ID: 458988
Cookbook: browseurl.jbs
Time: 00:55:09
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

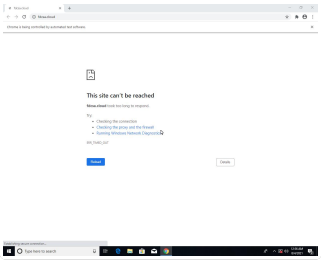
Windows Analysis Report http://fdcsa.cloud/

Overview

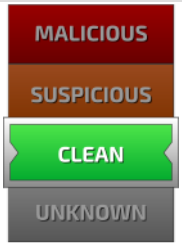
General Information

Sample URL:	http://fdcsa.cloud/
Analysis ID:	458988
Infos:	

Most interesting Screenshot:



Detection

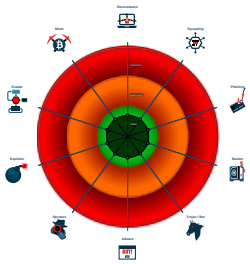


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5620 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://fdcsa.cloud/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5784 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1616,316435080101015694,4571778294657744348,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /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

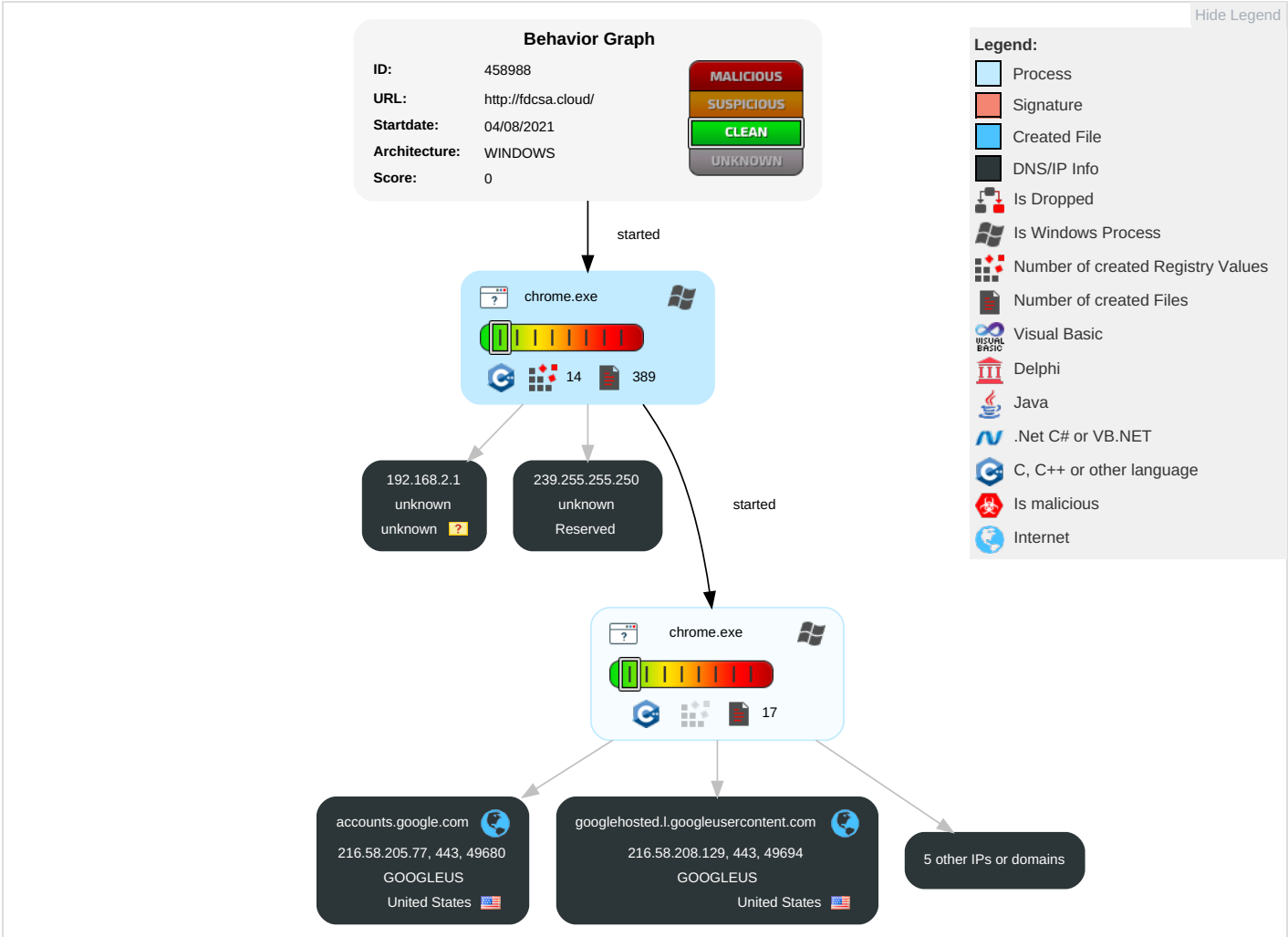
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

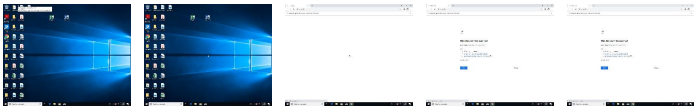
Behavior Graph

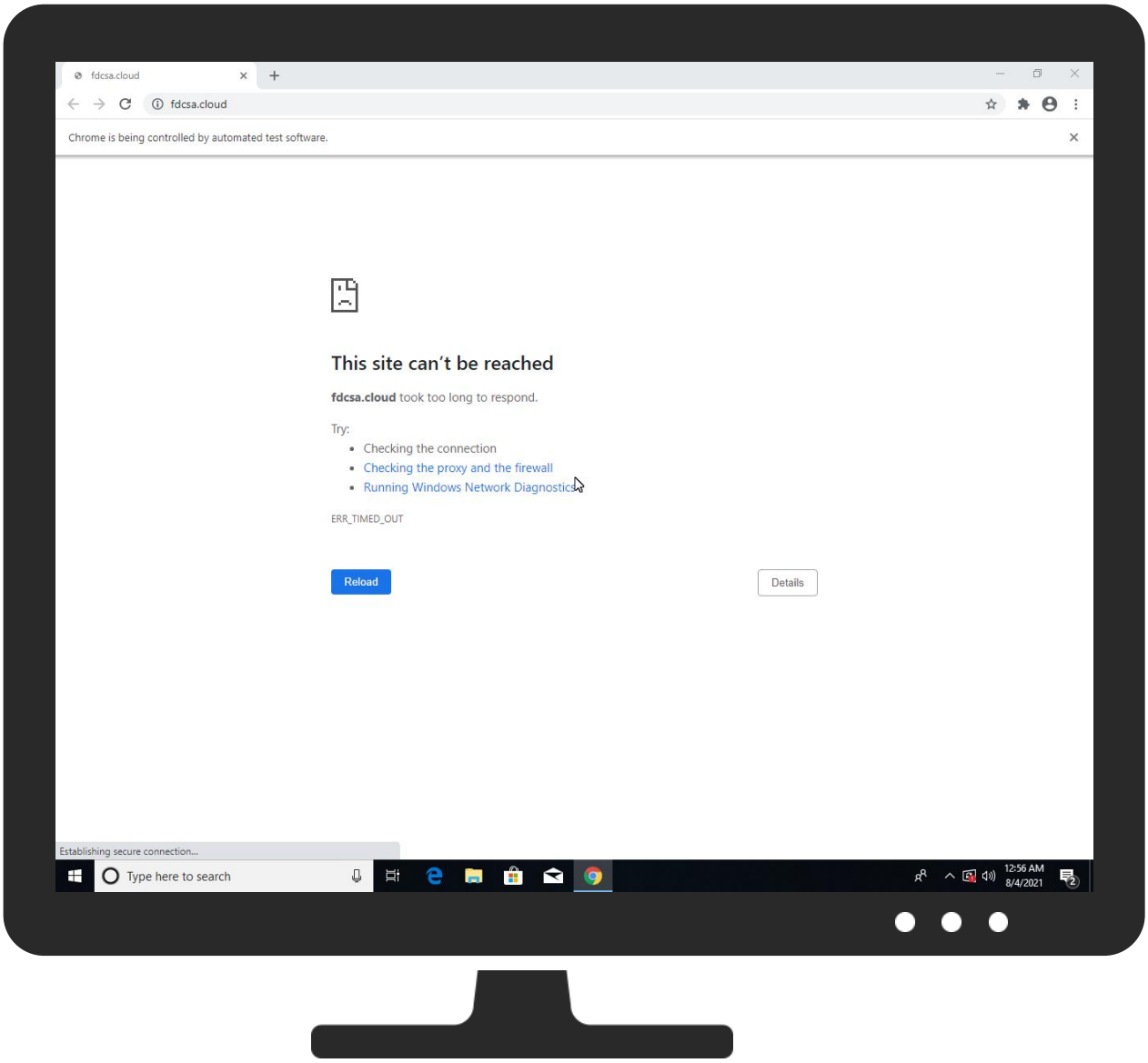


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://fdcsa.cloud/	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://dns.google	0%	URL Reputation	safe	
http://https://fdcsa.cloud/	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://fdcsa.cloud/t	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.205.77	true	false		high
fdcsa.cloud	162.0.217.32	true	false		unknown
clients.l.google.com	216.58.208.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://fdcsa.cloud/	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
162.0.217.32	fdcsa.cloud	Canada		35893	ACPCA	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458988
Start date:	04.08.2021
Start time:	00:55:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://fdcsa.cloud/

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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@31/199@4/7
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
00:56:01	API Interceptor	1x 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

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic

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

C:\Users\user\AppData\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:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2A0
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\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.145340414441777
Encrypted:	false
SSDEEP:	6:kK0doW+N+SkQlPlEGYRMY9z+4KlDA3RUeIID1Ut:s5kPlE99SNxAhUe0et
MD5:	32930DEC4A36F222F545AB6B4CDFAEDF
SHA1:	635E8A875C6D727608AE510280AEC916EC37CC80
SHA-256:	FC6619D0ADABBCA7CC989F0671A43FA9F0EE8B3F2360A13B2AE26E0F4D132E6F
SHA-512:	5A37A33E4133EF8B9116023606F2F86A9DF0CADC0FEE26A14889B8C3E9AD520C29BA6E85FFB2DF052E4DA7F158B686435449A6456C63D5391FD68439360DF0B9
Malicious:	false
Reputation:	low
Preview:	p..... .....*....(..... .....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\Local\Google\Chrome\User Data\39b6b98b-7d12-40c2-b97d-752d91bbedae.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):	174336
Entropy (8bit):	6.079379051247693
Encrypted:	false
SSDEEP:	3072:FXNGaYTJQE+mugy9+QV1T7IRwdfLSNPtFcbXafIB0u1GOJmA3iuRd:BoxaV+QfT7GSmhraqfIlUOoSiuRd
MD5:	299FBAC1D852FC15D5CABDDA32718E1F
SHA1:	CD95ED6FDD85FA9A3D5981566C04DF214BE2F191
SHA-256:	EE562FC01275DEA203EE6DBC87921F9A516DB00F3848C9F6DBBEBBE415D6B9A2

C:\Users\user\AppData\Local\Google\Chrome\User Data\39b6b98b-7d12-40c2-b97d-752d91bbedae.tmp	
SHA-512:	4F09D6853CC0552958E7075B846AB57CA0D6B4A05868D21B3470B75878B402A9B63A8371C0F8FF58E3E6B4A610F89E737AF163FDF8E57260FF1AA73F4CE296E6
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":1.628063760190436e+12,"network":1.628031361e+12,"ticks":5991353101.0,"uncertainty":2836332.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016956081"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\6360e0a7-6e46-4589-871d-a10cd40f8b1f.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):	165869
Entropy (8bit):	6.0496007940510035
Encrypted:	false
SSDEEP:	3072:e9GaYTJQE+mugy9+QV1T7IRwdfLSNPtFcbXafIB0u1GOJmA3iuRd:e4xaV+QfT7GSmhraqfIlUOoSiuRd
MD5:	DB15B838E46070DA40AADFF712AF7526
SHA1:	6E5E7E00A542FA520749D8EBBABB58C64DE00324
SHA-256:	F6D7B92C7B53D1D8C0A0131E0A5494E056A2AAFC8B833A52A17EAB5AE88FC10C
SHA-512:	70539B42BCEA0281B109A7BECEDA064FE84F3DBF45F0A0360CF44DDFC58BCBB0CB7DEDD337C08FE016740E3417F6D82871EA4A39FFCFB2804D9F090343BE4F4
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":1.628063760190436e+12,"network":1.628031361e+12,"ticks":5991353101.0,"uncertainty":2836332.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016956081"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\725e4c38-90b5-4875-b707-1c5f7ea85135.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):	174336
Entropy (8bit):	6.0793790995946
Encrypted:	false
SSDEEP:	3072:7XNGaYTJQE+mugy9+QV1T7IRwdfLSNPtFcbXafIB0u1GOJmA3iuRd:ToxaV+QfT7GSmhraqfIlUOoSiuRd
MD5:	3EEED448AE95273FF103C1D8B4C06646
SHA1:	EC4AE80153C126E50F33956A903659D56A30B2FA
SHA-256:	05D1907630B2064BE20CFA3024C0077ED6BF83C189DBCD9A79BBBE84F2CFE483
SHA-512:	E009DB3F05CBEA33EF0688D569E7564466B31FC84499E4CC9227039206A0ACA6C897454F925902F2C1C0D1A55D2FDF72C77BD86B57CA736734910237FEFA24F
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":1.628063760190436e+12,"network":1.628031361e+12,"ticks":5991353101.0,"uncertainty":2836332.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\75555033-d9d4-495c-8d13-3ef9bc2ba0a8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7495579362895044
Encrypted:	false
SSDEEP:	384:Fr4XHdaEh+lZVmsb2Njrov/l3IXdkHtkGkTrOJT/x4p59YrSvmKtKVrbLUORZDNS:lG61VSBkUcer/RBw3/ONKPlL5yx
MD5:	45E2652BFC7C268E836EFFC7EE75F9F9
SHA1:	77BEFE8280316AB515171C06CC6CBE6F2E54D778
SHA-256:	68D0D9718AF82A72611F9DF55507A9BE5F3803F56BC77805FB391B158F452593

C:\Users\user\AppData\Local\Google\Chrome\User Data\75555033-d9d4-495c-8d13-3ef9bc2ba0a8.tmp	
SHA-512:	2B8A96FF3AC604B55B1CE7C0977AD6BC30F375C2F14EC73C84FDDE4DDFFBDAC3696CF352EB592EE1CCB2D87400BA4DF1951EDC3934BBC19F7ED2C9C4B1E5D50
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.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\8a03defb-434f-4ac0-84ba-9295167521ca.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7497034153043542
Encrypted:	false
SSDEEP:	384:Lr4XHdaEtlKb2Njrov/l3lXdkHtkGkTrOJT/x4p59YrSvmKtKVrbLUORZDNG1jCj:w61VSBkUcer/RBw3/ONKPlL5B
MD5:	4BC2E0E315570CBCFC5F3A336682C8EE
SHA1:	E12AC84E9C86D778B9ACD193A82A899488063962
SHA-256:	175FC86842BCA8E856509039B2D728C2975569271919B5499E6E976C33EF4FAC
SHA-512:	9E9FAD09742519865ACDFFFB7BFEB17898D40792F8C7AC734A87DFE98D24C395FE90589B7AC408F3A36CA165A86EC3A6DEB9D73AF27154BDA7553EA220AE7E5E
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....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\589f4a07-1348-4da3-bd04-5f9d864b958a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22594
Entropy (8bit):	5.535857807722992
Encrypted:	false
SSDEEP:	384:aj0tkLlYEX61kXqKf/pUZNCgVLH2HfD4rUnHGUnTH23e4Z:iLlX61kXqKf/pUZNCgVLH2HfMrUHGUne
MD5:	82CA6FDA11FD868FFC707F1122FA6AEE
SHA1:	7FFDFCB027DB6A1DAA7338EC9DD574A570FED77D
SHA-256:	55C6E988F23311F96D46AEAFEF6F7B3DEDC566F46935C14EF15B69E935926A8A
SHA-512:	185E34E0EFA08F51151F8F1DCEBDDC1A997695EEC81F8592E241E6E8C8395524977CE6A0546FF7A081DB2BA200861087A8DFD114E31D8CD1122122ECD37C66F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\589f4a07-1348-4da3-bd04-5f9d864b958a.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":"13272537357950859","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\67dde7ba-e552-4549-8bc2-584627d9aa84.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\84ccd211-bfb7-4cba-a89a-11421272791a.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):	5461
Entropy (8bit):	5.18056389087524
Encrypted:	false
SSDEEP:	48:Yc+UklSLklwHjvcnqApLqqjoL8S+/Rp4lYqlQKHoTw0iOH3CH3G/s8C1Nfct/9Bp:nQCmqqL9xGcKIfok0JCKL8VbOTQVuwn
MD5:	C5AF104F41A0A5749DC8BA012F3EC03A
SHA1:	6A5B4C3D9039046764F9D3BC1C1393BA24A7341A
SHA-256:	FFAB4A2A613E2200ACBA6F3D8DC9D3F9B4D0171856F93C4DA49E5193CAFD58C2
SHA-512:	6A969CEB51609AE0CFAFE36D1EBAAF17D8C167119E6AAE11EE9DC855E76BBDCDD0DFD295A648B15AE15436B6721EF927F8A2F1CA938F47BB1B57CA6CBCC8E9CA
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272537358253419","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9c70dfbb-5d70-4cde-9543-dae20d57e8d7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2042
Entropy (8bit):	4.901059181904288
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5s8JRLs4Tsb5SR3sSZDshyKs13gYhbD:JTnOCXGDHz97O2gExhH
MD5:	7D08300C1EDD154BD7E90320714FADC3
SHA1:	11E02C453C1A23B3814E2242DD2E134F1F6E0D99
SHA-256:	65757AE9BABF4EDEB1E7CE29C86903B2C94A2B688B28EE9F2877A8B70B08A015
SHA-512:	167A22B5A50B070A37AD4C6097CF7CE0FFEE91C59192BE1B1E1FFBDE0F5E27688B9FC9CC072CF51DAD4A611134ECCF16B28C18F6E7F33F7719DCFD7925D6F A9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9c70dfbb-5d70-4cde-9543-dae20d57e8d7.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275129361049282","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275129361136326","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.201613867687401
Encrypted:	false
SSDEEP:	6:mo/Wt+q2PWXp+N23iKKdK9RXXTZIFUtpb0ZmwPbecVkwOWXp+N23iKKdK9RXX5LJ:Cova5Kk7XT2FUtpQ/PH5f5Kk7XVJ
MD5:	0E572C414F9BBAD109C16B0030AF7F70
SHA1:	64380133BCFC54BD8B02D3C70DBFADA8B90CFE63
SHA-256:	6DCCD7EE609C0134A50C22A9ED1029C55499E678324C5BF3B259B4E45A4A346B
SHA-512:	6666CC36B931CB13FDD9EEDA80C45179A971B4F0B3FCAD9303FBAFB2A84434390F03742D268326B43C760F89616B5658156A2287C4011EDE200D29C99514E31A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.055 1538 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-00:56:05.057 1538 Recovering log #3.2021/08/04-00:56:05.058 1538 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\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.201613867687401
Encrypted:	false
SSDEEP:	6:mo/Wt+q2PWXp+N23iKKdK9RXXTZIFUtpb0ZmwPbecVkwOWXp+N23iKKdK9RXX5LJ:Cova5Kk7XT2FUtpQ/PH5f5Kk7XVJ
MD5:	0E572C414F9BBAD109C16B0030AF7F70
SHA1:	64380133BCFC54BD8B02D3C70DBFADA8B90CFE63
SHA-256:	6DCCD7EE609C0134A50C22A9ED1029C55499E678324C5BF3B259B4E45A4A346B
SHA-512:	6666CC36B931CB13FDD9EEDA80C45179A971B4F0B3FCAD9303FBAFB2A84434390F03742D268326B43C760F89616B5658156A2287C4011EDE200D29C99514E31A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.055 1538 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-00:56:05.057 1538 Recovering log #3.2021/08/04-00:56:05.058 1538 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.189134635611307
Encrypted:	false
SSDEEP:	6:moKN+q2PWXp+N23iKKdKyDZIFUtpbUNZmwPbURVkwOWXp+N23iKKdKyJLJ:uIva5Kk02FUtpA/Po5f5KkWJ
MD5:	F1AC9A5E350E28331160C40F660EF13E
SHA1:	7792ADF609D511A1338EE69199427D48744A2BDC
SHA-256:	DD59CE2C6A3912360C753EC057404CD6AF7AE8A219A80EE40E95FF91DE5EA9F8
SHA-512:	48E517165C01036190ECDBE536D7C8A155BEA7F1DF34FFCF6207C246297282868E21F754E25B7423330208AB891DFC1DA82A024D9E15A15CAEA7CDFB5C0FD89
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.046 1538 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-00:56:05.048 1538 Recovering log #3.2021/08/04-00:56:05.048 1538 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old (copy)	
Size (bytes):	318
Entropy (8bit):	5.189134635611307
Encrypted:	false
SSDEEP:	6:moKN+q2PWXp+N23iKKdKyDZIFUtpbUNZmwPbURVkwOWXp+N23iKKdKyJLJ:uIva5Kk02FUtpA/Po5f5KkWJ
MD5:	F1AC9A5E350E28331160C40F660EF13E
SHA1:	7792ADF609D511A1338EE69199427D48744A2BDC
SHA-256:	DD59CE2C6A3912360C753EC057404CD6AF7AE8A219A80EE40E95FF91DE5EA9F8
SHA-512:	48E517165C01036190ECDBE536D7C8A155BEA7F1DF34FFCF6207C246297282868E21F754E25B7423330208AB891DFC1DA82A024D9E15A15CAEA7CDFB5C0FD89
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.046 1538 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-00:56:05.048 1538 Recovering log #3.2021/08/04-00:56:05.048 1538 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
Malicious:	false
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):	0.9686612645327055
Encrypted:	false
SSDEEP:	24:0cLgAZOZD/TfqLbJLbXaFpEO5bNmISHn06UwB8:08NOZ7q5LLOpEO5J/Kn7Uq8
MD5:	8757B0466AA33E58BA9FA9E33B00AD33
SHA1:	F9BA2E2784B2632134113840B7F1696944417008
SHA-256:	02E496F150B763E3199C68321B8B7EE8DC929D04522B1B77C9F205BF65756988
SHA-512:	ECDACF158C7EE73F997609383E0A725F4945BD3005703B6B4701DE772CC05FA80C47F35DD5285F3E0CA15F90E180E0AB846FBA2357C626E1AC1095E0B626F1A
Malicious:	false
Reputation:	low
Preview:	....

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):	901
Entropy (8bit):	3.0672881592418917
Encrypted:	false
SSDEEP:	12:3olydJh0vnz/TPlpxlpN8kIyTd1oameOqXBlptlpl:34SuPLLlrlAa1/mxwlLlL
MD5:	237D08C4A728FCCD6557D523108C5E6D
SHA1:	424110A573A0CBA98DD4039705A88D136BAD2411
SHA-256:	BC151C008245F6D5200F6DA93A2C759AC6671D3F5D40F6DD5015D195F3342968
SHA-512:	75B4EBB9CD936F794FFB88992F8547F9542525D19FF39987ED7D267D06A7CB20401758CED6A3A202FA236A0F7C1D70845F077F4AA0FA49780C12E067B543862E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...39762b0e_130e_47b5_8e5c_eae559ad8b4d.....d..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....https://fdcsa.cloud/....t...p.....h.....h.....`..... .....-"......-".....0.....h.t.t.p.s.:././.f.d.c.s.a...c.l.o.u.d./.....8.....0.....8..... ....https://fdcsa.cloud/....{..jM'/.....

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.245563238743274
Encrypted:	false
SSDEEP:	6:mI1Vq2PWXp+N23iKKdK8aPrqIFUtp3yMgZmwP3g0IkwOWXp+N23iKKdK8amLJ:H1Vva5KkL3FUtp3yMg/P3g0I5f5KkQJ
MD5:	5DE203D28A417D6D249D63360F20BD9C
SHA1:	09BDCE1C27E8371E9415FE9DD49CBB083F419E76
SHA-256:	9AAAF4E4CB4B956C693F5E7CBF7BA53880C793862476FCED010D01D54D456A8E
SHA-512:	0BA2A9E7D382DD7491424E584C614EE4AFCC4B61301BAE7D7298BC6D98C47BED5181E7B2DD056D450530E89A1063AAA02E1685B771D4C990319AFE8F7DE93C8
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.265 1664 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-00:55:58.269 1664 Recovering log #3.2021/08/04-00:55:58.270 1664 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 Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)

Entropy (8bit):	5.245563238743274
Encrypted:	false
SSDEEP:	6:mI1Vq2PWXp+N23iKKdK8aPrqIFUtp3yMgZmwP3g0IkwOWXp+N23iKKdK8amLJ:H1Vva5KkL3FUtp3yMg/P3g0I5f5KkQJ
MD5:	5DE203D28A417D6D249D63360F20BD9C
SHA1:	09BDCE1C27E8371E9415FE9DD49CBB083F419E76
SHA-256:	9AAAF4E4CB4B956C693F5E7CBF7BA53880C793862476FCED010D01D54D456A8E
SHA-512:	0BA2A9E7D382DD7491424E584C614EE4AFCC4B61301BAE7D7298BC6D98C47BED5181E7B2DD056D450530E89A1063AAA02E1685B771D4C990319AFE8F7DE93C 8
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.265 1664 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-00:55:58.269 1664 Recovering log #3.2021/08/04-00:55:58.270 1664 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.202385007599425
Encrypted:	false
SSDEEP:	6:m5aXq2PWXp+N23iKKdK8NIFUtpU+XZmwPU4FkwOWXp+N23iKKdK8+eLJ:EaXva5KkpFUtpU+X/PU05f5KkqJ
MD5:	A3A653235C0956E2AC573BACBF8D07BF
SHA1:	8312D10E14DA82E08EEF10A6C7F6B41F2AF9050A
SHA-256:	49363BB079D83FBE6C118011CDD1D5D4FE30311B4245015AF22DE377B533E3A1
SHA-512:	645A1C1097BD00075B0D84E90076706481EBE407D19FF6D6FD04B96CD375F732F663F28B428861B193D158969AC661291D46061C313AD59189B6C0F1122D5F37
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:00.482 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-00:56:00.483 16c4 Recovering log #3.2021/08/04-00:56:00.489 16c4 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\Extension State\LOG.old. (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.202385007599425
Encrypted:	false
SSDEEP:	6:m5aXq2PWXp+N23iKKdK8NIFUtpU+XZmwPU4FkwOWXp+N23iKKdK8+eLJ:EaXva5KkpFUtpU+X/PU05f5KkqJ
MD5:	A3A653235C0956E2AC573BACBF8D07BF
SHA1:	8312D10E14DA82E08EEF10A6C7F6B41F2AF9050A
SHA-256:	49363BB079D83FBE6C118011CDD1D5D4FE30311B4245015AF22DE377B533E3A1
SHA-512:	645A1C1097BD00075B0D84E90076706481EBE407D19FF6D6FD04B96CD375F732F663F28B428861B193D158969AC661291D46061C313AD59189B6C0F1122D5F37
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old. (copy)	
Reputation:	low
Preview:	2021/08/04-00:56:00.482 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-00:56:00.483 16c4 Recovering log #3.2021/08/04-00:56:00.489 16c4 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+e5QxYbUsclJ5n0ITpw5JBHV1Kph3/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:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.235532058624781
Encrypted:	false
SSDEEP:	6:moE+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpbkZmwPbFRVkwOWXp+N23iKKdK25+M:dva5KkTXfchI3FUtpY/PZ/5f5KkTXfcF
MD5:	CA4A066E0C814C94190D75121C75655E
SHA1:	F0E42C52FA91088B9D6B66D864D0B756FD63DC06
SHA-256:	049E5C448D997101A7E981474EB3FA4F822EC9F40B073686002060FC9EE3D502
SHA-512:	CC253DAEDD7961B276FB4464FBBFBCBCD9C2CDB2489E2775D8781ED6751835B387251F52CFFC8B1EB2E5771076491D58F9742465D7F035D20E6BF61519D4745
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.035 1538 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-00:56:05.040 1538 Recovering log #3.2021/08/04-00:56:05.041 1538 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.235532058624781
Encrypted:	false
SSDEEP:	6:moE+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpbkZmwPbFRVkwOWXp+N23iKKdK25+M:dva5KkTXfchI3FUtpY/PZ/5f5KkTXfcF
MD5:	CA4A066E0C814C94190D75121C75655E
SHA1:	F0E42C52FA91088B9D6B66D864D0B756FD63DC06
SHA-256:	049E5C448D997101A7E981474EB3FA4F822EC9F40B073686002060FC9EE3D502
SHA-512:	CC253DAEDD7961B276FB4464FBBFBCBCD9C2CDB2489E2775D8781ED6751835B387251F52CFFC8B1EB2E5771076491D58F9742465D7F035D20E6BF61519D4745
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.035 1538 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-00:56:05.040 1538 Recovering log #3.2021/08/04-00:56:05.041 1538 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.2155562964561994
Encrypted:	false
SSDEEP:	6:moNa3+q2PWXp+N23iKKdK25+XuoIFUtpbb5ZmwPbWHNVkwOWXp+N23iKKdK25+Xp:xaOva5KkTXYFUtpf5/PqT5f5KkTXHJ
MD5:	6AF88A97588BAAF4CC4C82C00F797589
SHA1:	8206811A6743D266E21E4856C86EACDE37A9AF85
SHA-256:	A98BD1D7898400085C3EB381137088FB58E31F6FE825C7AD848BF7C9AEC38774
SHA-512:	225A5BF8CBEAC182B3E00E2C6B2D21D965E62E88E10EA4B4167A2DAF1BD517216A0529A1F973E53443086FDFA3F71A7EDECF120F07D49448C6F18B925F89259
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.017 1538 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-00:56:05.018 1538 Recovering log #3.2021/08/04-00:56:05.019 1538 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\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.2155562964561994
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
SSDEEP:	6:moNa3+q2PWXp+N23iKKdK25+XuoIFUtpbb5ZmwPbWHNVkwOWXp+N23iKKdK25+Xp:xaOva5KkTXYFUtpf5/PqT5f5KkTXHJ
MD5:	6AF88A97588BAAF4CC4C82C00F797589
SHA1:	8206811A6743D266E21E4856C86EACDE37A9AF85
SHA-256:	A98BD1D7898400085C3EB381137088FB58E31F6FE825C7AD848BF7C9AEC38774
SHA-512:	225A5BF8CBEAC182B3E00E2C6B2D21D965E62E88E10EA4B4167A2DAF1BD517216A0529A1F973E53443086FDFA3F71A7EDECF120F07D49448C6F18B925F89259
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.017 1538 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-00:56:05.018 1538 Recovering log #3.2021/08/04-00:56:05.019 1538 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.223792807138997
Encrypted:	false
SSDEEP:	6:mo9UzN+q2PWXp+N23iKKdKWT5g1IdqIFUtpbIqZmwPbbFNVkwOWXp+N23iKKdKW4:6Iva5Kkg5gSRFUtpcq/P3F5f5Kkg5gSu
MD5:	E1CC33B24AC999B74307B1C75D274820
SHA1:	4723CEF946010754BDDB32B7FE097D2F06A7A6AE
SHA-256:	25DCC39F260F23F71D90F7DF44C49CA092AE0F5F081A2F2D500C8F6163AD3482
SHA-512:	16ED59B6991534C01DFAD0A631C8C37F9FB365FC0FB8A84CD0C75876E4B9D709FAA2761E3ED9829609B87A82B3EF67646E444D5FCB74B5B3856794113B0B757
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.006 1538 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-00:56:05.007 1538 Recovering log #3.2021/08/04-00:56:05.009 1538 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\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.223792807138997
Encrypted:	false
SSDEEP:	6:mo9UzN+q2PWXp+N23iKKdKWT5g1IdqIFUtpbIqZmwPbbFNVkwOWXp+N23iKKdKW4:6Iva5Kkg5gSRFUtpcq/P3F5f5Kkg5gSu
MD5:	E1CC33B24AC999B74307B1C75D274820
SHA1:	4723CEF946010754BDDB32B7FE097D2F06A7A6AE
SHA-256:	25DCC39F260F23F71D90F7DF44C49CA092AE0F5F081A2F2D500C8F6163AD3482
SHA-512:	16ED59B6991534C01DFAD0A631C8C37F9FB365FC0FB8A84CD0C75876E4B9D709FAA2761E3ED9829609B87A82B3EF67646E444D5FCB74B5B3856794113B0B757
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.006 1538 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-00:56:05.007 1538 Recovering log #3.2021/08/04-00:56:05.009 1538 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-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	0.3283577581710296
Encrypted:	false
SSDEEP:	6:L94/fMt76Y4QZVRtRex99pG/QqR4EZY4QZv8fOm:L94nMWQA9LABQZ8fOm
MD5:	0F67CB05CE74357FBD1E0CE18B24407D
SHA1:	E9245CCA0F463700A672BC467EDF4228EC148FBE
SHA-256:	25AC3CD1784FC64D161BC3FA977BB3EE53EEDF29FED34E20EE6A42ACA24427BA
SHA-512:	20EBDCF498BE9CE79521F3653A1961DEF88269DA6E3D8ABFB002F313D1773F56E16A9FA1DD9E6FB29A674406C13ACF1C5E7A800B78460FEB1BFBEAB4FBF19864
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Preview:	.....E..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session.O (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	901
Entropy (8bit):	3.0672881592418917
Encrypted:	false
SSDEEP:	12:3olydJh0vnz/TPlpxlpN8kIyTd1oameOqXBlptlpl:34SuPLLlrlAa1/mxwlLlL
MD5:	237D08C4A728FCCD6557D523108C5E6D
SHA1:	424110A573A0CBA98DD4039705A88D136BAD2411
SHA-256:	BC151C008245F6D5200F6DA93A2C759AC6671D3F5D40F6DD5015D195F3342968
SHA-512:	75B4EBB9CD936F794FFB88992F8547F9542525D19FF39987ED7D267D06A7CB20401758CED6A3A202FA236A0F7C1D70845F077F4AA0FA49780C12E067B543862E
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...39762b0e_130e_47b5_8e5c_eae559ad8b4d.....d..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....https://fdcsa.cloud/....t...p.....h.....h.....`..... .....-".....-".....0.....h.t.t.p.s.:././.f.d.c.s.a...c.l.o.u.d./.....8.....0.....8..... ....https://fdcsa.cloud/....{..jM'/.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.459689625889554
Encrypted:	false
SSDEEP:	48:auT6xGZknNJKLa7pMM8dbTEUsbQSefgGLNrS0U9RdiN9xAkV:a8Za7pMfdbTEUsbQ5fgG5rS08c
MD5:	0988EE516B821A30C8378EDC42B2D21C
SHA1:	48079DAFAF70566D2A8D44901E64C6263316A6E7
SHA-256:	75E012ED24C0D4CF3BCFB135B683B6E683EE486616B16D0478A7FD67F101437F
SHA-512:	4D1FDBFC14FD843FD45FA6EE172578C05B8E112469AEA537887AB3B1D23EDF2E862B582690C3CF4620641EB1F7714E72499FEFE161F8ACB037F9E234663B9D1
Malicious:	false
Reputation:	low
Preview:	qu.....*.....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..640405000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-04 00:56:06.83][INFO][mr.Init] MR instance ID: 255e6b7f-1dba-4433-a1e0-fa8ce7d6ba70\n","[2021-08-04 00:56:06.83][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-04 00:56:06.83][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-04 00:56:06.84][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-04 00:56:06.84][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-04 00:56:06.84][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-04 00:56:06.84][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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.208453647625829
Encrypted:	false
SSDEEP:	6:mIs4AQ+q2PWXp+N23iKKdK8a2jMGIFUtp3u2XAgZmwP3qAQVkwOWXp+N23iKKdKw:HxAVva5Kk8EFUtp3u4Ag/P3qAI5f5Kkw
MD5:	2AB567B3BDE93FC17A040B2A7C676F8B
SHA1:	3D765AE72A9FFA8BBB2D920D36AAE47E133B1A9D
SHA-256:	D753767A9032D0319E22C78452049C0FCEDEC6BA6991BD7871A51F0B70E59846
SHA-512:	255B4BAC00407C45BA3A91F88C322D8F8171CDB3E545C0DB187FD5EDAE00A744699B2B099D7EA1CF77FE04564D8B0A84AB3B4F2E9415EC3838F8D46A0A29BA39
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.091 16b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:55:58.093 16b8 Recovering log #3.2021/08/04-00:55:58.094 16b8 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\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.208453647625829
Encrypted:	false
SSDEEP:	6:mIs4AQ+q2PWXp+N23iKKdK8a2jMGIFUtp3u2XAgZmwP3qAQVkwOWXp+N23iKKdKw:HxAVva5Kk8EFUtp3u4Ag/P3qAI5f5Kkw
MD5:	2AB567B3BDE93FC17A040B2A7C676F8B
SHA1:	3D765AE72A9FFA8BBB2D920D36AAE47E133B1A9D
SHA-256:	D753767A9032D0319E22C78452049C0FCEDEC6BA6991BD7871A51F0B70E59846
SHA-512:	255B4BAC00407C45BA3A91F88C322D8F8171CDB3E545C0DB187FD5EDAE00A744699B2B099D7EA1CF77FE04564D8B0A84AB3B4F2E9415EC3838F8D46A0A29BA39
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.091 16b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:55:58.093 16b8 Recovering log #3.2021/08/04-00:55:58.094 16b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2042
Entropy (8bit):	4.901059181904288
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5s8JRLs4Tsb5SR3sSZDshyKs13gYhbD:JTnOCXGDHz97O2gExhH
MD5:	7D08300C1EDD154BD7E90320714FADC3
SHA1:	11E02C453C1A23B3814E2242DD2E134F1F6E0D99
SHA-256:	65757AE9BABF4EDEB1E7CE29C86903B2C94A2B688B28EE9F2877A8B70B08A015
SHA-512:	167A22B5A50B070A37AD4C6097CF7CE0FFEE91C59192BE1B1E1FFBDE0F5E27688B9FC9CC072CF51DAD4A611134ECCF16B28C18F6E7F33F7719DCFD7925D6FCA9
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275129361049282","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275129361136326","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateTM (copy)	
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.230674567479412
Encrypted:	false
SSDEEP:	6:mINOq2PWXp+N23iKKdKgXz4rRIFUtp3McG9ZmwP3tPkwOWXp+N23iKKdKgXz4q8d:HNOva5KkgXiuFUtp3xG9/P3tP5f5Kkgi
MD5:	9CE158006DD746E2414DEAE3A358AEE3
SHA1:	F9492362EBEC1167B393F522955C6A087E41B0C4
SHA-256:	A62097C1F872CC0EF80C673840F48AE78377D727B68181DC9E44A75552E50F0E
SHA-512:	A03CF7DE9950114C0A66BAA99DC604BCB1A190012713E040AB1A0418940C6447F9A771563DFBF6954B5D42AA1D8D742711C883535C74F16A6D4C04A8335F95F9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.283 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-00:55:58.284 16c4 Recovering log #3.2021/08/04-00:55:58.285 16c4 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.230674567479412
Encrypted:	false
SSDEEP:	6:mINOq2PWXp+N23iKKdKgXz4rRIFUtp3McG9ZmwP3tPkwOWXp+N23iKKdKgXz4q8d:HNOva5KkgXiuFUtp3xG9/P3tP5f5Kkgi
MD5:	9CE158006DD746E2414DEAE3A358AEE3
SHA1:	F9492362EBEC1167B393F522955C6A087E41B0C4
SHA-256:	A62097C1F872CC0EF80C673840F48AE78377D727B68181DC9E44A75552E50F0E
SHA-512:	A03CF7DE9950114C0A66BAA99DC604BCB1A190012713E040AB1A0418940C6447F9A771563DFBF6954B5D42AA1D8D742711C883535C74F16A6D4C04A8335F95F9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.283 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-00:55:58.284 16c4 Recovering log #3.2021/08/04-00:55:58.285 16c4 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\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5487
Entropy (8bit):	5.183522843010179
Encrypted:	false
SSDEEP:	48:Yc+UklSLklwHjvc2M+qApLqqjoL8S+/Rp4lYqlQKHoTw0iOH3CH3G/s8C1Nfct/N:nQCmTqL9xGcKIfok0JCKL8pbOTQVuwn
MD5:	616DD5E539B98613C1A25653B8E571DE
SHA1:	81B6AC72D897793E5CFCA9193012BD7952838205
SHA-256:	D31EAFBE8ECB5AFC29E6CEF842F8E80664A55E02F5E53D16496DBCA1DB1CAA1E
SHA-512:	65E013546A4A533EF7B2587C93626B7DE386F147B807420036EC31514470E60B852B72C5595833C28D26742FABEC5303CEF79939145C1F73EF11D7FD141FD326
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272537358253419","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"co untryid_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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8263347560211738
Encrypted:	false
SSDEEP:	48:SAqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU86:SAhIElwQF8mpcSN
MD5:	17A688B3753889E6106B9B56B6366A01
SHA1:	2EE0C56EFFF51C81694C1574B753C6A2D4223890
SHA-256:	7AC5768CE0DA4285F68DC3E2C34B4AAE502A5BE05A6ADFFF46056CFFF857FEB5
SHA-512:	DD63C9562B646896B47C10A5F9E89C6D2FC1E173F900AE4BE50FE302684FB68F42DF9CBC549E3BCDEF223ECCDBCFB8F96C37684502FD6A29B6F03C959A2AB 17
Malicious:	false
Reputation:	low
Preview:	............y.P... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.5357703748603635
Encrypted:	false
SSDEEP:	384:aj0tBLlYEX61kXqKf/pUZNCgVLH2HfD4rUnHGrnTfle4g:fLlX61kXqKf/pUZNCgVLH2HfMrUHGrng
MD5:	72567466DCF717277C0408E914B2D1C9
SHA1:	26C4CE292C1CC86EC870F81122847BA763328220
SHA-256:	B16FD0008898C69DCD63DF4EF136DE6BE60BDF7526E48A034A18647877F0C5ED
SHA-512:	6F23B298CBAA72501F5107D12B9CEAAA554C9C91B425D4E887DE5C16A6BFDA0840761CF07A6F29CD050948BE67EF3989A5A516FF8C6BE67E8A2C59760A5BB4 9
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13272537357950859","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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:5ljljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946 B
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):	320
Entropy (8bit):	5.196078756691591
Encrypted:	false
SSDEEP:	6:mIzRFUXq2PWXp+N23iKKdKrQMxIFUtp3zsZmwP3zfFdPkwOWXp+N23iKKdKrQMFd:HMXva5KkCFUtp34/P3bFJ5f5KktJ
MD5:	909F2B6B99B6DCE2554177046541F266
SHA1:	F93E7B5B19589E3229688639A13ED4C923EBAB53
SHA-256:	5949B092E50419B1B02544EDFDFC88A94BE0250B5F337D0B5B0122E2B9F15361
SHA-512:	4A98410B9B1BA8A50826121696CD802360579F22FD88DE2DE7B8D488FB97255184CCF430E42905045D12E479BF1228573E1577445CE7C80C33D830AE67BFDB63
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.186 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-00:55:58.187 16c4 Recovering log #3.2021/08/04-00:55:58.188 16c4 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\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.196078756691591
Encrypted:	false
SSDEEP:	6:mIzRFUXq2PWXp+N23iKKdKrQMxIFUtp3zsZmwP3zfFdPkwOWXp+N23iKKdKrQMFd:HMXva5KkCFUtp34/P3bFJ5f5KktJ
MD5:	909F2B6B99B6DCE2554177046541F266
SHA1:	F93E7B5B19589E3229688639A13ED4C923EBAB53
SHA-256:	5949B092E50419B1B02544EDFDFC88A94BE0250B5F337D0B5B0122E2B9F15361
SHA-512:	4A98410B9B1BA8A50826121696CD802360579F22FD88DE2DE7B8D488FB97255184CCF430E42905045D12E479BF1228573E1577445CE7C80C33D830AE67BFDB63
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.186 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-00:55:58.187 16c4 Recovering log #3.2021/08/04-00:55:58.188 16c4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.224240994900913
Encrypted:	false
SSDEEP:	6:mIHohfMM+q2PWXp+N23iKKdK7Uh2ghZIFUtp3HoZZZmwP3HooBMVkwOWXp+N23in:HIhEM+va5KklhHh2FUtp3IZZ/P3IaMVK
MD5:	DC9F34C0CCA16C171B467216D1AF8815
SHA1:	E9B28E767337E5233744E95972F1B4802DD7CF69
SHA-256:	7E62ABEC421B35C4B259DB64F9910D7C429AB3579E94B9653E6802FBAD4965D8
SHA-512:	AAEAFB68642BFA540ADF8D3D59FB389F6BA4B5D910116A07D13AC40501BEBF14B7A2FE49AC365B8096C322B6B50CF661005891E6869DDB3892F487A44615909
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:57.977 166c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/04-00:55:57.982 166c Recovering log #3.2021/08/04-00:55:57.986 166c 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\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.224240994900913
Encrypted:	false
SSDEEP:	6:mIHohfMM+q2PWXp+N23iKKdK7Uh2ghZIFUtp3HoZZZmwP3HooBMVkwOWXp+N23in:HIhEM+va5KklhHh2FUtp3IZZ/P3IaMVK
MD5:	DC9F34C0CCA16C171B467216D1AF8815
SHA1:	E9B28E767337E5233744E95972F1B4802DD7CF69
SHA-256:	7E62ABEC421B35C4B259DB64F9910D7C429AB3579E94B9653E6802FBAD4965D8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
SHA-512:	AAEAFB68642BFA540ADF8D3D59FB389F6BA4B5D910116A07D13AC40501BEBF14B7A2FE49AC365B8096C322B6B50CF661005891E6869DDB3892F487A44615909
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:57.977 166c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/04-00:55:57.982 166c Recovering log #3.2021/08/04-00:55:57.986 166c 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\4a7997b7-7e70-40f7-aa2b-246642427a01.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.284098625805302
Encrypted:	false
SSDEEP:	6:mI+u5SVq2PWXp+N23iKKdKusNpV/2jMGIFUtp3NgZmwP3NIkwOWXp+N23iKKdKux:H+ySVva5KkFFUtp3Ng/P3NI5f5KkOJ
MD5:	5D20B34C356AC9996E4589CA04DA987A
SHA1:	70E9A5CACB05FE5BD2A3253F243370CCDDD9A277
SHA-256:	E296FED110AFFF89BA2E7357F8F0850AB65B238ACA16D8FBB66CE905AF7CBF0C
SHA-512:	0D1266045003FEDAAE885642CE63C13CA934941FEB437769B841D127F18276E898748102577A4268559DC86E14AE4705887FD1E91517DF85DBB17CDD244AF966
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.228 1664 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:55:58.229 1664 Recovering log #3.2021/08/04-00:55:58.229 1664 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\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.284098625805302
Encrypted:	false
SSDEEP:	6:mI+u5SVq2PWXp+N23iKKdKusNpV/2jMGIFUtp3NgZmwP3NIkwOWXp+N23iKKdKux:H+ySVva5KkFFUtp3Ng/P3NI5f5KkOJ
MD5:	5D20B34C356AC9996E4589CA04DA987A
SHA1:	70E9A5CACB05FE5BD2A3253F243370CCDDD9A277
SHA-256:	E296FED110AFFF89BA2E7357F8F0850AB65B238ACA16D8FBB66CE905AF7CBF0C
SHA-512:	0D1266045003FEDAAE885642CE63C13CA934941FEB437769B841D127F18276E898748102577A4268559DC86E14AE4705887FD1E91517DF85DBB17CDD244AF966
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.228 1664 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:55:58.229 1664 Recovering log #3.2021/08/04-00:55:58.229 1664 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.280365093093198
Encrypted:	false
SSDEEP:	6:mIXM+q2PWXp+N23iKKdKusNpqz4rRIFUtp3OEZZmwP3OEMMVkwOWXp+N23iKKdKr:Hc+va5KkmiuFUtp3OY/P3OoV5f5Kkm2J
MD5:	570ECE702BD02F27AD5DE911C56CF44C
SHA1:	716E753A0678A455DB67C74DE117A47AA5994D8B
SHA-256:	0FBA0F89770E6F2C2B54B4C603222BCDA57B14780795D1699CC3E5D41092223A
SHA-512:	B0E9A31B05A5FB51E2207D766FAF2DFDC61046BFCDC0D45D34CB9A9C21FC0FDA2946DD117144538A19852BF133B25AE791DB764C48A71F9CF4834A1B0073CF 6
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.283 16ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/04-00:55:58.286 16ac Recovering log #3.2021/08/04-00:55:58.286 16ac 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.280365093093198
Encrypted:	false
SSDEEP:	6:mIXM+q2PWXp+N23iKKdKusNpqz4rRIFUtp3OEZZmwP3OEMMVkwOWXp+N23iKKdKr:Hc+va5KkmiuFUtp3OY/P3OoV5f5Kkm2J
MD5:	570ECE702BD02F27AD5DE911C56CF44C
SHA1:	716E753A0678A455DB67C74DE117A47AA5994D8B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
SHA-256:	0FBA0F89770E6F2C2B54B4C603222BCDA57B14780795D1699CC3E5D41092223A
SHA-512:	B0E9A31B05A5FB51E2207D766FAF2DFDC61046BFCDC0D45D34CB9A9C21FC0FDA2946DD117144538A19852BF133B25AE791DB764C48A71F9CF4834A1B0073CF6
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.283 16ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/04-00:55:58.286 16ac Recovering log #3.2021/08/04-00:55:58.286 16ac 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):	418
Entropy (8bit):	5.298231627778099
Encrypted:	false
SSDEEP:	6:mm8q2PWXp+N23iKKdKusNpZQMxIFUtpjhXZmwPjhFkwOWXp+N23iKKdKusNpZQMT:mva5KkMFUtpjt/Pjf5f5KkTJ
MD5:	557A6DCF88B3E07102BFAE39DEDE74F3
SHA1:	7E66A1E429CC243AFC6C49C97D0F7D2661C92CBB
SHA-256:	16FA862DDD11C573DB9B45454BB158672A875B14909A580243588FD9B85C2F8A
SHA-512:	0196CAA95D8C09C2ABD4294D4CB8F7A67136D97ED4C3094B30031AB05EBCF2C0EF5F96828169887B7D96A324E315FEC852C17786C661FBA19FE37CE3A3AFBBF
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:14.495 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/04-00:56:14.497 16c4 Recovering log #3.2021/08/04-00:56:14.497 16c4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.298231627778099
Encrypted:	false
SSDEEP:	6:mm8q2PWXp+N23iKKdKusNpZQMxIFUtpjhXZmwPjhFkwOWXp+N23iKKdKusNpZQMT:mva5KkMFUtpjt/Pjf5f5KkTJ
MD5:	557A6DCF88B3E07102BFAE39DEDE74F3
SHA1:	7E66A1E429CC243AFC6C49C97D0F7D2661C92CBB
SHA-256:	16FA862DDD11C573DB9B45454BB158672A875B14909A580243588FD9B85C2F8A
SHA-512:	0196CAA95D8C09C2ABD4294D4CB8F7A67136D97ED4C3094B30031AB05EBCF2C0EF5F96828169887B7D96A324E315FEC852C17786C661FBA19FE37CE3A3AFBBF
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:14.495 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/04-00:56:14.497 16c4 Recovering log #3.2021/08/04-00:56:14.497 16c4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.164721748808713
Encrypted:	false
SSDEEP:	12:dy+va5KkkGHArBFUtptC+/PtZV5f5KkkGHAryJ:dDa5KkkGgPg7x5f5KkkGga
MD5:	34C9E8343F7F838A7703A302695E0A05
SHA1:	7AB84ECC0EC4BC290526C8DFDAAEE6126B3583D0
SHA-256:	5ABC5DE6305FDB85DE2C3A13852BAE0F2F0A596EAB7D284B89C71454DCECF6DE
SHA-512:	6A946CF85D1A296620E21060A14492FC44EEBA20A69D94328F8655036FBA7B7F6C9CA9876A66EA5AAA35928392D4FDC1F7691903FB3C17EF1131C9129B161EBF
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.550 16ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:56:05.553 16ac Recovering log #3.2021/08/04-00:56:05.555 16ac Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.164721748808713
Encrypted:	false
SSDEEP:	12:dy+va5KkkGHArBFUtptC+/PtZV5f5KkkGHAryJ:dDa5KkkGgPg7x5f5KkkGga
MD5:	34C9E8343F7F838A7703A302695E0A05
SHA1:	7AB84ECC0EC4BC290526C8DFDAAEE6126B3583D0
SHA-256:	5ABC5DE6305FDB85DE2C3A13852BAE0F2F0A596EAB7D284B89C71454DCECF6DE
SHA-512:	6A946CF85D1A296620E21060A14492FC44EEBA20A69D94328F8655036FBA7B7F6C9CA9876A66EA5AAA35928392D4FDC1F7691903FB3C17EF1131C9129B161EBF
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.550 16ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:56:05.553 16ac Recovering log #3.2021/08/04-00:56:05.555 16ac Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy)	
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.202318555014653
Encrypted:	false
SSDEEP:	12:dY+va5KkkGHArqiuFUtptCNW/PtXV5f5KkkGHArq2J:dxa5KkkGgCg7v3f5KkkGg7
MD5:	86790C1825375C9A2F46AA55B9719585
SHA1:	F0909321599D9C5102CF98E5D4639BDECECF6AC9
SHA-256:	E4E73625C0A946AFEED0175D48F8D20AF7F39A437AEFB7046853B00CBCD8E2D2
SHA-512:	30C0FDD541E37209D90AB49ACF8095FF24204EADC7625D382614460F6707BEDC3A0A5FB9CF1B8A9169E2105201C050487926E7298C17E28FF6117B5E56404848
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.550 163c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/04-00:56:05.553 163c Recovering log #3.2021/08/04-00:56:05.555 163c 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.202318555014653
Encrypted:	false
SSDEEP:	12:dY+va5KkkGHArqiuFUtptCNW/PtXV5f5KkkGHArq2J:dxa5KkkGgCg7v3f5KkkGg7
MD5:	86790C1825375C9A2F46AA55B9719585
SHA1:	F0909321599D9C5102CF98E5D4639BDECECF6AC9
SHA-256:	E4E73625C0A946AFEED0175D48F8D20AF7F39A437AEFB7046853B00CBCD8E2D2
SHA-512:	30C0FDD541E37209D90AB49ACF8095FF24204EADC7625D382614460F6707BEDC3A0A5FB9CF1B8A9169E2105201C050487926E7298C17E28FF6117B5E56404848
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.550 163c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/04-00:56:05.553 163c Recovering log #3.2021/08/04-00:56:05.555 163c 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
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

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

Size (bytes):	418
Entropy (8bit):	5.216126949061899
Encrypted:	false
SSDEEP:	12:kva5KkkGHArAFUtp8/Pea5f5KkkGHArfJ:Oa5KkkGgkgNEf5KkkGgV
MD5:	2BB4DA9C41E4B338CC7045ADF422D4FC
SHA1:	0A67D42307E5D8750F7A0CB75AD7D97ACFC6E93B
SHA-256:	19B44684607DBB9636E9F96CFDF70F8C6614463AC8CF5D3FBA3BE3AE312507F1
SHA-512:	407826732FC95FFE55BCD39F19AEF81335B6048EA06A215D9AD51D1142F9E41A78900437BB7EC001A2B3E019A0D3D287E74BEB253F608906DC87734A801B8329
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:20.777 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/04-00:56:20.778 16c4 Recovering log #3.2021/08/04-00:56:20.779 16c4 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old41 (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.216126949061899
Encrypted:	false
SSDEEP:	12:kva5KkkGHArAFUtp8/Pea5f5KkkGHArfJ:Oa5KkkGgkgNEf5KkkGgV
MD5:	2BB4DA9C41E4B338CC7045ADF422D4FC
SHA1:	0A67D42307E5D8750F7A0CB75AD7D97ACFC6E93B
SHA-256:	19B44684607DBB9636E9F96CFDF70F8C6614463AC8CF5D3FBA3BE3AE312507F1
SHA-512:	407826732FC95FFE55BCD39F19AEF81335B6048EA06A215D9AD51D1142F9E41A78900437BB7EC001A2B3E019A0D3D287E74BEB253F608906DC87734A801B8329
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:20.777 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/04-00:56:20.778 16c4 Recovering log #3.2021/08/04-00:56:20.779 16c4 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\df8f9987-f205-4930-a922-5b9d25948763.tmp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.222035852500476
Encrypted:	false
SSDEEP:	6:mIGXq2PWXp+N23iKKdKpIFUtp3JVXZmwP3f6kwOWXp+N23iKKdKa/WLJ:HMva5KkmFUtp3JVX/P3C5f5KkaUJ
MD5:	69233355CA38E9ACA58929DACE478F14
SHA1:	D306587D35DFC65C4084EBEEC3C1A0DD688224A6
SHA-256:	3228FFBA55ED72AC9571182DCAA5B461A866386F9D4C50DD7787963F4F3DC3DE
SHA-512:	AD61078ACA7A301F0308DCB88493E986DD9F4C0D9886FDB730263610A69142A647224A40621F668A14F174A6A3C17C03DAA1BEB1B966E2CBE9D53788A0769EE
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.085 1670 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-00:55:58.087 1670 Recovering log #3.2021/08/04-00:55:58.088 1670 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 Data\LevelDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.222035852500476
Encrypted:	false
SSDEEP:	6:mIGXq2PWXp+N23iKKdKpIFUtp3JVXZmwP3f6kwOWXp+N23iKKdKa/WLJ:HMva5KkmFUtp3JVX/P3C5f5KkaUJ
MD5:	69233355CA38E9ACA58929DACE478F14
SHA1:	D306587D35DFC65C4084EBEEC3C1A0DD688224A6
SHA-256:	3228FFBA55ED72AC9571182DCAA5B461A866386F9D4C50DD7787963F4F3DC3DE
SHA-512:	AD61078ACA7A301F0308DCB88493E986DD9F4C0D9886FDB730263610A69142A647224A40621F668A14F174A6A3C17C03DAA1BEB1B966E2CBE9D53788A0769EE
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:55:58.085 1670 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-00:55:58.087 1670 Recovering log #3.2021/08/04-00:55:58.088 1670 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.325486029781136
Encrypted:	false
SSDEEP:	6:mfUdq2PWXp+N23iKKdKks8Y5JKKhdIFUtpmUaXZmwPmUaFkwOWXp+N23iKKdKksp:ddva5KkkOrsFUtptq/PtW5f5KkkOrzJ
MD5:	5CA0B12F560DB11EA79DB45E41C85BDA
SHA1:	39CCE13AE034D2AC8D70E24FB79BD348815C6EF9
SHA-256:	A961807639AB43C4DC427C4B76F866492F8BCF2CF286CACA7FC8D2158DC702B2
SHA-512:	BAB94ECAC6D153D072998E31672CD2C072DECA17916C34202F6D21EB11BCB680BAA6BDBF5521642640FE1FADE6AFFA4CF06F570F4707428E8410945C57C53A 7
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:06.831 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/04-00:56:06.833 16c4 Recovering log #3.2021/08/04-00:56:06.833 16c4 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\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.olds (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.olds (copy)	
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.325486029781136
Encrypted:	false
SSDEEP:	6:mfUdq2PWXp+N23iKKdKks8Y5JKKhdIFUtpmUaXZmwPmUaFkwOWXp+N23iKKdKksp:ddva5KkkOrsFUtptq/PtW5f5KkkOrzJ
MD5:	5CA0B12F560DB11EA79DB45E41C85BDA
SHA1:	39CCE13AE034D2AC8D70E24FB79BD348815C6EF9
SHA-256:	A961807639AB43C4DC427C4B76F866492F8BCF2CF286CACA7FC8D2158DC702B2
SHA-512:	BAB94ECAC6D153D072998E31672CD2C072DECA17916C34202F6D21EB11BCB680BAA6BDBF5521642640FE1FADE6AFFA4CF06F570F4707428E8410945C57C53A7
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:06.831 16c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/04-00:56:06.833 16c4 Recovering log #3.2021/08/04-00:56:06.833 16c4 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\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.566331189215954
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXv7b7wU+RUenHQ:YI6UUhVseKUewqPeUer2UefjwU+Uenw
MD5:	BAECECB9AD69F715CA291F8B632243E9
SHA1:	C1F2FEE0C8D802D0C90BEBA3B439A8211E34C79D
SHA-256:	D89ADF6D8C96FA62277C67EA5EBC4A34A7AA0A1D673F6ECB06EE6168F1EF1218
SHA-512:	86C46C4A5F21B2BC330292DED3B1CDE9BD1B22E2618BBA1E43980717EB19C38FC0A1FF17DA7AAF575D6A96667E57388CB65B905C1AD2379D91590E3318BFB4B
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659599761.049338,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628063761.049343},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b76ab89e-32ff-4ad5-b7d9-0b6e8af308fc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.5357703748603635
Encrypted:	false
SSDEEP:	384:aj0tBLlYEX61kXqKf/pUZNCgVLH2HfD4rUnHGrnTfle4g:fLlX61kXqKf/pUZNCgVLH2HfMrUHGrng
MD5:	72567466DCF717277C0408E914B2D1C9
SHA1:	26C4CE292C1CC86EC870F81122847BA763328220
SHA-256:	B16FD0008898C69DCD63DF4EF136DE6BE60BDF7526E48A034A18647877F0C5ED
SHA-512:	6F23B298CBAA72501F5107D12B9CEAAA554C9C91B425D4E887DE5C16A6BFDA0840761CF07A6F29CD050948BE67EF3989A5A516FF8C6BE67E8A2C59760A5BB49
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":"13272537357950859","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\d92bd89c-cf01-4f97-af30-abb6481dfe4f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d92bd89c-cf01-4f97-af30-abb6481dfe4f.tmp	
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\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.468949052759649
Encrypted:	false
SSDEEP:	3:tUK6HLWFw32WZmwv3IHLkUFYBh7V8sIHLkXWh7WGv:mlWmZZmwPAkUu7VvAke7tv
MD5:	F6069D66662FEB667A54A7A0A8BEAB2C
SHA1:	B8F3A56ADA381CD035B09597344F4082A2CC02E9
SHA-256:	86DD645FE3FD81C89811C16ABE2575F6C1A5696044A2428C125C2263262BD0FF
SHA-512:	FB225EA44845523516C1E645F6BE12ADA1E4DB6A289EA74B10F6C1DB735CDF2532A08EC0CA57C401835D20A7470F3733C41F98622B4C82A5207C37F3D7C2679
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:04.814 1538 Recovering log #3.2021/08/04-00:56:04.901 1538 Delete type=0 #3.2021/08/04-00:56:04.902 1538 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.468949052759649
Encrypted:	false
SSDEEP:	3:tUK6HLWFw32WZmwv3IHLkUFYBh7V8sIHLkXWh7WGv:mlWmZZmwPAkUu7VvAke7tv
MD5:	F6069D66662FEB667A54A7A0A8BEAB2C
SHA1:	B8F3A56ADA381CD035B09597344F4082A2CC02E9
SHA-256:	86DD645FE3FD81C89811C16ABE2575F6C1A5696044A2428C125C2263262BD0FF
SHA-512:	FB225EA44845523516C1E645F6BE12ADA1E4DB6A289EA74B10F6C1DB735CDF2532A08EC0CA57C401835D20A7470F3733C41F98622B4C82A5207C37F3D7C2679
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:04.814 1538 Recovering log #3.2021/08/04-00:56:04.901 1538 Delete type=0 #3.2021/08/04-00:56:04.902 1538 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ef73dd49-96b2-447d-a078-d28d880cf8f8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.566331189215954
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXv7b7wU+RUenHQ:YI6UUhVseKUewqPeUer2UefjwU+Uenw
MD5:	BAECECB9AD69F715CA291F8B632243E9
SHA1:	C1F2FEE0C8D802D0C90BEBA3B439A8211E34C79D
SHA-256:	D89ADF6D8C96FA62277C67EA5EBC4A34A7AA0A1D673F6ECB06EE6168F1EF1218
SHA-512:	86C46C4A5F21B2BC330292DED3B1CDE9BD1B22E2618BBA1E43980717EB19C38FC0A1FF17DA7AAF575D6A96667E57388CB65B905C1AD2379D91590E3318BFB4B
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659599761.049338,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628063761.049343},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fe9de5a1-5d56-4c87-9da4-eb089892d156.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):	5487
Entropy (8bit):	5.183522843010179
Encrypted:	false
SSDEEP:	48:Yc+UklSLklwHjvc2M+qApLqqjoL8S+/Rp4lYqlQKHoTw0iOH3CH3G/s8C1Nfct/N:nQCmTqL9xGcKIfok0JCKL8pbOTQVuwn
MD5:	616DD5E539B98613C1A25653B8E571DE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fe9de5a1-5d56-4c87-9da4-eb089892d156.tmp	
SHA1:	81B6AC72D897793E5CFCA9193012BD7952838205
SHA-256:	D31EAFBE8ECB5AFC29E6CEF842F8E80664A55E02F5E53D16496DBCA1DB1CAA1E
SHA-512:	65E013546A4A533EF7B2587C93626B7DE386F147B807420036EC31514470E60B852B72C5595833C28D26742FABEC5303CEF79939145C1F73EF11D7FD141FD326
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272537358253419","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.216914066476747
Encrypted:	false
SSDEEP:	6:moicWM+q2PWXp+N23iKKdKfrzAdIFUtpbic2ZZmwPbicQMVkwOWXp+N23iKKdKfa:+o+va5Kk9FUtpOF/PO+V5f5Kk2J
MD5:	A3F55EB007B47D5A006D20FF102279DE
SHA1:	C550061285DDC91C7010C3EE68DAAFD6979A6705
SHA-256:	8B37D07D6B224DD3462D9908CC798B7990DE54B5694502947749386975B76E49
SHA-512:	E6F37A3A5C2585B078BFFAD3AFCFD2EA8FB4A459AF3FDE4EB761100CCB40C32210D4B3E4C92D7AEF4568C43E542AB0B7B4FC74D36D839CEEBD99A5CFAC2DA5CF
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.393 16ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/04-00:56:05.394 16ac Recovering log #3.2021/08/04-00:56:05.395 16ac 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\Default\shared_proto_db\metadata\LOG.old8f (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.216914066476747
Encrypted:	false
SSDEEP:	6:moicWM+q2PWXp+N23iKKdKfrzAdIFUtpbic2ZZmwPbicQMVkwOWXp+N23iKKdKfa:+o+va5Kk9FUtpOF/PO+V5f5Kk2J
MD5:	A3F55EB007B47D5A006D20FF102279DE
SHA1:	C550061285DDC91C7010C3EE68DAAFD6979A6705
SHA-256:	8B37D07D6B224DD3462D9908CC798B7990DE54B5694502947749386975B76E49
SHA-512:	E6F37A3A5C2585B078BFFAD3AFCFD2EA8FB4A459AF3FDE4EB761100CCB40C32210D4B3E4C92D7AEF4568C43E542AB0B7B4FC74D36D839CEEBD99A5CFAC2DA5CF
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:56:05.393 16ac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/04-00:56:05.394 16ac Recovering log #3.2021/08/04-00:56:05.395 16ac Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	165869
Entropy (8bit):	6.0496007940510035
Encrypted:	false
SSDEEP:	3072:e9GaYTJQE+mugy9+QV1T7IRwdfLSNPtFcbXafIB0u1GOJmA3iuRd:e4xaV+QfT7GSmhraqfllUOoSiuRd
MD5:	DB15B838E46070DA40AADFF712AF7526
SHA1:	6E5E7E00A542FA520749D8EBBABB58C64DE00324
SHA-256:	F6D7B92C7B53D1D8C0A0131E0A5494E056A2AAFC8B833A52A17EAB5AE88FC10C
SHA-512:	70539B42BCEA0281B109A7BECEDA064FE84F3DBF45F0A0360CF44DDFC58BCBB0CB7DEDD337C08FE016740E3417F6D82871EA4A39FFCFB2804D9F090343BE4F4
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":1.628063760190436e+12,"network":1.628031361e+12,"ticks":5991353101.0,"uncertainty":2836332.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016956081"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174336
Entropy (8bit):	6.079379051247693
Encrypted:	false
SSDEEP:	3072:FXNGaYTJQE+mugy9+QV1T7IRwdfLSNPtFcbXafIB0u1GOJmA3iuRd:BoxaV+QfT7GSmhraqfllUOoSiuRd
MD5:	299FBAC1D852FC15D5CABDDA32718E1F
SHA1:	CD95ED6FDD85FA9A3D5981566C04DF214BE2F191
SHA-256:	EE562FC01275DEA203EE6DBC87921F9A516DB00F3848C9F6DBBEBBE415D6B9A2
SHA-512:	4F09D6853CC0552958E7075B846AB57CA0D6B4A05868D21B3470B75878B402A9B63A8371C0F8FF58E3E6B4A610F89E737AF163FDF8E57260FF1AA73F4CE296E6
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":1.628063760190436e+12,"network":1.628031361e+12,"ticks":5991353101.0,"uncertainty":2836332.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016956081"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7495579362895044
Encrypted:	false
SSDEEP:	384:Fr4XHdaEh+lZVmsb2Njrov/l3lXdkHtkGkTrOJT/x4p59YrSvmKtKVrbLUORZDNS:lG61VSBkUcer/RBw3/ONKPlL5yx
MD5:	45E2652BFC7C268E836EFFC7EE75F9F9
SHA1:	77BEFE8280316AB515171C06CC6CBE6F2E54D778
SHA-256:	68D0D9718AF82A72611F9DF55507A9BE5F3803F56BC77805FB391B158F452593
SHA-512:	2B8A96FF3AC604B55B1CE7C0977AD6BC30F375C2F14EC73C84FDDE4DDFFBDAC3696CF352EB592EE1CCB2D87400BA4DF1951EDC3934BBC19F7ED2C9C4B1EI 5D50
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.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\Module Info Cache9. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7497904135254227
Encrypted:	false
SSDEEP:	384:1r4XHdaEh+lZVmsb2Njrov/l3lXdkHtkGkTrOJT/x4p59YrSvmKOwKVrbLUORZDV:1G61VSB0Ucer/RBw3/ONKPlL5z
MD5:	6DD7E2AC9107BE1A5E4A795E0AAD4819
SHA1:	DA97316ACF0EDED171618BC570A93E6E1C3B4420
SHA-256:	C4CB00130A39326EB473BE503C17EE634392F0B8ADD0D07DEEB8435D27616739
SHA-512:	59C268D3DA996B54FF362ADFD1A887B1882E0D4DEA765D701519A6969E139472A94D63C1C940BFAFC61A753E35417A5EFA49E6D7911FBED43EEDCBF9B62CD6 A
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.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\bfe561cc-6a9f-4aa1-a343-40cf8d2d1545.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	95428
Entropy (8bit):	3.7497904135254227
Encrypted:	false
SSDEEP:	384:1r4XHdaEh+lZVmsb2Njrov/l3lXdkHtkGkTrOJT/x4p59YrSvmKOwKVrbLUORZDV:1G61VSB0Ucer/RBw3/ONKPlL5z
MD5:	6DD7E2AC9107BE1A5E4A795E0AAD4819
SHA1:	DA97316ACF0EDED171618BC570A93E6E1C3B4420
SHA-256:	C4CB00130A39326EB473BE503C17EE634392F0B8ADD0D07DEEB8435D27616739
SHA-512:	59C268D3DA996B54FF362ADFD1A887B1882E0D4DEA765D701519A6969E139472A94D63C1C940BFAFC61A753E35417A5EFA49E6D7911FBED43EEDCBF9B62CD6 A
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.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\c6e209dc-96a7-414f-8ab5-9ea627845bdc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\c6e209dc-96a7-414f-8ab5-9ea627845bdc.tmp	
Category:	dropped
Size (bytes):	174336
Entropy (8bit):	6.0793790995946
Encrypted:	false
SSDEEP:	3072:7XNGaYTJQE+mugy9+QV1T7IRwdfLSNPtFcbXafIB0u1GOJmA3iuRd:ToxaV+QfT7GSmhraqfIlUOoSiuRd
MD5:	3EEED448AE95273FF103C1D8B4C06646
SHA1:	EC4AE80153C126E50F33956A903659D56A30B2FA
SHA-256:	05D1907630B2064BE20CFA3024C0077ED6BF83C189DBCD9A79BBBE84F2CFE483
SHA-512:	E009DB3F05CBEA33EF0688D569E7564466B31FC84499E4CC9227039206A0ACA6C897454F925902F2C1C0D1A55D2FDF72C77BD86B57CA736734910237FEFA24F
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":1.628063760190436e+12,"network":1.628031361e+12,"ticks":5991353101.0,"uncertainty":2836332.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Temp\17f48631-6b45-4544-a260-e8f38e57c44d.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..

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 4, 2021 00:56:00.585769892 CEST	192.168.2.3	8.8.8.8	0x43ad	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 4, 2021 00:56:00.587254047 CEST	192.168.2.3	8.8.8.8	0x75b8	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:56:00.594811916 CEST	192.168.2.3	8.8.8.8	0x33f2	Standard query (0)	fdcsa.cloud	A (IP address)	IN (0x0001)
Aug 4, 2021 00:56:05.077116966 CEST	192.168.2.3	8.8.8.8	0x4c06	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
Aug 4, 2021 00:56:00.613651991 CEST	8.8.8.8	192.168.2.3	0x75b8	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 4, 2021 00:56:00.628690004 CEST	8.8.8.8	192.168.2.3	0x43ad	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:56:00.628690004 CEST	8.8.8.8	192.168.2.3	0x43ad	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:56:00.660914898 CEST	8.8.8.8	192.168.2.3	0x33f2	No error (0)	fdcsa.cloud		162.0.217.32	A (IP address)	IN (0x0001)
Aug 4, 2021 00:56:05.111053944 CEST	8.8.8.8	192.168.2.3	0x4c06	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:56:05.111053944 CEST	8.8.8.8	192.168.2.3	0x4c06	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- fdcsa.cloud

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49678	162.0.217.32	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 4, 2021 00:56:00.774316072 CEST	7	OUT	GET / HTTP/1.1 Host: fdcsa.cloud Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 4, 2021 00:56:00.809570074 CEST	8	IN	HTTP/1.1 301 Moved Permanently date: Tue, 03 Aug 2021 22:56:00 GMT server: Apache location: https://fdcsa.cloud/ content-length: 228 content-type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 64 63 73 61 2e 63 6c 6f 75 64 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	162.0.217.32	80	192.168.2.3	49681	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 4, 2021 00:56:01.678088903 CEST	916	IN	HTTP/1.1 400 Bad request content-length: 90 cache-control: no-cache content-type: text/html connection: close Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 72 65 71 75 65 73 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 6e 20 69 6e 76 61 6c 69 64 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 400 Bad request Your browser sent an invalid request.</body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5620 Parent PID: 4852

General

Start time:	00:55:57
Start date:	04/08/2021
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 'http://fdcsa.cloud/'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 5784 Parent PID: 5620

General

Start time:	00:55:58
Start date:	04/08/2021
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=1616,316435080101015694,457177829465774434 8,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly