7660A1029A8E
SHA1:	0FE966D67A9F962F6BF0BAA0D723E119C5FA8424
SHA-256:	4DA8C9E9C607AE936DBBDE3CE61FA99DE9CC3D4C51F57759B1ECEF56E9798EB1
SHA-512:	FA6DC59BE73B947DE7D2E5CF7960B5A93A54C5BBB5DF214CAF2909FC2FA2E244BB55B3AECF33CEA47EA388496B1F0B290AE9F616B6890891E66AFBDB03C1FC0D
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:54.298 15a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-01:41:54.299 15a4 Recovering log #3.2021/07/22-01:41:54.300 15a4 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):	431
Entropy (8bit):	5.206156250998835
Encrypted:	false
SSDEEP:	12:J+v45KkkGHArqiuFUtpB/PrSV5L5KkkGHArq2J:u45KkkGgCgn0L5KkkGg7
MD5:	C40AC4A4E44053A24D10B7B7FE09056F
SHA1:	1978ED8FD4DAB3C7EA6A1F9BE1C3AC34ED5463C8
SHA-256:	FC0B39648181B6398359B38692B9D7B0617709FA9E85BEAD56981987D965734B
SHA-512:	A7C322248BE66EF0FA24D0E1AA2C6C92751BA1F5AC6722DB924E5D519E81C6DA7FECDB53CF9F75A6A9E756CFEF93D622F315CBD8A05BFAECDD608D1DCF7A7022
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:54.311 82c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/07/22-01:41:54.315 82c Recovering log #3.2021/07/22-01:41:54.316 82c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	417
Entropy (8bit):	5.130282927580202
Encrypted:	false
SSDEEP:	12:2m+v45KkkGHArAFUtpGi/PGWIV5L5KkkGHArfJ:2v45KkkGgkgozHL5KkkGgV
MD5:	DDD14FDDB03370CBB0712326DBB97B6C
SHA1:	C422BD40AE9E0998BE629F0ED19C014DB3930459
SHA-256:	40D3F792099F34F2834F56B83795B28B7727630EBD6290A09DBE0ADC3CDC879D
SHA-512:	2C43F5639261F69070E1F196EB414969D1287E545C1BE4BE43555453ECB323EFD50FF3147320DD6A14B2C2D27CE05E8832A6C8D968AF41CDBE3018991E175F5E
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:42:10.239 82c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/07/22-01:42:10.240 82c Recovering log #3.2021/07/22-01:42:10.241 82c 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\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.198358215583921
Encrypted:	false
SSDEEP:	6:m18BIq2P923iKKdKpIFUtp6sZmwP6MkwO923iKKdKa/WLJ:liv45KkmFUtpf/PN5L5KkaUJ
MD5:	8D3383D9CCCB36FD2D1FA76FF32C0499
SHA1:	28FBE767951E72D601604918675CDEF256D4A4FA
SHA-256:	292C9B0CB3323316AB9377619372A0C87545F8B247B93E2C583D8CA553F6B1A3
SHA-512:	C3395D31D6B4DD789C845F2641DB6FF24B45032C7DC035BFE66F2DC0326A87D65344C9873518D71652B9959A438758C21054DFB613991F00B3B343A695634975
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:37.747 15e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/22-01:41:37.749 15e4 Recovering log #3.2021/07/22-01:41:37.749 15e4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.304884541102643
Encrypted:	false
SSDEEP:	12:8Zxv45KkkOrsFUtps1/PscP5L5KkkOrzJ:045Kk+guBL5Kkn

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
MD5:	D68087FA4CEF59B258F547B1C49AB221
SHA1:	D5C538306602E7CC39D881A57B975DBCB8DCC58E
SHA-256:	4360117B289E78B94674DDD24273D2DFED1022D912087F384C04897AE86127E0
SHA-512:	8D3B6823D24CCE9A754A19299FB6E2CF744C98BEEE2185B460F65495D78A603983011ECA506E86A8AD69F1120416787DE46A46E2861D2AEE4D5B4899177CA2E3
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:57.559 1560 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/22-01:41:57.561 1560 Recovering log #3.2021/07/22-01:41:57.562 1560 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	3.9387218755408684
Encrypted:	false
SSDEEP:	3:jxvyllINn7Fn:j8llX
MD5:	C851A4FA25CFB68B431542364CBF4643
SHA1:	F6B1F2E00DC4D136ACD079C886B0C66CD97F56D9
SHA-256:	00DBB0E687B28E0E9252150E3772211337AFA226372EAB21209A8F2F9E560B9D
SHA-512:	FA777A8166E97DA0D9EE431AB4D6357491B9FA46078BD11820379A31BDA854E7BF841AC9DEC5E126D00174FBFB5BB9BD97A81F239CD3778E8CA002B5968F840 3
Malicious:	false
Reputation:	low
Preview:	....G.....N....h...0VQ.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\013746d1-4c2c-474c-9ad7-7d6745933e04.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E.....I...k}....{.m.t.CP.....E...\.....=H...A..,J..;P.....nn p}nnp}.....~~~.....!...!---2---2... .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P.. .Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e..... ....nnnzXXXa.....RRR\.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168 B6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Preview:	F......r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a541d2cb-37ba-4265-9450-b472a013e93f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	874
Entropy (8bit):	5.552785910980076
Encrypted:	false
SSDEEP:	12:YdDZ6Hk3O+UAnIvld06cY8rNgmh4r+UAnIEllWcNnYj+UAnIECmtn+R7N+UAnIOh:YT6H0UhHPkG1KUe9aUeCJ7wU+pBRUeIQ
MD5:	09B8E104505368AD55F90BB2CD11DB17
SHA1:	D675C4F8A3DA685C78F8A45A773F5C9A0BD1822B
SHA-256:	2EA7A6EA34BF4F4B4825E97777065E7C81546ED63BEA41B4D26AFBEDC6A3B631
SHA-512:	27E00EBE36895DB198DD0C510DD017A38EE3D714869D7F96FA72A4F03FFA3118D359625387833A0AEFCB23D56F81B1C34844BDB21E099E1812F81359FA2DCED
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQlM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1658479301.337317,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626943301.337322},{"expiry":1633013028.952627,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.95263}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c4955e92-8b7c-4188-9eee-b70b929a6da1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d03ae835-d26c-40c4-9108-d1b71d0fb9b7.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):	3257
Entropy (8bit):	4.8794723351978995
Encrypted:	false
SSDEEP:	96:JnOTXDHzSN50L+hSWxC56N6651GHMVf0xhVD:JnOTXDHzSH0LwSWxC56N66518Wf0lD
MD5:	A17BE1C4FD6B40921E313A34D8621B1A
SHA1:	71F86EAD15ACD0DDB609B94FB5A48E029EBF6146
SHA-256:	EDF122D43C03433256CE715960839DADB20724B8FC72060D95AF8FAAAB721DC7
SHA-512:	C59CCC1A2B2C7BDFDBF8B1BF235A6618E3B61CC704B26DC6B144F5ED7E296A748D74204C30BDEBCCE358F051B7865ED68CA3C22545E2570F03E2140FD5555B8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274008901296101","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274008901337234","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"isolation":[],"server":"https://bit.ly","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.4379523822480005
Encrypted:	false
SSDEEP:	3:tUKIgr+11Zmwv32gzXx1V8s2gzXx1WGv:mMA1ZmwP7bVv7btv
MD5:	12D0E19EF27E99BFEA88F6F993535AB9
SHA1:	12E38531BC5162ADBDD01BBD3113FF04D9E82683
SHA-256:	10E4EF00703DE8FD06F77C5F0391AE6D3326F21E898A6860284A756A967360B2
SHA-512:	C106126D13EC6B67D66FE6E55AA147927F28643B6488DAE0D71F0A135DC021050854E555D33801537B14621BC053C051E9E57271F946AE4F9D3C9C2BDD04EBFE
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:49.912 1570 Recovering log #3.2021/07/22-01:41:50.036 1570 Delete type=0 #3.2021/07/22-01:41:50.036 1570 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e4382a79-d58a-4a7f-87da-a582ffab80be.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:	modified
Size (bytes):	22595
Entropy (8bit):	5.535549836164556
Encrypted:	false
SSDEEP:	384:le9tJLll4X31kXqKf/pUZNCgVLH2HfDdrUTHGknTA9fv4l:bLlc31kXqKf/pUZNCgVLH2Hf5rUzGknd
MD5:	B8CA495360A8EDCF08FC35D380DC72BF
SHA1:	6D11FFF2EB51EEA63BD196020AEE6E9C3FC7B62F
SHA-256:	5611732A812495E8334BE9783CBE323B50AFCC99C23733A70D0AACF2EA1B726E
SHA-512:	0F17C85046BF4A8AB035625D7B9FEF2AD6763540D8EE3BDB3F6C1CDF423F9B9CB2EADE5338D6568C036EC7C1DC484294412F94177320A332827BA2931906774
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e4382a79-d58a-4a7f-87da-a582ffab80be.tmp	
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":"13271416897739838","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\f619dc1a-d0be-458d-85fa-a5e521400f98.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):	5109
Entropy (8bit):	4.969322882364069
Encrypted:	false
SSDEEP:	96:nnr4GGMpSKISoIk0JCKL8cM7Ekj11TbOTQVuwn:nnrQMpSfC4KphkjX
MD5:	B1E3981B57841720D70577224BEBB782
SHA1:	E074CFF8E45998EBB10C5AC21A2DE760FED2192C
SHA-256:	0A65AEC806225D44F334956736AC9734D9B30FF2D500F79597AE588A26052DE4
SHA-512:	3947076D56A12FA798B7771F9879577E0211B1D962827A544F8C4F7C62C0ED17C735EF7529EFDB8713E728E5F70F3B0EFC647C2B628C190891571B6994E3EAC6
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271416898048991","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["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):	337
Entropy (8bit):	5.19416618089827
Encrypted:	false
SSDEEP:	6:m8XRF39+q2P923iKKdKfrzAdIFUtpEAWZmwP4VFb9VkwO923iKKdKfrzILJ:h9+v45Kk9FUtp9W/P4T9V5L5Kk2J
MD5:	DAEFFF4D21156FC464186A57941521D0
SHA1:	7D27031BFC5C7BD3A7E77AC351F90107B2BEAE4F
SHA-256:	C33C47DF712DA8362C859896BCC880233F028649C54BD64355468D33EFE7562F
SHA-512:	7FE3D2ED467DD331C9AEDD46195DE747D9192F715BB7CFF390DAC13A592EE775878F75920F98B859FD0818CADBFC9D1CDC4E0513E028CBCA0B869EAC6A009 5E
Malicious:	false
Reputation:	low
Preview:	2021/07/22-01:41:56.512 2cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/07/22-01:41:56.519 2cc Recovering log #3.2021/07/22-01:41:56.520 2cc 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:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\a5a0e8fc-4531-4afe-819e-04e7a966577b.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):	365373
Entropy (8bit):	6.015126479667403
Encrypted:	false
SSDEEP:	6144:aExzgRx37iWYFW8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBI:aizgRAxzurRDn9nfNxF4ijZVtilBI
MD5:	63CE5CF5EFA9387E85F5D0626E8C68C1
SHA1:	1C1A72374BA768F53A30F52ED821D4148C15F04E
SHA-256:	E428619AE923C4E993DCD8BEE5B775114CB95683D55B7B3B2A29461B038326DD
SHA-512:	F6FDA827D039E7C7B78E7A9DA3BF890E75EE05B3537074F1494D4A553521BB029C0CE89F0A812849BB264EAD2361E666B024B296AB9FEB3FC38C60898AE0CEA F
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":1.626943300553179e+12,"network":1.626910902e+12,"ticks":6945920597.0,"uncertainty":3795734.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327141689766

C:\Users\user\AppData\Local\Google\Chrome\User Data\b5d92db2-2909-4a30-9b1c-5a17f7f5c7f4.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):	365373
Entropy (8bit):	6.015126830886963
Encrypted:	false
SSDEEP:	6144:mExzgRx37iWYFW8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBI:mizgRAxzurRDn9nfNxF4ijZVtilBI
MD5:	51BCA3204C630E2524328ED053F276A7
SHA1:	E74645C7EAD81BE1089446543F61A081AF8D321D
SHA-256:	2C55D7860032D4D977F49FC53D5C6E545BD326CC676EF0B23073B2C0F5BFE24F
SHA-512:	7B388A81BC80F54695C278F149021B82EFD9AB43D7A14F15D0825558E96A17A0A0709662059CD5AA08C2EF003781DB0E4C26296C4CDD06389FDBB7BA76D4330
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":1.626943300553179e+12,"network":1.626910902e+12,"ticks":6945920597.0,"uncertainty":3795734.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075773862"},"policy":{"last_statistics_update":"1327141689766

C:\Users\user\AppData\Local\Temp\13a01df6-7808-4bed-977e-5d0d5bfaa295.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

C:\Users\user\AppData\Local\Temp\13a01df6-7808-4bed-977e-5d0d5bfaa295.tmp	
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\3ac89089-5989-4bf4-b897-920c99ff9380.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\816fbc22-bb51-423a-b064-5ac2d7852034.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;..._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\8430899a-f1a2-482f-8422-82464c9835ed.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

C:\Users\user\AppData\Local\Temp\8430899a-f1a2-482f-8422-82464c9835ed.tmp	
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	15606
Entropy (8bit):	4.643957801284171
Encrypted:	false
SSDEEP:	192:z0f/UOIIBWM7kZp/rIV2pf+oiO6wNxPwZJWSxOROIK/r45kxWP:z6U7kzoAf36wa8MlKz4n
MD5:	3610E88C66B6554A62BB724E4C197F93
SHA1:	E7E3F40A928B2FC51C147D7B0CC6DE52BCB96EA5
SHA-256:	390A5A409E8339AE100DC6C78DE2C15B11B60D4C7F85498768041DF802788783
SHA-512:	3595ED608304E0BBC6AC4A6D31C549404167C2138F88F43842D41DAD0DE403FE4EB0CB84D216C387D6779BF8CBB2A431C685A58C4C4439E7116863ACE922485
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET b1e79ba1c63aca3688cf75a4ae1b933567caaaf62f19a19e01238c2248ec9cf2 679c970f4f139ff11e16e1fcc49677637 505c9c9f1073b2d08416e2cf3723969.SERVER_HANDSHAKE_TRAFFIC_SECRET b1e79ba1c63aca3688cf75a4ae1b933567caaaf62f19a19e01238c2248ec9cf2 b b3fd92340ba08af52c9d5826f236303c02edc4e65fb8c5bda608cb7b19ba30d.CLIENT_HANDSHAKE_TRAFFIC_SECRET efea38a8f8f444f13c69b54f22b4e1f2dc 6cffcc49e689da438991535d619b77 1f471c7fcc4639c730709004d9eb1011fe775e7fd135a780ce76e13ffc1981e3.SERVER_HANDSHAKE_TRAFFIC_SECRET ef ea38a8f8f444f13c69b54f22b4e1f2dc6cffcc49e689da438991535d619b77 1be6e8ac8fc7bba21e9300bb9ae407422cfbcc128973b8fa23b6388365f3d94e.CLIENT_HANDS HAKE_TRAFFIC_SECRET e89acc785bc5bde0dfd0066faa088cc198bababcda09e70e7e88fcd792593011 856c4e0f3831368adc749056f55a57b99779f7d91c78a 89861a267cde646e936.SERVER_HANDSHAKE_TRAFFIC_SECRET e89acc785bc5bde0dfd0066faa088cc198bababcda09e70e7e88fcd792593011 64a4f102f095a d2c47307ca5d4f83dcd4e5b84d6c1fad35e2df453d964311eaa.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\dc43c9f8-0d71-4e30-b8ce-0de9add1ab74.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..& ..l.6r[yU...%..f.....N..V.....<+.....l.}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,.. .W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6.. @?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\df746303-f45c-462d-9a7c-9ef5d9dc9c93.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\3ac89089-5989-4bf4-b897-920c99ff9380.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l.}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\cs\messages.json	
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C53E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\el\messages.json	
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir768_1231487582\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

Static File Info

No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-01:41:43.564442	TCP	2515	WEB-MISC PCT Client_Hello overflow attempt	49744	443	192.168.2.5	52.217.134.120

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 01:41:41.572846889 CEST	192.168.2.5	8.8.8.8	0x5e98	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:41.590662956 CEST	192.168.2.5	8.8.8.8	0xe7e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:41.601324081 CEST	192.168.2.5	8.8.8.8	0x29e7	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:42.736963987 CEST	192.168.2.5	8.8.8.8	0x4dc9	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:42.739250898 CEST	192.168.2.5	8.8.8.8	0xd59f	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:42.756776094 CEST	192.168.2.5	8.8.8.8	0x19b0	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:42.795491934 CEST	192.168.2.5	8.8.8.8	0x74d8	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:43.437091112 CEST	192.168.2.5	8.8.8.8	0xea92	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:43.437186956 CEST	192.168.2.5	8.8.8.8	0x57e1	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:46.876543045 CEST	192.168.2.5	8.8.8.8	0xe892	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:50.621187925 CEST	192.168.2.5	8.8.8.8	0x3282	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:50.920727968 CEST	192.168.2.5	8.8.8.8	0x343	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 01:41:41.630038023 CEST	8.8.8.8	192.168.2.5	0x5e98	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 01:41:41.630038023 CEST	8.8.8.8	192.168.2.5	0x5e98	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:41.650578022 CEST	8.8.8.8	192.168.2.5	0xe7e	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 01:41:41.653666019 CEST	8.8.8.8	192.168.2.5	0x29e7	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:41.653666019 CEST	8.8.8.8	192.168.2.5	0x29e7	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:42.786828041 CEST	8.8.8.8	192.168.2.5	0x4dc9	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 01:41:42.799918890 CEST	8.8.8.8	192.168.2.5	0xd59f	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:42.799918890 CEST	8.8.8.8	192.168.2.5	0xd59f	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:42.816775084 CEST	8.8.8.8	192.168.2.5	0x19b0	No error (0)	use.fontawesome.com	use.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 01:41:42.844832897 CEST	8.8.8.8	192.168.2.5	0x74d8	No error (0)	s3.amazonaws.com		52.217.134.120	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:43.189697981 CEST	8.8.8.8	192.168.2.5	0x1a15	No error (0)	gstaticadssl.l.google.com		142.250.186.67	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:43.496901989 CEST	8.8.8.8	192.168.2.5	0xea92	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:43.496901989 CEST	8.8.8.8	192.168.2.5	0xea92	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:43.500461102 CEST	8.8.8.8	192.168.2.5	0x57e1	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:43.500461102 CEST	8.8.8.8	192.168.2.5	0x57e1	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:46.937796116 CEST	8.8.8.8	192.168.2.5	0xe892	No error (0)	s3.amazonaws.com		52.216.112.61	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:50.671844006 CEST	8.8.8.8	192.168.2.5	0x3282	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 01:41:50.671844006 CEST	8.8.8.8	192.168.2.5	0x3282	No error (0)	clients.l.google.com		142.250.185.238	A (IP address)	IN (0x0001)
Jul 22, 2021 01:41:50.989036083 CEST	8.8.8.8	192.168.2.5	0x343	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 01:41:50.989036083 CEST	8.8.8.8	192.168.2.5	0x343	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 01:41:43.168953896 CEST	52.217.134.120	443	192.168.2.5	49730	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jun 23 02:00:00 CEST 2021 Tue Dec 08 13:05:07 CET 2015	Mon Jul 25 01:59:59 CEST 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 01:41:43.323436975 CEST	52.217.134.120	443	192.168.2.5	49731	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jun 23 02:00:00 CEST 2021 Tue Dec 08 13:05:07 CET 2015	Mon Jul 25 01:59:59 CEST 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jul 22, 2021 01:41:43.723512888 CEST	52.217.134.120	443	192.168.2.5	49739	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jun 23 02:00:00 CEST 2021 Tue Dec 08 13:05:07 CET 2015	Mon Jul 25 01:59:59 CEST 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jul 22, 2021 01:41:43.725214005 CEST	52.217.134.120	443	192.168.2.5	49744	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jun 23 02:00:00 CEST 2021 Tue Dec 08 13:05:07 CET 2015	Mon Jul 25 01:59:59 CEST 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jul 22, 2021 01:41:43.726474047 CEST	52.217.134.120	443	192.168.2.5	49740	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jun 23 02:00:00 CEST 2021 Tue Dec 08 13:05:07 CET 2015	Mon Jul 25 01:59:59 CEST 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jul 22, 2021 01:41:43.726675034 CEST	52.217.134.120	443	192.168.2.5	49742	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jun 23 02:00:00 CEST 2021 Tue Dec 08 13:05:07 CET 2015	Mon Jul 25 01:59:59 CEST 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 01:41:43.727729082 CEST	52.217.134.120	443	192.168.2.5	49741	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jun 23 02:00:00 CEST 2021 Tue Dec 08 13:05:07 CET 2015	Mon Jul 25 01:59:59 CEST 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jul 22, 2021 01:41:43.729038000 CEST	52.217.134.120	443	192.168.2.5	49743	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jun 23 02:00:00 CEST 2021 Tue Dec 08 13:05:07 CET 2015	Mon Jul 25 01:59:59 CEST 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 768 Parent PID: 3904

General

Start time:	01:41:36
Start date:	22/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://bit.ly/36R4geg'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Copyright Joe Security LLC 2021

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 2968 Parent PID: 768

General

Start time:	01:41:38
Start date:	22/07/2021
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=1544,13602693734026748389,18434443092193835822,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1720 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 6672 Parent PID: 768

General

Start time:	01:41:45
Start date:	22/07/2021
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=audio.mojom.AudioService --field-trial-handle=1544,13602693734026748389,18434443092193835822,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=4720 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Copyright Joe Security LLC

Copyright Joe Security LLC 2021