ID: 458992
Cookbook: browseurl.jbs
Time: 01:20:53
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

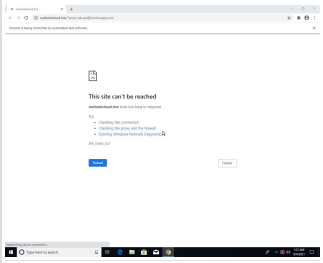
Windows Analysis Report https://securecloud-oauth.her…

Overview

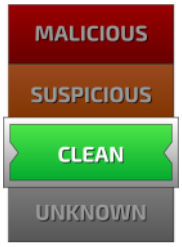
General Information

Sample URL:	http://https://securecloud-oauth.herokuapp.com/#abuse@herokuapp.com
Analysis ID:	458992
Infos:	

Most interesting Screenshot:



Detection

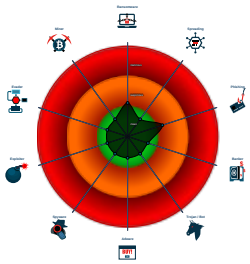


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

URL contains potential PII (phishing…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 1956 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://securecloud-oauth.herokuapp.com/#abuse@herokuapp.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5872 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,12548367778192904546,15575364818820007l7,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1740 /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

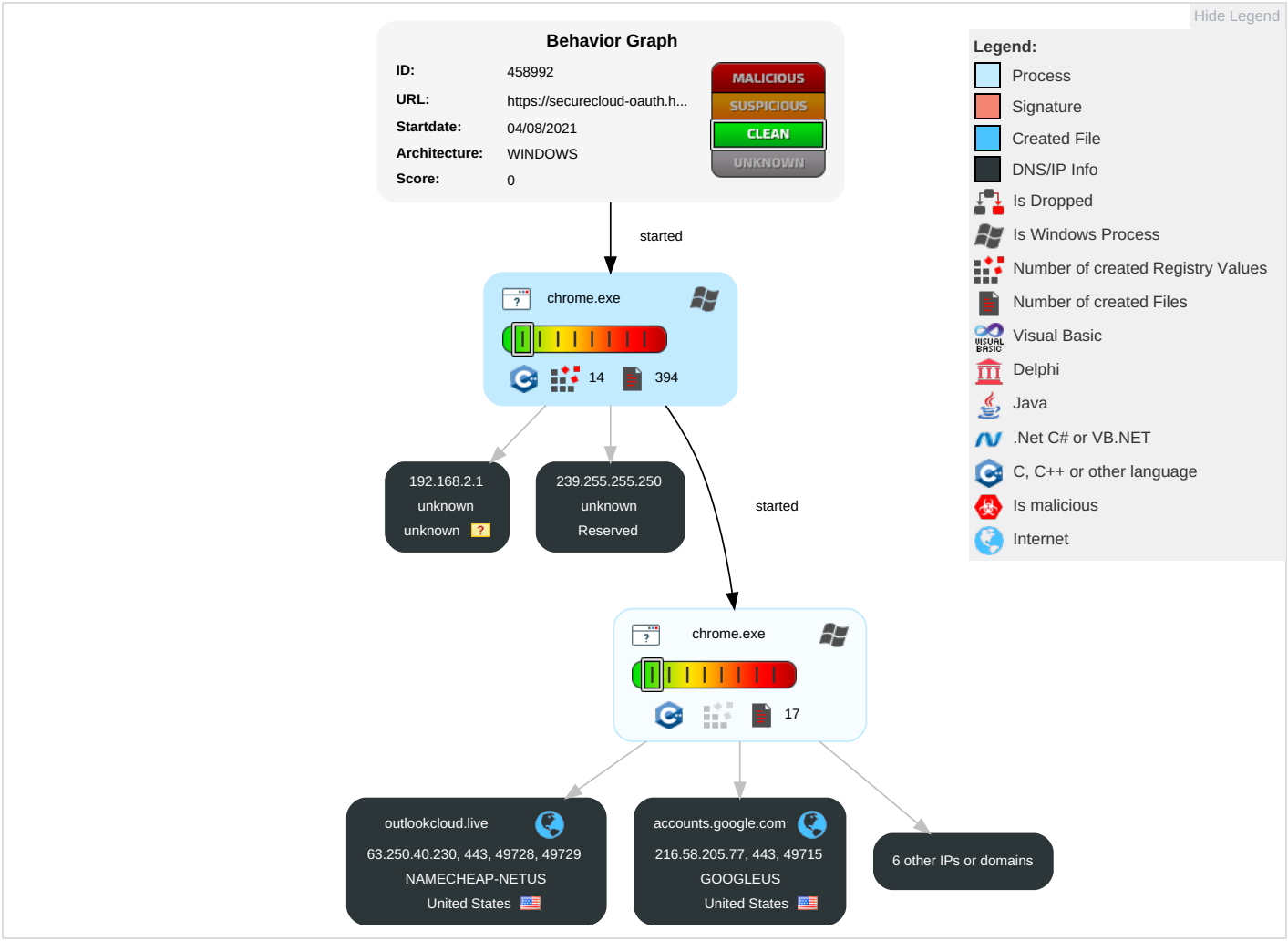
Click to jump to signature section

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

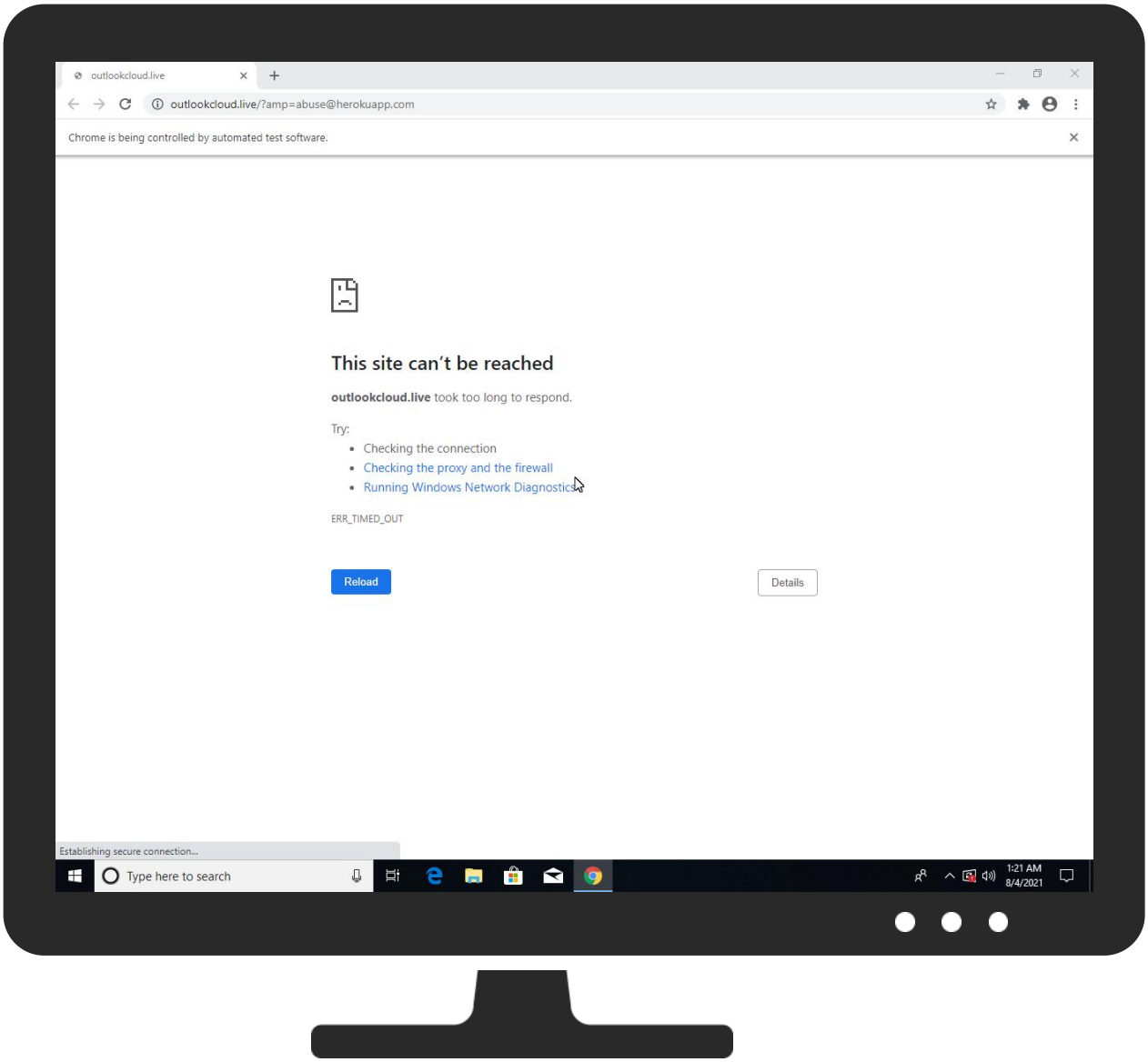
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://securecloud-oauth.herokuapp.com/#abuse@herokuapp.com	0%	Virustotal		Browse
http://https://securecloud-oauth.herokuapp.com/#abuse@herokuapp.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
securecloud-oauth.herokuapp.com	0%	Virustotal		Browse
outlookcloud.live	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://securecloud-oauth.herokuapp.com/#abuse	0%	Virustotal		Browse
http://https://securecloud-oauth.herokuapp.com/#abuse	0%	Avira URL Cloud	safe	
http://https://outlookcloud.live/?amp=abuse	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://securecloud-oauth.herokuapp.com/	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://securecloud-oauth.herokuapp.com	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.205.77	true	false		high
securecloud-oauth.herokuapp.com	3.223.221.167	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	216.58.208.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
outlookcloud.live	63.250.40.230	true	false	• 1%, Virustotal, Browse	unknown
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
63.250.40.230	outlookcloud.live	United States		22612	NAMECHEAP-NETUS	false
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
3.223.221.167	securecloud-oauth.herokuapp.com	United States		14618	AMAZON-AESUS	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:	458992
Start date:	04.08.2021
Start time:	01:20:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 42s
Hypervisor based Inspection enabled:	false

Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://securecloud-oauth.herokuapp.com/#abuse@herokuapp.com
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:	17
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@32/204@5/8
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
01:21:48	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

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

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{..,."':o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..l.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....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):	3.1392054451166236
Encrypted:	false
SSDEEP:	6:kK4doW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:w5kPlE99SNxAhUe0et
MD5:	439ECE741552FD2FD96520A55ADB80E4
SHA1:	4F709B04E813D2D6F9E4018B7C5FD07482735EF1
SHA-256:	A783C6A09F3AB5D8A6572FCD1B22FBCD4CA827D14D674F67FF057DE5BBADA0E4
SHA-512:	DCE1C058F529F8F62C098359F92E02E0513714D278AED6F2F41EC29250D34CE33DA1ABB5282C7BA2A623B1AC2285893B3B751DBE6A5C8BAE2235012789E957F
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\407fdfc4-1dc6-4f55-b074-c140375b6c39.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	95428
Entropy (8bit):	3.7493079716874647
Encrypted:	false
SSDEEP:	384:RPRumYbdgTw+VTV65Nmrzv6y3RqgtHIRGtkrPM+QxBkU03r/GmzHNf8eKCZOkIKy:laeZRKok5AenAiocvjGaKACKJs

C:\Users\user\AppData\Local\Google\Chrome\User Data\407fdfc4-1dc6-4f55-b074-c140375b6c39.tmp	
MD5:	A68BE2558FE9EAE03AD7C42AB626F71B
SHA1:	098BEBD46DE77FD965E4DA3E5D00F75C695ED70A
SHA-256:	1DD4752E64463AEDFF0117928B34E88EA04635FE2B78D389B43B2000204FEFE0
SHA-512:	B4DEE9084BDB556893FBEDD46ACF864BB98244842B8F44BB6011C8EEB08ED4A0B84329406491C1953E20361597605931935 67AF716C434E598BD6BAB012BD27E
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\63591980-6a47-4d2b-9d91-eed9a394b096.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7496020037927913
Encrypted:	false
SSDEEP:	384:hPRumYbdgTw+VTV65Nmrzv6y3RqgtHIRGtkrPM+QxBkU03r/GmzQf8eKCZOkIKN/:VaeZRKoJ5AenAiocvjGaKACKJn
MD5:	07B9499221B1A6B2B2502119F41D212C
SHA1:	866F7674A3FD67BCBBCCC96678554A1F47D0F53D
SHA-256:	FA5736A884A8C8039C70F39E909CB887328C37DD70D4B9D36F8C71D9C75F089C
SHA-512:	8265C726700D1A17A344924FAEA621B5EA72F0A8A04D44BE397F2EBC92B81B8DC88992A15FB3A5D62F1F8EDE8520F2CF4F9C36AB8FC3CAC72A01B218F6DA49 2
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\6e22357c-0abe-42d4-a674-9d1e2a882347.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):	174337
Entropy (8bit):	6.079378767676914
Encrypted:	false
SSDEEP:	3072:Tl7GaYTJQE+mugy9+QV1T7IRwdfLSNP4FcbXafIB0u1GOJmA3iuRL:ZaxaV+QfT7GSmhmaqfIlUOoSiuRL
MD5:	4B9F0E01D10B0CE283E21DF5C9674C2B
SHA1:	F00A407E7910DCE42628B5C37C69F5A939F3617A
SHA-256:	5ACFD754080E972AA7DE0051359AE27D9526F556F4940139285BE5500D09AA2E
SHA-512:	AEE6C8A041816F9BADC1F9A1D86DCF4DC71A1FF9E47A664DA7C6962DEEEC18BFE845D180E0570F12DB7121E6B9C628AA5B07D02FD0AF88E79DB6C4C3B6205 06A
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":1.628065305353572e+12,"network":1.628032906e+12,"ticks":7042783713.0,"uncertainty":4539989.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016335422"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\744d6a6a-6890-4d67-9f00-415cc091265a.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):	174337
Entropy (8bit):	6.079378960890367
Encrypted:	false
SSDEEP:	3072:hAiGaYTJQE+mugy9+QV1T7IRwdfLSNP4FcbXafIB0u1GOJmA3iuRL:q3xaV+QfT7GSmhmaqfIlUOoSiuRL
MD5:	FB324A97D4E2CDAFA30046DB83B8554C

C:\Users\user\AppData\Local\Google\Chrome\User Data\744d6a6a-6890-4d67-9f00-415cc091265a.tmp	
SHA1:	435A04FE0C8D34EAEEF724F39918557E9905DFBD
SHA-256:	156833ABFA3BC91FEE9D4CB6E191F077585B1707A8F120AFC46575EDBAB8A293
SHA-512:	AA6139D0C80A0EE46496BA18F579735F2CE96DE6282BD7C0CF3AB00A0EEF250A6AE930E08C9D676FA7B455035B4A72FB8DD03764ED064593E6B28A14C556784F
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":1.628065305353572e+12,"network":1.628032906e+12,"ticks":7042783713.0,"uncertainty":4539989.0}},"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\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:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D0212942563 72C916B8155AC
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\1c8611e7-9767-40b7-98fb-080600599041.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.536026569811818
Encrypted:	false
SSDEEP:	384:T6ttWLl6pXS1kXqKf/pUZNCgVLH2HfDHrUdHGmnTq/X4i:VLlaS1kXqKf/pUZNCgVLH2HfrrUBGmnO
MD5:	DE368A20D139676D95760463B159ECDC
SHA1:	DF1D0A440EF8B279BAFECD74D132B0E5125FA22D
SHA-256:	733FD1EE5C5A3DD101B98556612C1315A8C208F346E29639982C954231626D7A
SHA-512:	9165B111364CF88B6FF579477A9FF4679224F93E24E80A38ED35B8EA322685087EE5175A4F152D595C4B3B3ACEDD5790B0763186C2FFEFF117A110949E27FB1F
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":"13272538902336091","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ea9fa42-651e-49b6-b335-1db1c80c7013.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):	4.89615034618684
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5slRLsVTsY6SPs0DsVyKsT3gYhbD:JTnOCXGDHzuSkcwexhH
MD5:	4F1483747C84BC991B66C594F3D17B17
SHA1:	1F77773EE73E65D8C3CA6B7E2A4ED9B9E266BD73
SHA-256:	6945CC282B545A3F6E832253FE30ABCA001DFDB6C4BC9184A582204027025AED
SHA-512:	29805930EF89513FF7218093FB92FEB8D877A56F8B5CD2FF5FBADBDD010AC3DFABEAB7287E89616D589F77FA41856C9087ED3CCDB3D961BFB309DC46A5DFF10E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ea9fa42-651e-49b6-b335-1db1c80c7013.tmp	
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":"13275130907002097","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275130907007717","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\242dc786-0d28-45fe-b300-d4e2a8f25d86.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):	5143
Entropy (8bit):	4.986738447713696
Encrypted:	false
SSDEEP:	96:nhCmHX9pcKIr8ok0JCKL88kvS1vbOTQVuwn:nhCS9pc9L4Kdkat
MD5:	92A0A25019E7C653034A5AD6ED32CEB4
SHA1:	026F057AE9309F32F86100F47E07A90236AC63DC
SHA-256:	51D319BE15A34614B2A43FBDFEF4B0674AF9E5E450F307EECEF22E556071A431
SHA-512:	7961A255D227CABFAF5F7B4F7FA648BDCE5110B041B03607897FDDC86FBA72948A7DCDD96E3DDB6D0186C87EE8D2E09BB6D33230584EF3E83712ED4A3A3D4 DE
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272538902616079","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\312eeaf0-24ad-4793-95eb-a649fef18b37.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):	5.535803918938002
Encrypted:	false
SSDEEP:	384:T6ttWLl6pXS1kXqKf/pUZNCgVLH2HfDHrUdHGZnTqEFX46:VLlaS1kXqKf/pUZNCgVLH2HfrrUBGZn3
MD5:	66BF191A067AEAC6026F43DB293E097C
SHA1:	D0D54E3E68653F050822FA3829F915C1F30926C1
SHA-256:	5DB7EFCD0890F09BCBC5F97DC827232EAF0D2848A367FB34623A3ABC687272DA
SHA-512:	C83C1A0D2641F464E5A0536FE8646DA1CC72C8F685E756B1A2E979B0E7C754D13FB0473179F615AF20D7B202BB7698923211C9027A9FB20E287377A5BC356A36
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":"13272538902336091","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\3828018e-0f34-414e-bb05-b40c7d3a4ca5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3828018e-0f34-414e-bb05-b40c7d3a4ca5.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\55c64302-ee12-4fc0-a399-d0f0e79ebf4e.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):	1038
Entropy (8bit):	5.5626922784812765
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvtpA7wUU9RUenHQ:YI6UUhVseKUewqPeUer2UefPWwUyUenw
MD5:	5BDC24C37CDD072AEB129DC938EB6CAD
SHA1:	48E3C0D60B37CBDB7C902CDA068E56F5110181E3
SHA-256:	802476CC04D05A4361C9CC9AD07EC2C7AF4CDB035194CC5D1203E0CAFCBF371F
SHA-512:	5D4869DFFE421D3DF2D0892604E0853BF8A9D9D9B9A73978F77A60BF51B677841313354EF832DA6F24F0B8C40FBC68FCDE791E2BA95A827B275AB566D0DA58A
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":1659601307.002176,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628065307.00218},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7006c2c3-1605-4326-a86c-ee56ed483ca3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577337372987438
Encrypted:	false
SSDEEP:	384:T6ttDLl6pXS1kXqKf/pUZNCgVLH2HfDHrU9nX4LA:2LlaS1kXqKf/pUZNCgVLH2HfrrUZXH
MD5:	086878ABFD9D7A92226751D87E8FC02E
SHA1:	BE9E3CEB740EEA3003ACCB196BE706799959E840
SHA-256:	3D6FE6B7DCDEB972F9F00C27D35B82ED2DBF4DBC91E7822B0F129C98F8D44B73
SHA-512:	6BAC01F33CFD0C2204DCBC0A0C8BB29D9944C344428F8306C172ABA7DC4D6EFA39291A84D0727D9EBA57AE9BACBE7F1DE056AB5939BC509502496E9E96E712C
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":"13272538902336091","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\9ea1a38d-5039-4f4d-8deb-0432d87f5240.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):	5739
Entropy (8bit):	5.187138086182509
Encrypted:	false
SSDEEP:	96:nhCmqG9rvyJxQScKIr8ok0JCKL88kvS1vbOTQVuwn:nhCW9LyJKSc9L4Kdkat
MD5:	42A6324BB3B88E249B2E035B2FF17539
SHA1:	945DF601F710FF062B6B2AAC0F185837E2B868E0
SHA-256:	F7E9B21A646ACABF2597585846A6B2E3E72B0B3DFB1B972E33C5413F6D368A54
SHA-512:	27EA022D9144EB5F9FC11290E0C84A0638BCDB87A7C47A655A1F8C4502FE8C0F33AFE1FA535A7A9C7A853BAAB6ABD8B1AA33E2C1207103F451417F69A299533F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9ea1a38d-5039-4f4d-8deb-0432d87f5240.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272538902616079","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

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):	5.2230570840464905
Encrypted:	false
SSDEEP:	6:mgWL4q2PWXp+N23iKKdK9RXXTZIFUtp1Y3JZmwP1GNDkwOWXp+N23iKKdK9RXX5d:FWL4va5Kk7XT2FUtp1aJ/P1GND5f5KkT
MD5:	084C32D72416DD3A99925C8439C9CBF4
SHA1:	C8C334E0939FD697163FE2A1F7ED21B372491062
SHA-256:	90E13EE8B0780F95F7E57B6F8E64705F0D3371F0E26802BD51DCAFDFB712E4E3
SHA-512:	09182B03710003E31CEC0F7C17747B376A122A55F324A0ACE208215AFF1CB50494B715F178A7FF4B766E81A35913D3F372D9F94C081E6B0BE80F3CC3295693F4
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.127 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-01:21:58.136 1ab4 Recovering log #3.2021/08/04-01:21:58.138 1ab4 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.oldn (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2230570840464905
Encrypted:	false
SSDEEP:	6:mgWL4q2PWXp+N23iKKdK9RXXTZIFUtp1Y3JZmwP1GNDkwOWXp+N23iKKdK9RXX5d:FWL4va5Kk7XT2FUtp1aJ/P1GND5f5KkT
MD5:	084C32D72416DD3A99925C8439C9CBF4
SHA1:	C8C334E0939FD697163FE2A1F7ED21B372491062
SHA-256:	90E13EE8B0780F95F7E57B6F8E64705F0D3371F0E26802BD51DCAFDFB712E4E3
SHA-512:	09182B03710003E31CEC0F7C17747B376A122A55F324A0ACE208215AFF1CB50494B715F178A7FF4B766E81A35913D3F372D9F94C081E6B0BE80F3CC3295693F4
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.127 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-01:21:58.136 1ab4 Recovering log #3.2021/08/04-01:21:58.138 1ab4 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):	5.183495657484754
Encrypted:	false
SSDEEP:	6:mgJHL4q2PWXp+N23iKKdKyDZIFUtp1yRNJZmwP13Hj3DkwOWXp+N23iKKdKyJLJ:FJHL4va5Kk02FUtp1yLJ/P13j3D5f5K1
MD5:	4306654E4BC089B566BB1D297DB35141
SHA1:	43C8D5DF03B3B44A56712AAF27AF850F89543868
SHA-256:	B138BA67DC4DC3FFE2356072E03822D6A0153F38ACCB829E818C79A3DD955501
SHA-512:	F567283ED9CC688B5395EC0B5CD35AC359ACBD8932E9710E79D53E736DEC98BF319B08EB26C6201D1CF2D84A465504CE28E4F6EA3A556A0C6D67AD0D9AFC4C6
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.083 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-01:21:58.088 1ab4 Recovering log #3.2021/08/04-01:21:58.089 1ab4 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old (copy)	
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.183495657484754
Encrypted:	false
SSDEEP:	6:mgJHL4q2PWXp+N23iKKdKyDZIFUtp1yRNJZmwP13Hj3DkwOWXp+N23iKKdKyJLJ:FJHL4va5Kk02FUtp1yLJ/P13j3D5f5K1
MD5:	4306654E4BC089B566BB1D297DB35141
SHA1:	43C8D5DF03B3B44A56712AAF27AF850F89543868
SHA-256:	B138BA67DC4DC3FFE2356072E03822D6A0153F38ACCB829E818C79A3DD955501
SHA-512:	F567283ED9CC688B5395EC0B5CD35AC359ACBD8932E9710E79D53E736DEC98BF319B08EB26C6201D1CF2D84A465504CE28E4F6EA3A556A0C6D67AD0D9AFC4C6
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.083 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-01:21:58.088 1ab4 Recovering log #3.2021/08/04-01:21:58.089 1ab4 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):	0.9676589174760831
Encrypted:	false
SSDEEP:	24:ncLgAZOZD/RqLbJLbXaFpEO5bNmISHn06UwRt8:n8NOZRq5LLOpEO5J/Kn7Uo8
MD5:	8B2C3AC09E17AA96D073EE337E222BCC
SHA1:	D0B3F97AC02F4F72054C944F199996999AD6B6A6
SHA-256:	124D84797918841A941D09969C6B940597638A164653B51261B17DCE57E7C187
SHA-512:	2AE90E53DC7FF8BCFE784DEE043790ED4C1F3C5A811CE732E1969F02F686628CBEFEFC3C2F0DE13AA88D1083B90ED047E39A37BEB40E961BAB481E740DD0D9B
Malicious:	false
Reputation:	low
Preview:	.....;.R..... ....

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):	1232
Entropy (8bit):	3.613320933099622
Encrypted:	false
SSDEEP:	24:34SS2IlrlAzlNwqcgulaTtU+53DaO4U+5wZbkZxwRlL:34N1xmfPiWTaOTWGL
MD5:	2023EB9DA6815EEED66278E2A07111F5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
SHA1:	6CF5F427589B2867DD7CD7648420F41C94DF4C0C
SHA-256:	69C279C2FC29F7757F1372905AF7341304DD15D5688F283F599A1A91839B6852
SHA-512:	0600FAD07EDEF9AD9E9F797B8309A9EAB723B8B71180FF78DBE869C5838A7DFE4B7EFA4D7950E0AE835A3510FB53123B0AFA514A0E6B338839874EE2C83BA465
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...093f40ae_4bb1_47c7_86f5_e770a2b6f3ec.....9t.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....A..<.....2...https://outlookcloud.live/?amp=abuse@herokuapp.com.....L...H.....@.....h.....`.....8.....@.....8.....q.c~....r.c~....x.....l...2...h.t.t.p.s.:././.o.u.t.l.o.o.k.c.l.o.u.d...l.i.v.e./.?.a.m.p.=.a.b.u.s.e.@.h.e.r.o.k.u.a.p.p...c.o.m.....X...(...h.t.t.p.s.:././.s.e.c.u.r.e.c.l.o.u.d.-.o.a.u.t.h...h.e.r.o.k.u.a.p.p...c.o.m./.....8.....0.....8..... ...../...'...https://se

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):	5.183657367052181
Encrypted:	false
SSDEEP:	6:mgJ+gq2PWXp+N23iKKdK8aPrqIFUtp1JGujZmwP1J45kwOWXp+N23iKKdK8amLJ:FJ+gva5KkL3FUtp1JGuj/P1J+5f5KkQJ
MD5:	4373312D1E49BF9783F54643663CAB8A
SHA1:	BE43F8D590F76518B9805CEC1A2D56905CBA8FBC
SHA-256:	E91764F9E8EC601A6116E4C4537B3EF82BEACCFC5667BBE60EBB1CDE71074864
SHA-512:	27ACF8E61570F314952FABB52587137A68BC36DF671BA56913BF2418DC87CC38996EF651753649204A933241B499F252BBBAD9AF0AAC3A2CDF3ADE5286CDE4AC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.622 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-01:21:42.623 14b0 Recovering log #3.2021/08/04-01:21:42.624 14b0 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
Entropy (8bit):	5.183657367052181
Encrypted:	false
SSDEEP:	6:mgJ+gq2PWXp+N23iKKdK8aPrqIFUtp1JGujZmwP1J45kwOWXp+N23iKKdK8amLJ:FJ+gva5KkL3FUtp1JGuj/P1J+5f5KkQJ
MD5:	4373312D1E49BF9783F54643663CAB8A
SHA1:	BE43F8D590F76518B9805CEC1A2D56905CBA8FBC
SHA-256:	E91764F9E8EC601A6116E4C4537B3EF82BEACCFC5667BBE60EBB1CDE71074864
SHA-512:	27ACF8E61570F314952FABB52587137A68BC36DF671BA56913BF2418DC87CC38996EF651753649204A933241B499F252BBBAD9AF0AAC3A2CDF3ADE5286CDE4A C
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.622 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-01:21:42.623 14b0 Recovering log #3.2021/08/04-01:21:42.624 14b0 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................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):	317
Entropy (8bit):	5.221469520709735
Encrypted:	false
SSDEEP:	6:mgvn6+q2PWXp+N23iKKdK8NIFUtp1XZmwP1hSX9VkwOWXp+N23iKKdK8+eLJ:Ffbva5KkpFUtp1X/P1hST5f5KkqJ
MD5:	FCDE2D8028B4408541B5D5F726845344
SHA1:	595A3B24A805788A9179291CC8D049B383B22FCF
SHA-256:	9C6BD8DACD9F722437574D3F39B579B64BC2ECE5B167B9D73A13FD42E1AC321D
SHA-512:	F2F5E1DA9D228FF99D23A8B13B17EEA78AAB2B5D55211244ED8286DE5CC7987873D5B5ED328FFE02A3BBB19CD9AEE2F149432D5A26DE6A697197E6E9243521 B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:45.076 878 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-01 :21:45.077 878 Recovering log #3.2021/08/04-01:21:45.078 878 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.oldp (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.221469520709735
Encrypted:	false
SSDEEP:	6:mgvn6+q2PWXp+N23iKKdK8NIFUtp1XZmwP1hSX9VkwOWXp+N23iKKdK8+eLJ:Ffbva5KkpFUtp1X/P1hST5f5KkqJ
MD5:	FCDE2D8028B4408541B5D5F726845344

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.oldp (copy)	
SHA1:	595A3B24A805788A9179291CC8D049B383B22FCF
SHA-256:	9C6BD8DACD9F722437574D3F39B579B64BC2ECE5B167B9D73A13FD42E1AC321D
SHA-512:	F2F5E1DA9D228FF99D23A8B13B17EEA78AAB2B5D55211244ED8286DE5CC7987873D5B5ED328FFE02A3BBB19CD9AEE2F149432D5A26DE6A697197E6E9243521B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:45.076 878 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-01:21:45.077 878 Recovering log #3.2021/08/04-01:21:45.078 878 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=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["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=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.26242255019604
Encrypted:	false
SSDEEP:	6:mgN934q2PWXp+N23iKKdK25+Xqx8chI+IFUtp1J73JZmwP1JSLrDkwOWXp+N23ib:FNV4va5KkTXfchI3FUtp1JzJ/P1JorD6
MD5:	F6470F81E9CE3AFE6771EDA4715FCE4B
SHA1:	37507F3F1CFCD5FD660CFA8930FF261A8AE58688
SHA-256:	3FF70D77EA7283C6EBDE990BB46FB2B544D00C989007F3E3A2AB32FC9403690D
SHA-512:	1671420C6A1A3016975F71037742118326F93731E03E928DB8038D0218A802AF61F80E472FB5AC7AAE46015253D856454515B4CA780DFDE0D33F56A02CF5DB42
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.034 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-01:21:58.076 1ab4 Recovering log #3.2021/08/04-01:21:58.077 1ab4 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.a (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.26242255019604
Encrypted:	false
SSDEEP:	6:mgN934q2PWXp+N23iKKdK25+Xqx8chI+IFUtp1J73JZmwP1JSLrDkwOWXp+N23ib:FNV4va5KkTXfchI3FUtp1JzJ/P1JorD6
MD5:	F6470F81E9CE3AFE6771EDA4715FCE4B
SHA1:	37507F3F1CFCD5FD660CFA8930FF261A8AE58688
SHA-256:	3FF70D77EA7283C6EBDE990BB46FB2B544D00C989007F3E3A2AB32FC9403690D
SHA-512:	1671420C6A1A3016975F71037742118326F93731E03E928DB8038D0218A802AF61F80E472FB5AC7AAE46015253D856454515B4CA780DFDE0D33F56A02CF5DB42
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.034 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-01:21:58.076 1ab4 Recovering log #3.2021/08/04-01:21:58.077 1ab4 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):	5.274446399818093
Encrypted:	false
SSDEEP:	6:mgj0j34q2PWXp+N23iKKdK25+XuoIFUtp1jTED3JZmwP1jTED3DkwOWXp+N23iKX:Fm4va5KkTXYFUtp1EJ/P1ED5f5KkTXHJ
MD5:	1248278C4FA1B33AB5178A762316D403
SHA1:	D90F836EC76467E2A823690B43E2B5B457A5946E
SHA-256:	74708FC0956A1B8C15BC4A7BBC7A93131874AFAEE1745B023378FCF4BC42863F
SHA-512:	71A91B9CEF8830B23D24A9BE3145FDFF30C6119760F56F1DFF2EAB2FE804E945245E5409D21644929A57235130C9EC3BE345C27B07A9332EFA5C03A0E1A5AE9E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:57.984 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-01:21:57.986 1ab4 Recovering log #3.2021/08/04-01:21:57.986 1ab4 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.274446399818093
Encrypted:	false
SSDEEP:	6:mgj0j34q2PWXp+N23iKKdK25+XuoIFUtp1jTED3JZmwP1jTED3DkwOWXp+N23iKX:Fm4va5KkTXYFUtp1EJ/P1ED5f5KkTXHJ
MD5:	1248278C4FA1B33AB5178A762316D403
SHA1:	D90F836EC76467E2A823690B43E2B5B457A5946E
SHA-256:	74708FC0956A1B8C15BC4A7BBC7A93131874AFAEE1745B023378FCF4BC42863F
SHA-512:	71A91B9CEF8830B23D24A9BE3145FDFF30C6119760F56F1DFF2EAB2FE804E945245E5409D21644929A57235130C9EC3BE345C27B07A9332EFA5C03A0E1A5AE9E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:57.984 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-01:21:57.986 1ab4 Recovering log #3.2021/08/04-01:21:57.986 1ab4 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):	5.288933139874608
Encrypted:	false
SSDEEP:	6:mgjjn4q2PWXp+N23iKKdKWT5g1IdqIFUtp1jjZxF3JZmwP1jjQ3DkwOWXp+N23im:FX4va5Kkg5gSRFUtp1JxNJ/P1qD5f5Kg
MD5:	599391F18BCACA9D745EB643B5E8C34D
SHA1:	5E68B1A1A54567FA7AB009E54153B8F33A282BF0
SHA-256:	B875FEDC1E66FA57193E2557EAA9E8B05BAD305DD873902F832532F4853A04DD
SHA-512:	EA146A8620ECEF06C16BD86145256193475A900242C56DF0FCA6138E5DD14D2FAFDDFD529A302ABE8E9742065B32E21A1DA901D6516FF52557F11DF7130D9BD
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:57.972 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-01:21:57.974 1ab4 Recovering log #3.2021/08/04-01:21:57.975 1ab4 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.old0 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.288933139874608
Encrypted:	false
SSDEEP:	6:mgjjn4q2PWXp+N23iKKdKWT5g1IdqIFUtp1jjZxF3JZmwP1jjQ3DkwOWXp+N23im:FX4va5Kkg5gSRFUtp1JxNJ/P1qD5f5Kg
MD5:	599391F18BCACA9D745EB643B5E8C34D
SHA1:	5E68B1A1A54567FA7AB009E54153B8F33A282BF0
SHA-256:	B875FEDC1E66FA57193E2557EAA9E8B05BAD305DD873902F832532F4853A04DD
SHA-512:	EA146A8620ECEF06C16BD86145256193475A900242C56DF0FCA6138E5DD14D2FAFDDFD529A302ABE8E9742065B32E21A1DA901D6516FF52557F11DF7130D9BD
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:57.972 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-01:21:57.974 1ab4 Recovering log #3.2021/08/04-01:21:57.975 1ab4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.11783565942325995
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvPaH+RfxAQ1EnQFSDmnl+Oo/lCxthiZgGCxC+/eryGltAQ1EnQr:TL+A/ZlRfxA/USDmncNuQeGI/3+A/USc
MD5:	2AB6D6159DCCB9B1B60BC43406CE4DD2
SHA1:	5FA495BDD87487F7A138C608BC0CCAD1BA3CCC66
SHA-256:	BE18AD9D4166F0C56E5E2BB90937596D6D87E93BCAB999D41721CBE742A2F18B
SHA-512:	05BC625599151745935133374 9F48362EE2D8FED9D328FD2A3F1A99FF968FB8AAD6E57DC4E1FC3230CD552BE8FEA7F777B50584967136C0F69363ADE23393890

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	561
Entropy (8bit):	5.26619922404809
Encrypted:	false
SSDEEP:	12:Iohv0B3b4rCssegSEZVGomc+mqiWl+zetV2lh1YxD5Bk778B/xgskJfA/USnjfWb:Iohv01E57umc+kWl+zbh6xDY78BJgskl
MD5:	C8334947FBDCCB91C84AD2567142D883
SHA1:	C858FB7B56ED887B464F14BABA5B0EDAE8B9F292
SHA-256:	CDBAE0FBB8EF3D35BC58A3E68EAE4DAB5F181A36C67F23E8DA8F0120DCB10DDF
SHA-512:	37EEA41E2FD90D5D469CDFD114C42EE4D1658978D94FFFB11271D158DF5FEE63960B22B0A52C9963A9CA4D6DB4A1AD67F98287B8F13D1561BF4BE34A932D6ED
Malicious:	false
Reputation:	low
Preview:	....."=....abuse..com..herokuapp..https..oauth..securecloud..working*Y.....abuse.....com.....herokuapp.....https.....oauth.....securecloud.....working..2.....a.....b.....c.....d.....e.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....w...:A.....Bk...g.....*<https://securecloud-oauth.herokuapp.com/#abuse@herokuapp.com2.Working:.....J.....$)/9...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11651018133072062
Encrypted:	false
SSDEEP:	12:woCqLBj/W4t3l+4nMWQA9LcihBQZ8fOAS:+qLB3t3NbNcITfU
MD5:	4329B91DA0BA99BA8536F4068B717C00
SHA1:	FE4C4304B4C1DB8FA79602846098FF17E5925788
SHA-256:	73D73A95794D440C5F504BF8FF93EEAEF32E2ED3CC97B9B5A3D02EEAE18D0A3A
SHA-512:	9EDF0D50D73A920E1CFB4830B4FC6C7F97F1B5D740E778C207F1F8222C75BEF79DD26295A45EF931BA59FD2A1B90AB423DFC019BF60472D4F9F193E2567EA1E2
Malicious:	false
Reputation:	low
Preview:	.....c~..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session.| (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1232
Entropy (8bit):	3.613320933099622
Encrypted:	false
SSDEEP:	24:34SS2llrlAzlNwqcgulaTtU+53DaO4U+5wZbkZxwRlL:34N1xmfPiWTaOTWGL
MD5:	2023EB9DA6815EEED66278E2A07111F5
SHA1:	6CF5F427589B2867DD7CD7648420F41C94DF4C0C
SHA-256:	69C279C2FC29F7757F1372905AF7341304DD15D5688F283F599A1A91839B6852
SHA-512:	0600FAD07EDEF9AD9E9F797B8309A9EAB723B8B71180FF78DBE869C5838A7DFE4B7EFA4D7950E0AE835A3510FB53123B0AFA514A0E6B338839874EE2C83BA465
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...093f40ae_4bb1_47c7_86f5_e770a2b6f3ec.....9t..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....A..<.....2...https://outlookcloud.live/?amp=abuse@herokuapp.com.....L...H.....@.....h.....`.....8.....@.....8.....q.c~....r.c~....x.....l...2...h.t.t.p.s.:.//.o.u.t.l.o.o.k.c.l.o.u.d...l.i.v.e./.?.a.m.p.=.a.b.u.s.e.@.h.e.r.o.k.u.a.p.p...c.o.m.....X...(...h.t.t.p.s.:.//.s.e.c.u.r.e.c.l.o.u.d.-.o.a.u.t.h...h.e.r.o.k.u.a.p.p...c.o.m./.....8.....0.....8..... ...../...'...https://se

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabs.. (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):	5.4830017154344395
Encrypted:	false
SSDEEP:	48:F/GCfa7qMB8db8hx2bQSefgGDNrS0U9RdiN9J:Ra7qMCdb8hx2bQ5fgGRrS0/
MD5:	5990B6D9FB0D6D0657D3E40ADBB38A6A
SHA1:	4D4247579C982A48150432205469C1EE0087DC26
SHA-256:	EC0E5E12B46F65B8EFDA731A0E49CAD892C49D836DFF974C7D565CF03831BEFB
SHA-512:	88A5A7E533CCE81ABBED9936F36DACDA9DC4BA0AAF9F3BBD702660AF7979AB599EA5E9F8870476A6AAF51E172673CC39B2C2E49A879A5EB02F37019E68ED2EBA
Malicious:	false
Reputation:	low
Preview:	.G.4...*.....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..152138000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-04 01:21:59.35][INFO][mr.Init] MR instance ID: 7354ae8f-148f-4671-90a0-baa622c65d63\n","[2021-08-04 01:21:59.35][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-04 01:21:59.35][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-04 01:21:59.35][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-04 01:21:59.35][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-04 01:21:59.35][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-04 01:21:59.35][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.108580978835119
Encrypted:	false
SSDEEP:	6:mgJ+ML+q2PWXp+N23iKKdK8a2jMGIFUtp1JMUnzKWZmwP1JOVaLVkwOWXp+N23iP:FJ+ML+va5Kk8EFUtp1JcW/P1JO0LV5fs
MD5:	4452121018B27D90D36339FC5C21CC1B
SHA1:	4457F827F09B7EF6D1787DFEB33601E32AF15D17
SHA-256:	CF3D9E23BF942276523C795EE53BF3F1D0A3BF3090F61957BE413C985E97503F
SHA-512:	F41F4BE1FE1DCB4888BFC318554E1CCD2E88D174EBD45F96645FAD476A5E549E51F06A15E21800FB59D24618EA7F9D6C7DE0375196A149071C3323B1B892707
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.407 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:21:42.409 10ec Recovering log #3.2021/08/04-01:21:42.410 10ec 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):	5.108580978835119
Encrypted:	false
SSDEEP:	6:mgJ+ML+q2PWXp+N23iKKdK8a2jMGIFUtp1JMUnzKWZmwP1JOVaLVkwOWXp+N23iP:FJ+ML+va5Kk8EFUtp1JcW/P1JO0LV5fs
MD5:	4452121018B27D90D36339FC5C21CC1B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
SHA1:	4457F827F09B7EF6D1787DFEB33601E32AF15D17
SHA-256:	CF3D9E23BF942276523C795EE53BF3F1D0A3BF3090F61957BE413C985E97503F
SHA-512:	F41F4BE1FE1DCB4888BFC318554E1CCD2E88D174EBD45F96645FAD476A5E549E51F06A15E21800FB59D24618EA7F9D6C7DE0375196A149071C3323B1B892707
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.407 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:21:42.409 10ec Recovering log #3.2021/08/04-01:21:42.410 10ec 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):	4.89615034618684
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5slRLsVTsY6SPs0DsVyKsT3gYhbD:JTnOCXGDHzuSkcwexhH
MD5:	4F1483747C84BC991B66C594F3D17B17
SHA1:	1F77773EE73E65D8C3CA6B7E2A4ED9B9E266BD73
SHA-256:	6945CC282B545A3F6E832253FE30ABCA001DFDB6C4BC9184A582204027025AED
SHA-512:	29805930EF89513FF7218093FB92FEB8D877A56F8B5CD2FF5FBADBDD010AC3DFABEAB7287E89616D589F77FA41856C9087ED3CCDB3D961BFB309DC46A5DFF10E
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":"13275130907002097","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275130907007717","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

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):	5.23381288548764
Encrypted:	false
SSDEEP:	6:mgJW0JjM+q2PWXp+N23iKKdKgXz4rRIFUtp1J0ZmwP1JyFUmMVkwOWXp+N23iKK2:FJWijM+va5KkgXiuFUtp1J0/P1JyFlM5
MD5:	C16DB0064A6F25EE53FF3B1D6E766D47
SHA1:	2CB56F8CAA07F85EC4240C227DB42BE080001B9C
SHA-256:	466EB1E5D94F4ACF95FC7751607ACB4C11A7BF37FD036742F4380FE436A8A6A1
SHA-512:	21A5B03A04D6A5498303385B8357C04132F545E7CF0CC4FA830EC8E86DF4D28DBE259CA5A7714ECB670AA3E0F8BD09C7C715E12D98F3342937B56D095B6E986
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.639 158c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-01:21:42.640 158c Recovering log #3.2021/08/04-01:21:42.641 158c 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):	5.23381288548764
Encrypted:	false
SSDEEP:	6:mgJW0JjM+q2PWXp+N23iKKdKgXz4rRIFUtp1J0ZmwP1JyFUmMVkwOWXp+N23iKK2:FJWijM+va5KkgXiuFUtp1J0/P1JyFlM5
MD5:	C16DB0064A6F25EE53FF3B1D6E766D47
SHA1:	2CB56F8CAA07F85EC4240C227DB42BE080001B9C
SHA-256:	466EB1E5D94F4ACF95FC7751607ACB4C11A7BF37FD036742F4380FE436A8A6A1
SHA-512:	21A5B03A04D6A5498303385B8357C04132F545E7CF0CC4FA830EC8E86DF4D28DBE259CA5A7714ECB670AA3E0F8BD09C7C715E12D98F3342937B56D095B6E986
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old[, (copy)	
Preview:	2021/08/04-01:21:42.639 158c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-01:21:42.640 158c Recovering log #3.2021/08/04-01:21:42.641 158c 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):	5765
Entropy (8bit):	5.188907843272366
Encrypted:	false
SSDEEP:	96:nhCmTG9rvyJxQScKIr8ok0JCKL88kvS1MbOTQVuwn:nhCB9LyJKSc9L4Kdka8
MD5:	215E8345DA80D7DB30613B1CDFB15E79
SHA1:	9029E1E844317965EFF75E4B21747E11BF069080
SHA-256:	0D3F7B8A55F2A8AA0DE764F52D0BABAD64F1A4240DAAAED13977B715307E4689
SHA-512:	2EC7B5004FFF620DD67D4C545CDAE6EAA08C2CCEE2EE63F30417C635FA53B3048D317B33F0F638ED1B0C16AFC05F40454BF3D78A0E3556CE178D06CC37331E7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272538902616079","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1798003135526698
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU9oTRs/oTRseCB:wIElwQF8mpcSibT/o1
MD5:	553ED19428DE6F930E593C27FE45E2E4
SHA1:	1F9EA2CF7AA3696373208E9F031C3B9CD26125C1
SHA-256:	198F080C21C050F8181645E810929C18E794BE3BCFDF067275D2292377EA4C43
SHA-512:	A72932772330702D1BD766EE47C40ED61402E1C6B7C9B0C72E6CAED5F735411DF947F97D1E90922D4C100DA768EDD0C761FA74F1710EC9CBBB3D5B2814C083A
Malicious:	false
Reputation:	low
Preview:	SQLite format 3......@ ....C..........g...^.........j..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8252634780891891
Encrypted:	false
SSDEEP:	48:yHIqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUc6:yohIElwQF8mpcS9
MD5:	09C921ADDB62B1C81207A6973DA7DA82
SHA1:	4E03CC62BB971DE425770EA1BC63E49B6CA79A9C
SHA-256:	03EAA76D9170F75830384BA2169AF8920AD8EF6AA591B32B730C1C6669ACAFFB
SHA-512:	F6D68A8D92AAD96EF4C853E95D34EBD13BD81425A1BF51CA28A0F26F5810C1624DBDE4ED716A682303ED55A97C76CCF5474878F4803AA4D282D5275C7C8C197
Malicious:	false
Reputation:	low
Preview:	............I.X..

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):	5.535803918938002
Encrypted:	false
SSDEEP:	384:T6ttWLl6pXS1kXqKf/pUZNCgVLH2HfDHrUdHGZnTqEFX46:VLlaS1kXqKf/pUZNCgVLH2HfrrUBGZn3
MD5:	66BF191A067AEAC6026F43DB293E097C
SHA1:	D0D54E3E68653F050822FA3829F915C1F30926C1
SHA-256:	5DB7EFCD0890F09BCBC5F97DC827232EAF0D2848A367FB34623A3ABC687272DA
SHA-512:	C83C1A0D2641F464E5A0536FE8646DA1CC72C8F685E756B1A2E979B0E7C754D13FB0473179F615AF20D7B202BB7698923211C9027A9FB20E287377A5BC356A36
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":"13272538902336091","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.179900852184048
Encrypted:	false
SSDEEP:	6:mgJiyq2PWXp+N23iKKdKrQMxIFUtp1JZe81ZmwP1JZeqRkwOWXp+N23iKKdKrQMT:FJHva5KkCFUtp1Jj1/P1JD5f5KktJ
MD5:	8357EAB3DA75A076A5F754912892C339
SHA1:	F40E09AA3CFCD31F99710CA407C44369A834DE7D
SHA-256:	14363EC75F09D6D186B8660E70383ECC28CB8E4646E980D0EFF6574D7B8605D5
SHA-512:	CEA45CA101CAD9521AAE55020A7F273BD4B522BE005CDEE94D2EBEF208547F2650A9E5C47D5E16DC9ED06BB0E769D670671CDE2A4325EF80ACCA0E975B457D4A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.566 14c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-01:21:42.567 14c0 Recovering log #3.2021/08/04-01:21:42.567 14c0 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):	5.179900852184048
Encrypted:	false
SSDEEP:	6:mgJiyq2PWXp+N23iKKdKrQMxIFUtp1JZe81ZmwP1JZeqRkwOWXp+N23iKKdKrQMT:FJHva5KkCFUtp1Jj1/P1JD5f5KktJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old. (copy)	
MD5:	8357EAB3DA75A076A5F754912892C339
SHA1:	F40E09AA3CFCD31F99710CA407C44369A834DE7D
SHA-256:	14363EC75F09D6D186B8660E70383ECC28CB8E4646E980D0EFF6574D7B8605D5
SHA-512:	CEA45CA101CAD9521AAE55020A7F273BD4B522BE005CDEE94D2EBEF208547F2650A9E5C47D5E16DC9ED06BB0E769D670671CDE2A4325EF80ACCA0E975B457D4A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.566 14c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-01:21:42.567 14c0 Recovering log #3.2021/08/04-01:21:42.567 14c0 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):	5.129923658346133
Encrypted:	false
SSDEEP:	6:mgJVVq2PWXp+N23iKKdK7Uh2ghZIFUtp1JfpgZmwP1JGUXIkwOWXp+N23iKKdK7w:FJfva5KkIhHh2FUtp1Jfm/P1JD45f5KF
MD5:	C7695B2BF564F37A64090787AE23EA56
SHA1:	A4BC4E28F5AB6C9F05694D1F6C06A9F20B42E671
SHA-256:	54CAC2D2D0F2C0A3FF9800EB808B113BF194D0BFB0D02F05FE3E54E18EAEC9B0
SHA-512:	554A8680F2B1B5C0C173B32F6BBB390222F3F929C90CC9A03BB228E015AE838EC335ED55D9341CCFDBBD30AF1A44CA8983E9BDDA9D25813243CDBE1E810A07E1
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.328 14c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/04-01:21:42.337 14c4 Recovering log #3.2021/08/04-01:21:42.344 14c4 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.oldre (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.129923658346133
Encrypted:	false
SSDEEP:	6:mgJVVq2PWXp+N23iKKdK7Uh2ghZIFUtp1JfpgZmwP1JGUXIkwOWXp+N23iKKdK7w:FJfva5KkIhHh2FUtp1Jfm/P1JD45f5KF
MD5:	C7695B2BF564F37A64090787AE23EA56
SHA1:	A4BC4E28F5AB6C9F05694D1F6C06A9F20B42E671
SHA-256:	54CAC2D2D0F2C0A3FF9800EB808B113BF194D0BFB0D02F05FE3E54E18EAEC9B0
SHA-512:	554A8680F2B1B5C0C173B32F6BBB390222F3F929C90CC9A03BB228E015AE838EC335ED55D9341CCFDBBD30AF1A44CA8983E9BDDA9D25813243CDBE1E810A07E1
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.328 14c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/04-01:21:42.337 14c4 Recovering log #3.2021/08/04-01:21:42.344 14c4 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\17993abe-5598-4d60-9531-709b347999fd.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\17993abe-5598-4d60-9531-709b347999fd.tmp	
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):	427
Entropy (8bit):	5.264259760967136
Encrypted:	false
SSDEEP:	6:mgJUF4q2PWXp+N23iKKdKusNpV/2jMGIFUtp1JUuZmwP1JU/zkwOWXp+N23iKKdD:FJTva5KkFFUtp1JX/P1Jg5f5KkOJ
MD5:	9AFD0FA084715D7AFEFAEB8CE948D4BD
SHA1:	6FA66DF7B63B24648EBF8A465AA874CD83F78DC2
SHA-256:	E15C6B6DE5F69499FA7340F477E86E6A73D992E845AB9E2C8E53B9311992A2A4
SHA-512:	1B98FAC9DAE538F00922217EB25B1A1516779274EC47FE31C3344EBECFE15CC343D9DB24B3E47FB11743E9DE17B3F650A54C2C4AEF406A7AEFE74FFBCDD5BBA9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.612 970 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:21:42.613 970 Recovering log #3.2021/08/04-01:21:42.614 970 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
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.264259760967136
Encrypted:	false
SSDEEP:	6:mgJUF4q2PWXp+N23iKKdKusNpV/2jMGIFUtp1JUuZmwP1JU/zkwOWXp+N23iKKdD:FJTva5KkFFUtp1JX/P1Jg5f5KkOJ
MD5:	9AFD0FA084715D7AFEFAEB8CE948D4BD
SHA1:	6FA66DF7B63B24648EBF8A465AA874CD83F78DC2
SHA-256:	E15C6B6DE5F69499FA7340F477E86E6A73D992E845AB9E2C8E53B9311992A2A4
SHA-512:	1B98FAC9DAE538F00922217EB25B1A1516779274EC47FE31C3344EBECFE15CC343D9DB24B3E47FB11743E9DE17B3F650A54C2C4AEF406A7AEFE74FFBCDD5BBA9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.612 970 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:21:42.613 970 Recovering log #3.2021/08/04-01:21:42.614 970 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\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State. (copy)	
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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.308225096047378
Encrypted:	false
SSDEEP:	12:FJWslyva5KkmiuFUtp1JWiG/P1J6R5f5Kkm2J:FJT6a5KkSgzJiJlf5Kkr
MD5:	1305CB65175505FB57573385355EEFD4
SHA1:	B9D94981DC9E9BF6AD37733A720BF16FBDAB304F
SHA-256:	451C8AA033F3B36E12C0862CB2BEAEC6B20A56A188E1B9FC2E5162913E4C12E7
SHA-512:	27B126B2190E5926F52E0DF2EE190F84A49F277629CC7F810EF7803B5A19026362ECF23B53933411E42F84C350008548A2D93C63A90F5C3D11A9E87FD8561914
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.638 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/04-01:21:42.639 1570 Recovering log #3.2021/08/04-01:21:42.640 1570 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):	5.308225096047378
Encrypted:	false
SSDEEP:	12:FJWslyva5KkmiuFUtp1JWiG/P1J6R5f5Kkm2J:FJT6a5KkSgzJiJlf5Kkr
MD5:	1305CB65175505FB57573385355EEFD4
SHA1:	B9D94981DC9E9BF6AD37733A720BF16FBDAB304F
SHA-256:	451C8AA033F3B36E12C0862CB2BEAEC6B20A56A188E1B9FC2E5162913E4C12E7
SHA-512:	27B126B2190E5926F52E0DF2EE190F84A49F277629CC7F810EF7803B5A19026362ECF23B53933411E42F84C350008548A2D93C63A90F5C3D11A9E87FD8561914
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.638 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/04-01:21:42.639 1570 Recovering log #3.2021/08/04-01:21:42.640 1570 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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.270303430037827
Encrypted:	false
SSDEEP:	6:mgtf+3+q2PWXp+N23iKKdKusNpZQMxIFUtp1tRuZmwP1tRqVkwOWXp+N23iKKdKl:Ft2Ova5KkMFUtp1tRu/P1tRC5f5KkTJ
MD5:	132CFFE55A036C2AA057090AD94769E5
SHA1:	60709598DCD9599478014B9E7EAEBFD53E64196C
SHA-256:	6B8073DC2E2967311E08675FD9D767636DCF29224034EACC6F6B52D41A2D31FA
SHA-512:	8019EBD39557C2F1210105E3FF580D3C2ACDD0E81A741168CF8370AD4890F83BA06FD28E3B0F6E43D97BBF0203EA7E01BAD75C3EB2EB2FCD8C0DED768E840E 26
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:59.077 a88 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Session Storage/MANIFEST-000001.2021/08/04-01:21:59.079 a88 Recovering log #3.2021/08/04-01:21:59.079 a88 Reusing old log C:\Users\user\AppData\Lo cal\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.oldes (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.270303430037827
Encrypted:	false
SSDEEP:	6:mgtf+3+q2PWXp+N23iKKdKusNpZQMxIFUtp1tRuZmwP1tRqVkwOWXp+N23iKKdKl:Ft2Ova5KkMFUtp1tRu/P1tRC5f5KkTJ
MD5:	132CFFE55A036C2AA057090AD94769E5
SHA1:	60709598DCD9599478014B9E7EAEBFD53E64196C
SHA-256:	6B8073DC2E2967311E08675FD9D767636DCF29224034EACC6F6B52D41A2D31FA
SHA-512:	8019EBD39557C2F1210105E3FF580D3C2ACDD0E81A741168CF8370AD4890F83BA06FD28E3B0F6E43D97BBF0203EA7E01BAD75C3EB2EB2FCD8C0DED768E840E 26
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:59.077 a88 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Session Storage/MANIFEST-000001.2021/08/04-01:21:59.079 a88 Recovering log #3.2021/08/04-01:21:59.079 a88 Reusing old log C:\Users\user\AppData\Lo cal\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\97cd849e-c5e8-4760-9af5-2ae8b4d0d089.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\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
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):	5.184279011909439
Encrypted:	false
SSDEEP:	12:FpRM+va5KkkGHArBFUtp1p3/P1pFMV5f5KkkGHAryJ:FpRda5KkkGgPgzp1pF2f5KkkGga
MD5:	0D3F08923EBA6396EA378930DC6D3039
SHA1:	CEC351C2E84EE3C37F7200C05BE960BBDBAEEC09
SHA-256:	0DDC0033A096C73E8E8C3B2AEC68B53FC33AFAD7B712ABC031232A44A5778D62
SHA-512:	A995F39D21DCF8AFD18EF1EBF48EC59F2703D8D996270454B3070E1EB952BC17BA9804B9477C8754CD6751F103162234313A5F0058E8D5137BE346BDD54F0B5E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.214 158c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:21:58.217 158c Recovering log #3.2021/08/04-01:21:58.218 158c 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.old10 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.184279011909439
Encrypted:	false
SSDEEP:	12:FpRM+va5KkkGHArBFUtp1p3/P1pFMV5f5KkkGHAryJ:FpRda5KkkGgPgzp1pF2f5KkkGga
MD5:	0D3F08923EBA6396EA378930DC6D3039
SHA1:	CEC351C2E84EE3C37F7200C05BE960BBDBAEEC09
SHA-256:	0DDC0033A096C73E8E8C3B2AEC68B53FC33AFAD7B712ABC031232A44A5778D62
SHA-512:	A995F39D21DCF8AFD18EF1EBF48EC59F2703D8D996270454B3070E1EB952BC17BA9804B9477C8754CD6751F103162234313A5F0058E8D5137BE346BDD54F0B5E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.214 158c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:21:58.217 158c Recovering log #3.2021/08/04-01:21:58.218 158c 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
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	5.217696644515243
Encrypted:	false
SSDEEP:	12:Fpryva5KkkGHArqiuFUtp1p8vZ/P1piS9R5f5KkkGHArq2J:Fp0a5KkkGgCgzp8vHpikf5KkkGg7
MD5:	20DFA3975EEC2C5FA0446954044328E3
SHA1:	C3365BA14475E6EE78B90AA878BCDBB16AF23160
SHA-256:	A4188FB1FC66AE63A1D290A7D58AF435BF0583CE2B8B83140777C2314CE9AE42
SHA-512:	AA62069793F0187A3C50059E9581BFB16C416EED3B44C72352F8B6096A3DB1E71277597D6EAA628E215C09D7E2659F24A8A8B3F27441AAE25DBF65272677F73D
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.215 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/04-01:21:58.218 1570 Recovering log #3.2021/08/04-01:21:58.219 1570 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):	5.217696644515243
Encrypted:	false
SSDEEP:	12:Fpryva5KkkGHArqiuFUtp1p8vZ/P1piS9R5f5KkkGHArq2J:Fp0a5KkkGgCgzp8vHpikf5KkkGg7
MD5:	20DFA3975EEC2C5FA0446954044328E3
SHA1:	C3365BA14475E6EE78B90AA878BCDBB16AF23160
SHA-256:	A4188FB1FC66AE63A1D290A7D58AF435BF0583CE2B8B83140777C2314CE9AE42
SHA-512:	AA62069793F0187A3C50059E9581BFB16C416EED3B44C72352F8B6096A3DB1E71277597D6EAA628E215C09D7E2659F24A8A8B3F27441AAE25DBF65272677F73D
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.215 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/04-01:21:58.218 1570 Recovering log #3.2021/08/04-01:21:58.219 1570 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
Size (bytes):	418
Entropy (8bit):	5.19185992325086
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
SSDEEP:	12:adyva5KkkGHArAFUtpgu/P8R5f5KkkGHArfJ:aSa5KkkGgkgezf5KkkGgV
MD5:	CD13871ACF1FED7D01D0B0B80B28DBCB
SHA1:	E349BBD2C266BD436882D33332241A45827B0B2A
SHA-256:	3BABFBCA19D55EE93821685DA5587FE97666F62DF4CCF80CD71F4D9AEADE2D85
SHA-512:	BAE3C51DEF041758DDCF1C10B27DF9E086F69D411881506AB6186D0882378E6AA69FD4DFDCC7E72C136B956B0C66B1F3D8E7BE4607960A8369BB7B0A35AF5D9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:22:13.405 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/04-01:22:13.406 1570 Recovering log #3.2021/08/04-01:22:13.407 1570 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.oldon (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.19185992325086
Encrypted:	false
SSDEEP:	12:adyva5KkkGHArAFUtpgu/P8R5f5KkkGHArfJ:aSa5KkkGgkgezf5KkkGgV
MD5:	CD13871ACF1FED7D01D0B0B80B28DBCB
SHA1:	E349BBD2C266BD436882D33332241A45827B0B2A
SHA-256:	3BABFBCA19D55EE93821685DA5587FE97666F62DF4CCF80CD71F4D9AEADE2D85
SHA-512:	BAE3C51DEF041758DDCF1C10B27DF9E086F69D411881506AB6186D0882378E6AA69FD4DFDCC7E72C136B956B0C66B1F3D8E7BE4607960A8369BB7B0A35AF5D9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:22:13.405 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/04-01:22:13.406 1570 Recovering log #3.2021/08/04-01:22:13.407 1570 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.245888622180551
Encrypted:	false
SSDEEP:	6:mgJ56+q2PWXp+N23iKKdKpIFUtp1JbXZmwP1JztVkwOWXp+N23iKKdKa/WLJ:FJ5bva5KkmFUtp1JbX/P1Jv5f5KkaUJ
MD5:	0BC464484F2E40F96A67B5DDF142028B
SHA1:	A8152C8B92964F406DBB47F394240BCF237045F0
SHA-256:	A9354050408FA4FF12A9C8EAD2E788C4C5E440A4C492C7D2E599F736903FFBF1
SHA-512:	2271CAEFBB63ADB00F88D14FA825CCBC468D91290FD2F71652EB1F58B6ECB3FF0D15060F823877A2D9A696BA158429CA5977226B580EE87A25056962008DAB0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Preview:	2021/08/04-01:21:42.350 878 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-01:21:42.380 878 Recovering log #3.2021/08/04-01:21:42.399 878 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.oldg (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.245888622180551
Encrypted:	false
SSDEEP:	6:mgJ56+q2PWXp+N23iKKdKpIFUtp1JbXZmwP1JztVkwOWXp+N23iKKdKa/WLJ:FJ5bva5KkmFUtp1JbX/P1Jv5f5KkaUJ
MD5:	0BC464484F2E40F96A67B5DDF142028B
SHA1:	A8152C8B92964F406DBB47F394240BCF237045F0
SHA-256:	A9354050408FA4FF12A9C8EAD2E788C4C5E440A4C492C7D2E599F736903FFBF1
SHA-512:	2271CAEFBB63ADB00F88D14FA825CCBC468D91290FD2F71652EB1F58B6ECB3FF0D15060F823877A2D9A696BA158429CA5977226B580EE87A25056962008DAB0
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:42.350 878 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-01:21:42.380 878 Recovering log #3.2021/08/04-01:21:42.399 878 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):	5.344710236181029
Encrypted:	false
SSDEEP:	12:FtW2yva5KkkOrsFUtp1tWB/P1tW4dR5f5KkkOrzJ:F8a5Kk+gzkVf5Kkn
MD5:	ABC7CC4D18B757E028805BF550F12B35
SHA1:	00EE765F1FF28408411AD02927B787172327E09D
SHA-256:	4C10B8F37CF0CF3ED19A3EA406AE8BB8235EB7D5D25B58AAA55F7D5D987063FB
SHA-512:	5CC50617AB135E6B5A50D7D9CAB5AAB2C777094D501225F81F9418DA1CE99742D49DC725FCB781DE2EFD71555829F237332AD99D776EC4C49090898D305D396
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:59.322 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/04-01:21:59.323 1570 Recovering log #3.2021/08/04-01:21:59.324 1570 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
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.344710236181029
Encrypted:	false
SSDEEP:	12:FtW2yva5KkkOrsFUtp1tWB/P1tW4dR5f5KkkOrzJ:F8a5Kk+gzkVf5Kkn
MD5:	ABC7CC4D18B757E028805BF550F12B35
SHA1:	00EE765F1FF28408411AD02927B787172327E09D
SHA-256:	4C10B8F37CF0CF3ED19A3EA406AE8BB8235EB7D5D25B58AAA55F7D5D987063FB
SHA-512:	5CC50617AB135E6B5A50D7D9CAB5AAB2C777094D501225F81F9418DA1CE99742D49DC725FCB781DE2EFD71555829F237332AD99D776EC4C49090898D305D396
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:59.322 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/04-01:21:59.323 1570 Recovering log #3.2021/08/04-01:21:59.324 1570 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\TransportSecurityTM (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):	1038
Entropy (8bit):	5.5626922784812765

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurityTM (copy)	
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvtpA7wUU9RUenHQ:YI6UUhVseKUewqPeUer2UefPWwUyUenw
MD5:	5BDC24C37CDD072AEB129DC938EB6CAD
SHA1:	48E3C0D60B37CBDB7C902CDA068E56F5110181E3
SHA-256:	802476CC04D05A4361C9CC9AD07EC2C7AF4CDB035194CC5D1203E0CAFCBF371F
SHA-512:	5D4869DFFE421D3DF2D0892604E0853BF8A9D9D9B9A73978F77A60BF51B677841313354EF832DA6F24F0B8C40FBC68FCDE791E2BA95A827B275AB566D0DA58A
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":1659601307.002176,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628065307.00218},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:yw:n
MD5:	47FC67CE4F874D2316C70BD6764E931A
SHA1:	44464E7A2906CC32073B763A22F857DCBCDA1126
SHA-256:	D19656EABEEF120ECF01B7817342A301FDECB7CA88F4037AE7C874E69547990F
SHA-512:	7C91C714EFA1446AFF191A00FB1AF04501528031977580BA860CAA4A130DFF138511F4A907B24E9D25BCE7555A27C30FAC35EF3B0CD693923731A69A0ED4877A
Malicious:	false
Reputation:	low
Preview:	.....c..+...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ce583fbf-fdef-483b-9b23-bf1a1df97648.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Preview:	MANIFEST-000004.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.5524283659218
Encrypted:	false
SSDEEP:	3:tUK6NXUhtRXGNAgZmwv3INXUm1Shs0V8sINXUmois0WGv:mghtRWNJZmwP1yShs0Vv1ws0tv
MD5:	E6293BCACBB8633CE339A413131D36C3
SHA1:	7758BF40316E78DD15E326E208E62CC72D537E13
SHA-256:	0F18E66E3497CE9EDBDF41005F3143A592E516B8F56CC65DC877E5C81634B2A6
SHA-512:	8D8F9E15425BA6864C5435A182F855973BDE0CE8BEF889013093824F05324F24CD71223135533940CE900A662C3BD9469332A36AE5E81A278D0D99B026062B02
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:56.709 142c Recovering log #3.2021/08/04-01:21:56.777 142c Delete type=0 #3.2021/08/04-01:21:56.778 142c 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):	4.5524283659218
Encrypted:	false
SSDEEP:	3:tUK6NXUhtRXGNAgZmwv3INXUm1Shs0V8sINXUmois0WGv:mghtRWNJZmwP1yShs0Vv1ws0tv
MD5:	E6293BCACBB8633CE339A413131D36C3
SHA1:	7758BF40316E78DD15E326E208E62CC72D537E13
SHA-256:	0F18E66E3497CE9EDBDF41005F3143A592E516B8F56CC65DC877E5C81634B2A6
SHA-512:	8D8F9E15425BA6864C5435A182F855973BDE0CE8BEF889013093824F05324F24CD71223135533940CE900A662C3BD9469332A36AE5E81A278D0D99B026062B02
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:56.709 142c Recovering log #3.2021/08/04-01:21:56.777 142c Delete type=0 #3.2021/08/04-01:21:56.778 142c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V........leveldb.BytewiseComparator...#...........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ebfbf43a-3189-4129-9dd0-1507bb8d5081.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):	5765
Entropy (8bit):	5.188907843272366
Encrypted:	false
SSDEEP:	96:nhCmTG9rvyJxQScKIr8ok0JCKL88kvS1MbOTQVuwn:nhCB9LyJKSc9L4Kdka8
MD5:	215E8345DA80D7DB30613B1CDFB15E79
SHA1:	9029E1E844317965EFF75E4B21747E11BF069080
SHA-256:	0D3F7B8A55F2A8AA0DE764F52D0BABAD64F1A4240DAAAED13977B715307E4689
SHA-512:	2EC7B5004FFF620DD67D4C545CDAE6EAA08C2CCEE2EE63F30417C635FA53B3048D317B33F0F638ED1B0C16AFC05F40454BF3D78A0E3556CE178D06CC37331E 7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272538902616079","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.2126863721035885
Encrypted:	false
SSDEEP:	6:mgRKVq2PWXp+N23iKKdKfrzAdIFUtp1pgZmwP1TZ0IkwOWXp+N23iKKdKfrzILJ:Fsva5Kk9FUtp1m/P1T95f5Kk2J
MD5:	C8B3A57892D32BC42613C82AFEA7CD4E
SHA1:	324747CC46D7A2604BB06B3524934801E91D4B98
SHA-256:	466F079B57804731C1EF2EAFC6969B90312ED0FF100B8F6A1794BCB8EC2A95D3
SHA-512:	6959A1531F0A75D7C8DF65064C37DC0176F917CD29C875046E2F78B7C583CB51F8857F09CD4D36E2DFBF16EE72B9E1406E8595F5A6277D60303C7CE61C956C9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.164 14c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/04-01:21:58.165 14c4 Recovering log #3.2021/08/04-01:21:58.166 14c4 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.2126863721035885
Encrypted:	false
SSDEEP:	6:mgRKVq2PWXp+N23iKKdKfrzAdIFUtp1pgZmwP1TZ0IkwOWXp+N23iKKdKfrzILJ:Fsva5Kk9FUtp1m/P1T95f5Kk2J
MD5:	C8B3A57892D32BC42613C82AFEA7CD4E
SHA1:	324747CC46D7A2604BB06B3524934801E91D4B98
SHA-256:	466F079B57804731C1EF2EAFC6969B90312ED0FF100B8F6A1794BCB8EC2A95D3
SHA-512:	6959A1531F0A75D7C8DF65064C37DC0176F917CD29C875046E2F78B7C583CB51F8857F09CD4D36E2DFBF16EE72B9E1406E8595F5A6277D60303C7CE61C956C9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:21:58.164 14c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/04-01:21:58.165 14c4 Recovering log #3.2021/08/04-01:21:58.166 14c4 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
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):	165870
Entropy (8bit):	6.04960571208538
Encrypted:	false
SSDEEP:	3072:mGaYTJQE+mugy9+QV1T7IRwdfLSNP4FcbXafIB0u1GOJmA3iuRL:LxaV+QfT7GSmhmaqfIlUOoSiuRL
MD5:	C27022DFBA4177B9DC3A5DC4F0A749E5
SHA1:	22D7A17DF2E36569D5728884BFD61001F2EBCD54
SHA-256:	61B3C698B8E60CE8B561EE13C5F3B645AF845E9C08ED31B4E364697D2D815ED9
SHA-512:	85700E61496E9D2FEFE96788ED67E8FB3C999FAF133D03143C48970EE8B84E2FB8E865AB370D494ECA56F1C89D5830C560813BDC053247A3843CC69B11D49172
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":1.628065305353572e+12,"network":1.628032906e+12,"ticks":7042783713.0,"uncertainty":4539989.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016335422"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local Statep (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):	174337
Entropy (8bit):	6.079378767676914
Encrypted:	false
SSDEEP:	3072:Tl7GaYTJQE+mugy9+QV1T7IRwdfLSNP4FcbXafIB0u1GOJmA3iuRL:ZaxaV+QfT7GSmhmaqfIlUOoSiuRL
MD5:	4B9F0E01D10B0CE283E21DF5C9674C2B
SHA1:	F00A407E7910DCE42628B5C37C69F5A939F3617A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local Statep (copy)	
SHA-256:	5ACFD754080E972AA7DE0051359AE27D9526F556F4940139285BE5500D09AA2E
SHA-512:	AEE6C8A041816F9BADC1F9A1D86DCF4DC71A1FF9E47A664DA7C6962DEEEC18BFE845D180E0570F12DB7121E6B9C628AA5B07D02FD0AF88E79DB6C4C3B6205 06A
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":1.628065305353572e+12,"network":1.628032906e+12,"ticks":7042783713.0,"uncertainty":4539989.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016335422"},"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
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7493079716874647
Encrypted:	false
SSDEEP:	384:RPRumYbdgTw+VTV65Nmrzv6y3RqgtHIRGtkrPM+QxBkU03r/GmzHNf8eKCZOkIKy:laeZRKok5AenAiocvjGaKACKJs
MD5:	A68BE2558FE9EAE03AD7C42AB626F71B
SHA1:	098BEBD46DE77FD965E4DA3E5D00F75C695ED70A
SHA-256:	1DD4752E64463AEDFF0117928B34E88EA04635FE2B78D389B43B2000204FEFE0
SHA-512:	B4DEE9084BDB556893FBEDD46ACF864BB98244842B8F44BB6011C8EEB08ED4A0B84329406491C1953E20361597605931935 67AF716C434E598BD6BAB012BD27E
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.

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 01:21:46.472148895 CEST	192.168.2.3	8.8.8.8	0xef53	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.473931074 CEST	192.168.2.3	8.8.8.8	0x25c6	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.477180004 CEST	192.168.2.3	8.8.8.8	0x56f7	Standard query (0)	securecloud-oauth.herokuapp.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:47.225625038 CEST	192.168.2.3	8.8.8.8	0x66c2	Standard query (0)	outlookcloud.live	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 4, 2021 01:21:57.420178890 CEST	192.168.2.3	8.8.8.8	0xce5c	Standard query (0)	clients2.google usercontent.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 01:21:46.509556055 CEST	8.8.8.8	192.168.2.3	0x25c6	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.513797045 CEST	8.8.8.8	192.168.2.3	0x56f7	No error (0)	securecloud-oauth.herokuapp.com		3.223.221.167	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.513797045 CEST	8.8.8.8	192.168.2.3	0x56f7	No error (0)	securecloud-oauth.herokuapp.com		52.5.119.46	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.513797045 CEST	8.8.8.8	192.168.2.3	0x56f7	No error (0)	securecloud-oauth.herokuapp.com		54.156.27.150	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.513797045 CEST	8.8.8.8	192.168.2.3	0x56f7	No error (0)	securecloud-oauth.herokuapp.com		52.0.12.63	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.513797045 CEST	8.8.8.8	192.168.2.3	0x56f7	No error (0)	securecloud-oauth.herokuapp.com		3.213.42.86	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.513797045 CEST	8.8.8.8	192.168.2.3	0x56f7	No error (0)	securecloud-oauth.herokuapp.com		23.22.180.24	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.513797045 CEST	8.8.8.8	192.168.2.3	0x56f7	No error (0)	securecloud-oauth.herokuapp.com		3.223.104.152	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.513797045 CEST	8.8.8.8	192.168.2.3	0x56f7	No error (0)	securecloud-oauth.herokuapp.com		34.237.27.35	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:46.515702009 CEST	8.8.8.8	192.168.2.3	0xef53	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 01:21:46.515702009 CEST	8.8.8.8	192.168.2.3	0xef53	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:47.426850080 CEST	8.8.8.8	192.168.2.3	0x66c2	No error (0)	outlookcloud.live		63.250.40.230	A (IP address)	IN (0x0001)
Aug 4, 2021 01:21:57.463435888 CEST	8.8.8.8	192.168.2.3	0xce5c	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 01:21:57.463435888 CEST	8.8.8.8	192.168.2.3	0xce5c	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 4, 2021 01:21:46.787159920 CEST	3.223.221.167	443	192.168.2.3	49717	CN=*.herokuapp.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat May 29 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Jun 28 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Aug 4, 2021 01:21:46.788892984 CEST	3.223.221.167	443	192.168.2.3	49718	CN=*.herokuapp.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat May 29 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Jun 28 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 1956 Parent PID: 2128

General

Start time:	01:21:41
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 'https://securecloud-oauth.herokuapp.com/#abuse@herokuapp.com'
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: 5872 Parent PID: 1956

General

Start time:	01:21:43
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=1556,12548367778192904546,1557536481882000717,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1740 /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

Disassembly