ID: 458991
Cookbook: browseurl.jbs
Time: 01:14:52
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report https://securecloud-oauth.herokuapp.com 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 4
Thumbnails 4
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 5
Domains 5
URLs 6
Domains and IPs 6
Contacted Domains 6
URLs from Memory and Binaries 6
Contacted IPs 6
Public 6
Private 6
General Information 6
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 7
IPs 7
Domains 7
ASN 7
JA3 Fingerprints 7
Dropped Files 7
Created / dropped Files 7
Static File Info 37
No static file info 37
Network Behavior 37
Network Port Distribution 37
TCP Packets 38
UDP Packets 38
DNS Queries 38
DNS Answers 38
HTTPS Packets 38
Code Manipulations 39
Statistics 40
Behavior 40
System Behavior 40
Analysis Process: chrome.exe PID: 3484 Parent PID: 4864 40
General 40
File Activities 40
Registry Activities 40
Analysis Process: chrome.exe PID: 5608 Parent PID: 3484 40
General 40
File Activities 40
Disassembly 40

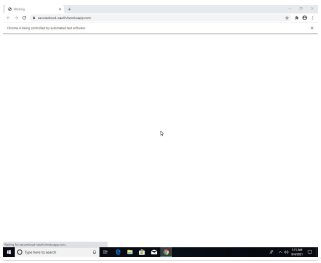
Windows Analysis Report https://securecloud-oauth.her…

Overview

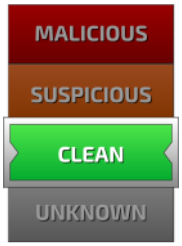
General Information

Sample URL:	http://https://securecloud-oauth.herokuapp.com
Analysis ID:	458991
Infos:	

Most interesting Screenshot:



Detection

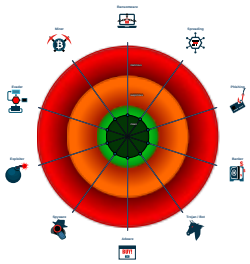


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3484 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://securecloud-oauth.herokuapp.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5608 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,3241909227358404563,10164897485226726443,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1716 /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

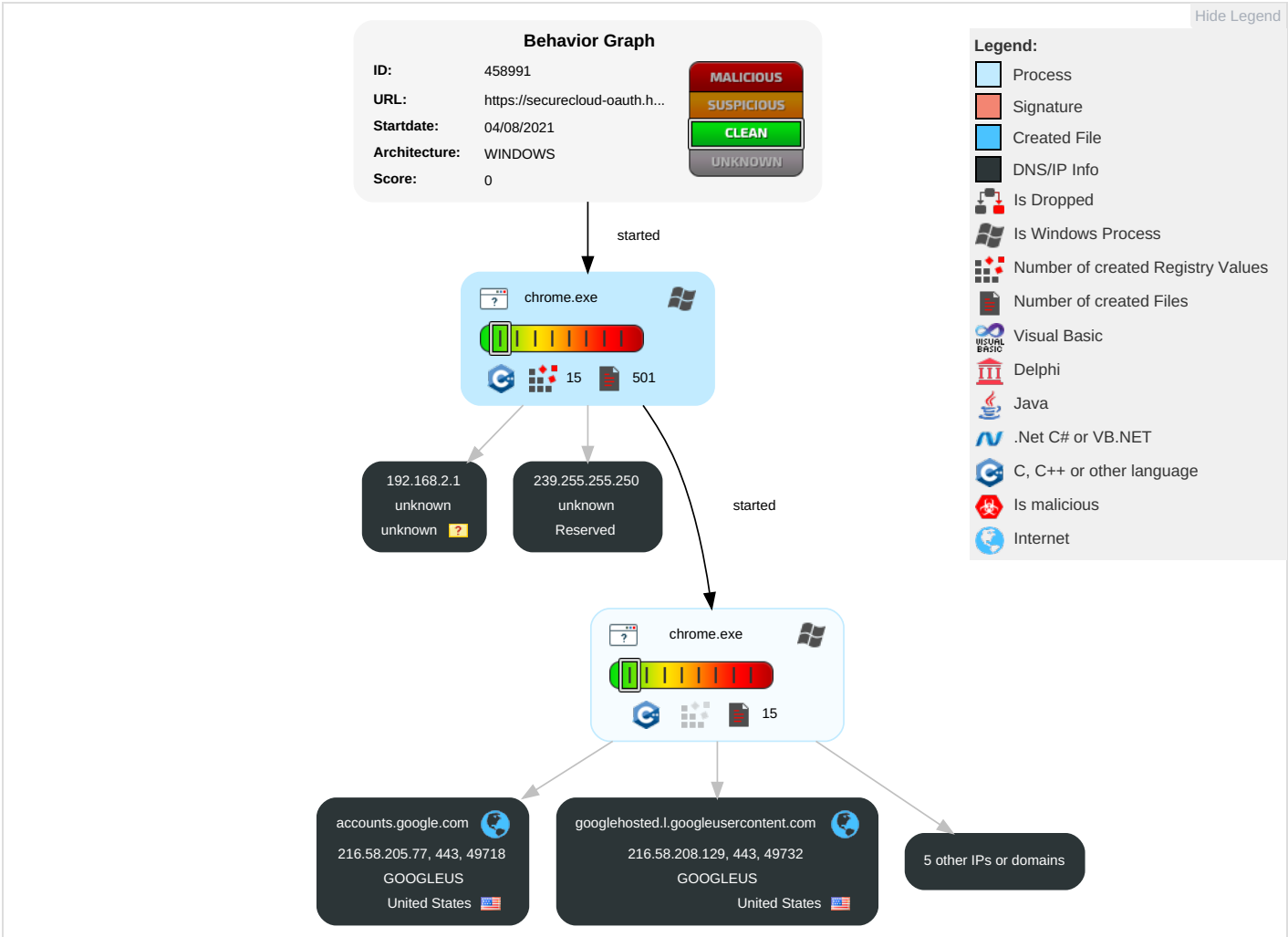
Click to jump to signature section

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

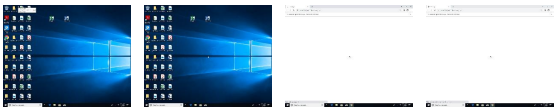
Behavior Graph

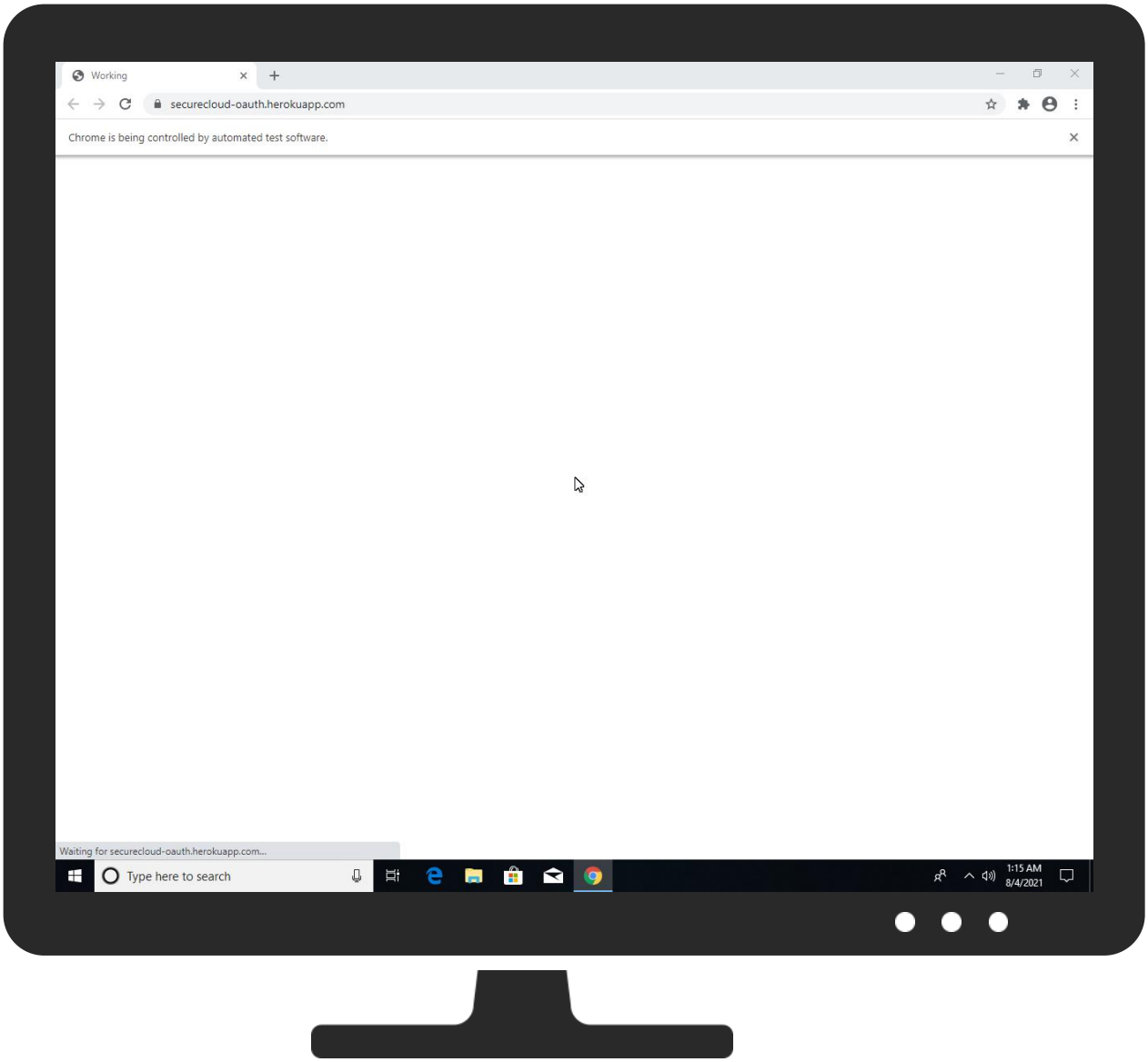


Screenshots

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	0%	Virustotal		Browse
http://https://securecloud-oauth.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

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://securecloud-oauth.herokuapp.com/	0%	Virustotal		Browse
http://https://securecloud-oauth.herokuapp.com/	0%	Avira URL Cloud	safe	
http://https://securecloud-oauth.herokuapp.com/Working	0%	Avira URL Cloud	safe	
http://https://securecloud-oauth.herokuapp.com/Working/	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	
http://https://securecloud-oauth.herokuapp.com/2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
securecloud-oauth.herokuapp.com	3.232.85.60	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	216.58.205.77	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
3.232.85.60	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:	458991
Start date:	04.08.2021
Start time:	01:14:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://securecloud-oauth.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:	11
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@33/245@4/7
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\1da99810-427a-433c-a1b5-d3dc7283f974.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7489538170141197
Encrypted:	false
SSDEEP:	384:nPRumYbdEwf65Nmrzv6y3RqgtHIRGtkrPM+QxBkU03r/GmzQf8eKCZOkIKNH1OPA:LeZRKoJ5AenAiocvjGaKACKJz
MD5:	402A499FC2C8AAD06C9827650C0838A3
SHA1:	9D0A487664DE108EC93700C68756A5E574025579
SHA-256:	E20B05DDD4BF4B8F12548DCA269D9086C1EE5D86433348AF22AB7BD28B5D033C
SHA-512:	4CD23341C39ABF0B219A827623D1E50F49B829A274759CB7B265F2D59E0AC69A85C4B5455FDBF62ABA63791147305F568B38B4EBAECD4A634A1C1ACD88A5E3F5
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\24ca3ff7-ab57-4b62-bd90-ee351162497e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174336
Entropy (8bit):	6.079345761837566
Encrypted:	false
SSDEEP:	3072:38PGaYTJQE+mugy9+QV1T7IRwdfLSNPWFcbXafIB0u1GOJmA3iuRL:M+xaV+QfT7GSmh8aqfIlUOoSiuRL
MD5:	034D15902678D021BB2FC1F1453C8C8D
SHA1:	6D9D2AD5E39A1ADF29B6249B80B3C511E221C16B
SHA-256:	691F365874741976036 60ACB1B505C1D86360C73576212CDCA7EA2E10FDFC62C
SHA-512:	EA41F1E62785E84FD5E36EC30E386F3B3AB5143EE6C6AD8FD1546B9E7811A84F4192C8BD0FCEA79E4D0EBE7C48770C0DF8403881A4AA2CE1B8586D94599B937
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":1.628064943269636e+12,"network":1.628032544e+12,"ticks":5759005818.0,"uncertainty":4684117.0}},"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\53501311-fd7c-47ef-b7f9-5cda8dd217ac.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):	174336
Entropy (8bit):	6.079345199189187
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\53501311-fd7c-47ef-b7f9-5cda8dd217ac.tmp	
SSDEEP:	3072:31/GaYTJQE+mugy9+QV1T7IRwdfLSNPWFcbXafIB0u1GOJmA3iuRL:FOxaV+QfT7GSmh8aqfIlUOoSiuRL
MD5:	4D85AC6BC3F81ABA9AAC70F614FFDD16
SHA1:	677EE75482F0911DCDE1F3660244745472FBEDA1
SHA-256:	883C865883D686C0BDAE6AD6BECAB1E9CD83D7A3B48E22EF037E1D7629D07FED
SHA-512:	07ECB95F70B043BDE86AFD5182C5CCDB7814BCBAEA8C64589DFB412FA18D36D75CE0189C72862ABF147CA1CE9174136E732FCEFFFABD3C0922B6C700BA3B6B54
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":1.628064943269636e+12,"network":1.628032544e+12,"ticks":5759005818.0,"uncertainty":4684117.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+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:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\05934ea8-9a50-4354-a97d-d5d6b5affd19.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):	24054
Entropy (8bit):	5.533837760712972
Encrypted:	false
SSDEEP:	384:y/ftWLlahXt1kXqKf/pUZNCgVLH2HfDwrU7HG9HGCnT8lMF4p:dLlGt1kXqKf/pUZNCgVLH2HfUrULGhG/
MD5:	735E070E2EC120DA9B19C96A5BA6031A
SHA1:	6F36D0441FCAF9263E84D664905A37FB45A138CF
SHA-256:	718587ED5959DE0D4A8CCCC95532FC266BC4903DECE2850460EF117E0955F8BD
SHA-512:	8F27C8E0F22FD8BB7809834F029DE5BC24A9D8D523AF4994EAFE6698BFA9CB80E3B02CEEAB350540E5EA9D4C5E70CEF92E8F65BCD86B39133EE6600D8EE4BCF
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":"13272538540178986","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\10c743ab-f83c-4477-9234-3349a23c7c73.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):	5.536100595222747
Encrypted:	false
SSDEEP:	384:y/ftvLlahXt1kXqKf/pUZNCgVLH2HfDwrU9HGlnTqlsF4A:KLlGt1kXqKf/pUZNCgVLH2HfUrUhGlnz
MD5:	F170489B7BF225B96D7F5A4AD08A95AE
SHA1:	DFC07400A5F77DD44326E029C16EDE87274A5C15
SHA-256:	5E1E341998CD45B3F0859AD3ABF95FE2278D86E98989A8D7CC7C4888AF38577A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\10c743ab-f83c-4477-9234-3349a23c7c73.tmp	
SHA-512:	55D4181C7F667BC9248C3CD4D03B58FCF75CD5C436AD5671E1E69EF1866358E5EC4DCA9EAA6A43DB3C08674EFD6849737C4205BB633356D6E8A65C053F8A2C3
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":"13272538540178986","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\17a13fac-c95d-43c7-b108-5af6639f4d0f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.566210022658869
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvtP7wU5RUenHQ:YI6UUhVseKUewqPeUer2UefxwUfUenw
MD5:	43098F2E2FDAE70C41ED593A8A5199B0
SHA1:	147DEFD8D0B5FBCFAE3294D10954B7A7019A26CB
SHA-256:	ACE1E54E64A6F8EFA77593EB1CE7205CBA12F12DFDF932B2BA9100E076FD6734
SHA-512:	178C362528C1B7FDEDCAB5A0231012C1A0B083BD9C3F811B4DE1204568A36F03C69785B4C44DBC0C8983616516D1E89F09F2DB5C27BB802AF39A8A0C347CADE
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":1659600945.004806,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628064945.004809},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5abce158-d8fc-4204-aeb9-4d3cf136208c.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):	24056
Entropy (8bit):	5.533918680747312
Encrypted:	false
SSDEEP:	384:y/ftvLlahXt1kXqKf/pUZNCgVLH2HfDwrU7HG9HGxnTqlCF4A:KLlGt1kXqKf/pUZNCgVLH2HfUrULGhGz
MD5:	789E3946C3F97E4B52585E10578E106F
SHA1:	AE680D0EF79B455FF14D020F8B6A96BAD920F281
SHA-256:	7D05B079ED3F0C96383113D8B4AFED11D1AC0132A6643E1909F7671BB3695B28
SHA-512:	7132DC16D263C63780FAA3A3BC71AB2D8DD488F66B8FE1BA39C5D49300070AF9CEAA3CD6C4EC5A0D4EC608F86E097C689917CA6C103AF9CC4EB048FE872A7D8
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":"13272538540178986","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\8841f5d6-8aa9-4c3b-ae9a-881898a8c816.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):	5754
Entropy (8bit):	5.197500512295057
Encrypted:	false
SSDEEP:	96:nbCd359jUB/fcKllok0JCKL8fk01YbOTQVuwn:nbCr9jgHcC4KSk0k
MD5:	B9496BF5B8A662309779DCF4A10E57E4
SHA1:	C8F53D3AA074C96DF7E6E0B7FE016E2BBFCC8259

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8841f5d6-8aa9-4c3b-ae9a-881898a8c816.tmp	
SHA-256:	87E42905BD6FB8B4F8712EE0C1D024F3AB95DC9A769FFEDCE3727E2B67235863
SHA-512:	B9B4D25A1DFEFCA5CD18482BBF34B075EEBFEEDA314DDCA08886D9E0D8AEAA40BC00EDF3E9EC043D68601EAD5B98A81EF0F336CFD5AC698C17A07D240F9F C097
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272538540475030","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\95080399-0038-491a-a0aa-1a3fd3867c9c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9ef4ee65-a6d7-46b3-b6c9-037914c7d43f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.216013121483808
Encrypted:	false
SSDEEP:	6:mIzSVq2PWXp+N23iKKdK9RXXTZIFUtpvOgZmwPvOIkwOWXp+N23iKKdK9RXX5LJ:7SVva5Kk7XT2FUtp2g/P2I5f5Kk7XVJ
MD5:	4E2BD4EC8C7B54478A734466E5FE4BCD
SHA1:	A42EF2952E27EDE2AF2D7AB80DF939CE103EB7A2
SHA-256:	13FA357D4BB4471D9310E1F8C66E4E8C666D28FD31710B2CAD0C825963A4836C
SHA-512:	8A2F0480324652D4D53D9793A76D7E57164FE2C70596241C7293D099D4A9FE6859D7D60E7B5B070C5BEB51BBC1A0D56D0BFD9DA863532B4802DA13D38A15FF3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2021/08/04-01:15:47.746 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-01:15:47.755 1200 Recovering log #3.2021/08/04-01:15:47.755 1200 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.216013121483808
Encrypted:	false
SSDEEP:	6:mIzSVq2PWXp+N23iKKdK9RXXTZIFUtpvOgZmwPvOIkwOWXp+N23iKKdK9RXX5LJ:7SVva5Kk7XT2FUtp2g/P2I5f5Kk7XVJ
MD5:	4E2BD4EC8C7B54478A734466E5FE4BCD
SHA1:	A42EF2952E27EDE2AF2D7AB80DF939CE103EB7A2
SHA-256:	13FA357D4BB4471D9310E1F8C66E4E8C666D28FD31710B2CAD0C825963A4836C
SHA-512:	8A2F0480324652D4D53D9793A76D7E57164FE2C70596241C7293D099D4A9FE6859D7D60E7B5B070C5BEB51BBC1A0D56D0BFD9DA863532B4802DA13D38A15FF3
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.746 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-01:15:47.755 1200 Recovering log #3.2021/08/04-01:15:47.755 1200 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):	5.185278940154012
Encrypted:	false
SSDEEP:	6:mIYxVq2PWXp+N23iKKdKyDZIFUtpv1SgZmwPv1SIkwOWXp+N23iKKdKyJLJ:cVva5Kk02FUtpgg/PgI5f5KkWJ
MD5:	19E4076CA543D968875378397A91862C
SHA1:	0290EF82003DDDCBDCD6C81DE8D9D080CE33AE50
SHA-256:	98F88C5438DEB7064FCCE78757E7B91D8E8A457A2CC2082E54FFF5CCF7EE9CC1
SHA-512:	1D9DB1A3DAFE78B248B9BA1C2228804E19713D81652955221C9E2771AEED3520C6C90FAA873A093D7C4A31C9A35C352586C3ED502E727848E09FCA21E88DC4
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.739 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-01:15:47.740 1200 Recovering log #3.2021/08/04-01:15:47.740 1200 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.oldit (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.185278940154012
Encrypted:	false
SSDEEP:	6:mIYxVq2PWXp+N23iKKdKyDZIFUtpv1SgZmwPv1SIkwOWXp+N23iKKdKyJLJ:cVva5Kk02FUtpgg/PgI5f5KkWJ
MD5:	19E4076CA543D968875378397A91862C
SHA1:	0290EF82003DDDCBDCD6C81DE8D9D080CE33AE50
SHA-256:	98F88C5438DEB7064FCCE78757E7B91D8E8A457A2CC2082E54FFF5CCF7EE9CC1
SHA-512:	1D9DB1A3DAFE78B248B9BA1C2228804E19713D81652955221C9E2771AEED3520C6C90FAA873A093D7C4A31C9A35C352586C3ED502E727848E09FCA21E88DC4
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.739 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-01:15:47.740 1200 Recovering log #3.2021/08/04-01:15:47.740 1200 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC761F
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):	0.9680104828397914
Encrypted:	false
SSDEEP:	24:JcLgAZOZD/MfqqLbJLbXaFpEO5bNmISHn06UwI8:J8NOZlqq5LLOpEO5J/Kn7Un8
MD5:	9DEDA3580F77078F4F9E0CAD63A84E63
SHA1:	7D51127257BDCAE2F1341B292A026B52C95BD36C
SHA-256:	4CA4A05F977CF3C6FB53E6872CF5E4C96998F3141033643295A9641644A3788B
SHA-512:	19649AB3708607C3B737C4C1E62224703AC7B8407E4F3F4F57E13A9A0DB85A91E955DEA0406BFD73A361F1A423DE2295B88CEFFA8FF2369F47438730FDFAB87A
Malicious:	false
Reputation:	low
Preview:	.....T.J-.....

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):	981
Entropy (8bit):	3.3137807819980645
Encrypted:	false
SSDEEP:	12:3olydJheJaGPlpxlpN8klyT4ZA/tl/U0aG3CLU+5ByZA/Zt5lptlpl:34SAlrlADZlM0aO4U+5EZyPlLIL
MD5:	442E29B4B063C3B41726E61DC3381653
SHA1:	24DEF8E1CA279CF3DCCFE54F50AB515C0CF0D08A
SHA-256:	DAB96FD9E32D49FC49896B969E242D62D990DF1490BFF9BAAB0690771AEC81C5
SHA-512:	8B2EF558041A3158D05B1F7A8172D15983FB23A008FD1004DA9672597F01F68331E8233261D5C7164227C5FDA1C850F8F3668C790760A246756E50082DE57018
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...909f5e03_d8eb_447e_b077_166c34f598ed.....\.W.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.209888987493457
Encrypted:	false
SSDEEP:	6:mIO79+q2PWXp+N23iKKdK8aPrqIFUtpvOeWJZmwPvO219VkwOWXp+N23iKKdK8a4:Q4va5KkL3FUtpbWJ/PpD5f5KkQJ
MD5:	5CE04E22B51B942EEF8055EB82E7C6F5
SHA1:	25B4297AC87E553FB22C8A8381B7A67E525B1C07
SHA-256:	CC1F3092B2B01679FF664106ACFC6F8BDD0CF18E8D1784EDBBD56381DF088567
SHA-512:	E46CFFBEF21DBA559867A57C84EEF586E1FD239F7F7FFE356A121E310F4A58B4A6D969491A710C9F35BBC59B500A6E00B760787105E02CE3D709731C917CE8B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.480 1368 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-01:15:40.482 1368 Recovering log #3.2021/08/04-01:15:40.483 1368 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):	5.209888987493457
Encrypted:	false
SSDEEP:	6:mIO79+q2PWXp+N23iKKdK8aPrqIFUtpvOeWJZmwPvO219VkwOWXp+N23iKKdK8a4:Q4va5KkL3FUtpbWJ/PpD5f5KkQJ
MD5:	5CE04E22B51B942EEF8055EB82E7C6F5
SHA1:	25B4297AC87E553FB22C8A8381B7A67E525B1C07
SHA-256:	CC1F3092B2B01679FF664106ACFC6F8BDD0CF18E8D1784EDBBD56381DF088567
SHA-512:	E46CFFBEF21DBA559867A57C84EEF586E1FD239F7F7FFE356A121E310F4A58B4A6D969491A710C9F35BBC59B500A6E00B760787105E02CE3D709731C917CE8B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.480 1368 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-01:15:40.482 1368 Recovering log #3.2021/08/04-01:15:40.483 1368 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4C
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5.. ....f.5................f.5................f.5................f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.244702311626284
Encrypted:	false
SSDEEP:	6:mIMjgq2PWXp+N23iKKdK8NIFUtpvMcZZmwPvMpkwOWXp+N23iKKdK8+eLJ:UMva5KkpFUtpEw/PEp5f5KkqJ
MD5:	909724DF1135E368741A8EF16BBCEC9A
SHA1:	022600A79177F55BBCE08085665EDB055A4D1970
SHA-256:	B734A3DAC2F17017FAF41645794FE500E9D13C1938F264434C6ED9D5C02856F3
SHA-512:	216C453609886EF7AAD9669F385170F8D7BE7A498E476D509313E91EB5C6F54184D638BDF74ECE1AC4746E06D0CBC26CED3E58464EDD65D9CCBC431B06FC646
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:42.617 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-01:15:42.618 15b0 Recovering log #3.2021/08/04-01:15:42.619 15b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.244702311626284
Encrypted:	false
SSDEEP:	6:mIMjgq2PWXp+N23iKKdK8NIFUtpvMcZZmwPvMpkwOWXp+N23iKKdK8+eLJ:UMva5KkpFUtpEw/PEp5f5KkqJ
MD5:	909724DF1135E368741A8EF16BBCEC9A
SHA1:	022600A79177F55BBCE08085665EDB055A4D1970
SHA-256:	B734A3DAC2F17017FAF41645794FE500E9D13C1938F264434C6ED9D5C02856F3
SHA-512:	216C453609886EF7AAD9669F385170F8D7BE7A498E476D509313E91EB5C6F54184D638BDF74ECE1AC4746E06D0CBC26CED3E58464EDD65D9CCBC431B06FC646
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:42.617 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-01:15:42.618 15b0 Recovering log #3.2021/08/04-01:15:42.619 15b0 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	5.246640685597809
Encrypted:	false
SSDEEP:	6:mIzXKVq2PWXp+N23iKKdK25+Xqx8chI+IFUtpvDgZmwPvMIkwOWXp+N23iKKdK2L:jKVva5KkTXfchI3FUtpLg/PkI5f5KkTM
MD5:	6CF2681939260AFEBC8D73FE4C8D5BE2
SHA1:	03B73A9603426CC3BE4643F6B72CC0E4E22CF182
SHA-256:	8BA0F54D37CFEDFF4D273F4F46CDA85AD17041F31BDF26D4222756E9F4436561
SHA-512:	FF252C35E7BA91A36F8CE309FE8E50368DD35F4594E9028BF35F04BEB86DC14A83D62330B01BDA1F43D287254F0820F424E7C2EDBD7156BA145A0992B4F5681
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.683 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-01:15:47.707 1200 Recovering log #3.2021/08/04-01:15:47.708 1200 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.246640685597809
Encrypted:	false
SSDEEP:	6:mIzXKVq2PWXp+N23iKKdK25+Xqx8chI+IFUtpvDgZmwPvMIkwOWXp+N23iKKdK2L:jKVva5KkTXfchI3FUtpLg/PkI5f5KkTM
MD5:	6CF2681939260AFEBC8D73FE4C8D5BE2
SHA1:	03B73A9603426CC3BE4643F6B72CC0E4E22CF182
SHA-256:	8BA0F54D37CFEDFF4D273F4F46CDA85AD17041F31BDF26D4222756E9F4436561
SHA-512:	FF252C35E7BA91A36F8CE309FE8E50368DD35F4594E9028BF35F04BEB86DC14A83D62330B01BDA1F43D287254F0820F424E7C2EDBD7156BA145A0992B4F5681
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.683 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-01:15:47.707 1200 Recovering log #3.2021/08/04-01:15:47.708 1200 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):	5.22377547352238
Encrypted:	false
SSDEEP:	6:mIYYVq2PWXp+N23iKKdK25+XuoIFUtpv/gZmwPvfYIkwOWXp+N23iKKdK25+Xuxo:zVva5KkTXYFUtpng/PII5f5KkTXHJ
MD5:	5FB98B064F7E5CC614AB328F92D8B6DB
SHA1:	DEBFC266797101ADE9154142587428A8BA78ED97
SHA-256:	F393708BFAC6AC4F536D62F1ABE0475535D2F2CA501326FEEA8144177067D958
SHA-512:	CED87ECB2034B2D7C29A32A924C7F8414E449DA6DFB3712C3555F89844F0E0CC8754E27EA38102C4AA65C910823C0A73B6BF9E1190BB72E18A4D7C1CAD3CFD5
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.673 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-01:15:47.677 1200 Recovering log #3.2021/08/04-01:15:47.678 1200 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Size (bytes):	358
Entropy (8bit):	5.22377547352238
Encrypted:	false
SSDEEP:	6:mIYYVq2PWXp+N23iKKdK25+XuoIFUtpv/gZmwPvfYIkwOWXp+N23iKKdK25+Xuxo:zVva5KkTXYFUtpng/PII5f5KkTXHJ
MD5:	5FB98B064F7E5CC614AB328F92D8B6DB
SHA1:	DEBFC266797101ADE9154142587428A8BA78ED97
SHA-256:	F393708BFAC6AC4F536D62F1ABE0475535D2F2CA501326FEEA8144177067D958
SHA-512:	CED87ECB2034B2D7C29A32A924C7F8414E449DA6DFB3712C3555F89844F0E0CC8754E27EA38102C4AA65C910823C0A73B6BF9E1190BB72E18A4D7C1CAD3CFD5
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.673 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-01:15:47.677 1200 Recovering log #3.2021/08/04-01:15:47.678 1200 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):	5.241730936982529
Encrypted:	false
SSDEEP:	6:mI94Vq2PWXp+N23iKKdKWT5g1IdqIFUtpv96gZmwPv9jxIkwOWXp+N23iKKdKWTk:F4Vva5Kkg5gSRFUtpV6g/PVjxI5f5Kkn
MD5:	CDC787BDBCEDB74174161E7A35DFE28B
SHA1:	BF7B150E3930E1F331F79ACD38C616AE9C277A46
SHA-256:	BC07ECF5644562B2615FAD946FB4A093A3AB3058B42623BB7AAAC4FAA7AD7451
SHA-512:	74B9F09E93403296C4F650D3B825440196940B21B1E840C9D5D7E0D39C87C20F63E7D42C9413620E3AFD7C8B8EB1927C5C4A7385E3B806EBB7FF76D038386B4E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.661 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-01:15:47.663 1200 Recovering log #3.2021/08/04-01:15:47.664 1200 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.241730936982529
Encrypted:	false
SSDEEP:	6:mI94Vq2PWXp+N23iKKdKWT5g1IdqIFUtpv96gZmwPv9jxIkwOWXp+N23iKKdKWTk:F4Vva5Kkg5gSRFUtpV6g/PVjxI5f5Kkn
MD5:	CDC787BDBCEDB74174161E7A35DFE28B
SHA1:	BF7B150E3930E1F331F79ACD38C616AE9C277A46
SHA-256:	BC07ECF5644562B2615FAD946FB4A093A3AB3058B42623BB7AAAC4FAA7AD7451
SHA-512:	74B9F09E93403296C4F650D3B825440196940B21B1E840C9D5D7E0D39C87C20F63E7D42C9413620E3AFD7C8B8EB1927C5C4A7385E3B806EBB7FF76D038386B4E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.661 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-01:15:47.663 1200 Recovering log #3.2021/08/04-01:15:47.664 1200 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):	0.10176964463293874
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvAl/fxAQ1E2PnqoOo/lCxthiZnAGCxC+/erKsKxAQ1E7:TL+A/SfxA/2PHNuQ1AGI/LxA/7
MD5:	B86C2FDE68054B358709D3F69783F320
SHA1:	C65AD5581B2438204EC564AE0319823FC67CA0AA
SHA-256:	6D86D921C28E7E9D8686BA1FA96F056DCC974E573F47EDF5539FE00F0410FEC5
SHA-512:	E39E0ADE2DC6573B719FA4A726B89AF17C6EF3FD2F4CA353E2B6E0810A89A1A3D664637797F388406F2A256E81279F7F4AF7E8460C046AF726E08F22F65D7597
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
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):	498
Entropy (8bit):	5.16652318905477
Encrypted:	false
SSDEEP:	12:FX1BlOcXYKD5u/BP1RZQndYcVQWaFBk778B/xgsht17A/UfDn:FX1/35kp1ROdvQ7Y78BJgs7ZDD
MD5:	74030C716B93460FEC7AB01646AE09B9
SHA1:	9133BBFF9BAB31B1FFD2CEEEE6824B9CD0CE4812
SHA-256:	EA3B387F64A1ADB53E43AC1D7CEFF76305B902E1BE1BA4A84959E5B88F5BDC23
SHA-512:	74FC3ECD2490B3FF0D97E427799EE841A789BAE4B8DDE908A26608FFC57271927C1A2A6945AD82F5BBDE22321D5E398AFFE49ACEEEF60021087FF37AC71F925F
Malicious:	false
Reputation:	low
Preview:	....."6....com..herokuapp..https..oauth..securecloud..working*N.....com.....herokuapp.....https.....oauth.....securecloud.....working..2.....a.....c.....d.....e.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....w...:8.....BW...S..... .....*(https://securecloud-oauth.herokuapp.com/2.Working:.....J.....$...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33356
Entropy (8bit):	0.04747596494984347
Encrypted:	false
SSDEEP:	6:8o9j+qX/s6OX6kUqng9bNFlWCj/lAQIl3n:L90OeqLBj/9Y3n
MD5:	E9EA03A8B9335CEA4CA33B5A582AE042
SHA1:	1D8EC3071705FC2C486BA6C8E65E1FC1D7C72979
SHA-256:	AF91FCCB4EDE036EE1CE73FE860C9E5F0E2495B7EF17F23A363418FF49FF994E
SHA-512:	F697FCD61D14DE29E18AD20E3BCA3F4EF3B568B51FEB6A3099E6FBC8E1321E78FD09684675D50E3AFBC8EAF64D6D4058DE849A91FBE00E8E6ADCC99755F0CCC
Malicious:	false
Reputation:	low
Preview:	.....e..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Sessionn (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	981
Entropy (8bit):	3.3137807819980645
Encrypted:	false
SSDEEP:	12:3olydJheJaGPlpxlpN8klyT4ZA/tl/U0aG3CLU+5ByZA/Zt5lptlpl:34SAlrlADZlM0aO4U+5EZyPlLlL
MD5:	442E29B4B063C3B41726E61DC3381653
SHA1:	24DEF8E1CA279CF3DCCFE54F50AB515C0CF0D08A
SHA-256:	DAB96FD9E32D49FC49896B969E242D62D990DF1490BFF9BAAB0690771AEC81C5
SHA-512:	8B2EF558041A3158D05B1F7A8172D15983FB23A008FD1004DA9672597F01F68331E8233261D5C7164227C5FDA1C850F8F3668C790760A246756E50082DE57018
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...909f5e03_d8eb_447e_b077_166c34f598ed.....\.W..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....Q..L.....(...https://securecloud-oauth.herokuapp.com/..... .....h.....`..... ..h...!..h.....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://securecloud-oauth.herokuapp.com/.....B.M'/..... .....

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):	5.470738603656764
Encrypted:	false
SSDEEP:	48:oD7GNwza74MT8db+6KHbQSefgGiNrS0U9RdiN9Atu:tia74Mgdb+6KHbQ5fgGurS0itu
MD5:	C4BB6F81C88B3624E7ADE9022F93BCE6
SHA1:	A02F3BBF92EEC72CB275D2F4253DDBC65A62EEFC
SHA-256:	5557646353F908AF931450197C7C9F19F455A49FBEEEB903BF6B31DEFFA64C6A
SHA-512:	EBAE312C58BB519E5BF3AEC65EE3FD08593F0C2EDC4A28F503C8F94D1CB4355D6887A84E0D10C762471F13A8842CF740295A04BB09258D89074AAAA5F008F45A
Malicious:	false
Reputation:	low
Preview:	.x.....*.....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..822842000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-04 01:15:49.19][INFO][mr.Init] MR instance ID: 3bcd1320-f8c9-4dcc-be59-8d575eb37a8e\n","[2021-08-04 01:15:49.19][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-04 01:15:49.19][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-04 01:15:49.19][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-04 01:15:49.19][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-04 01:15:49.19][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-04 01:15:49.19][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):	5.189511228465767
Encrypted:	false
SSDEEP:	6:mIOOEF39+q2PWXp+N23iKKdK8a2jMGIFUtpvOqmJZmwPvOqd19VkwOWXp+N23iKi:EF34va5Kk8EFUtpIJ/PL1D5f5Kk8bJ
MD5:	2543F29E81F4BA3DDE7BA82F8DF0D1D0
SHA1:	0550F32691EDF6B765769FC156045FF99CB44682
SHA-256:	0CDBA18278ACEB242FCF26315FA1118598E23B8591CE962ABC325541AB2E3396
SHA-512:	CE7D1706A8389BE7F48E8ABE0D57E914AC9776F20CBB91B33F1A1B708E05FC43942A1AEEDC915B6954ACAD5379F58072A0D5E532D929D5038CD65F4121D80FB
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.226 1368 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:15:40.233 1368 Recovering log #3.2021/08/04-01:15:40.238 1368 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):	5.189511228465767
Encrypted:	false
SSDEEP:	6:mIOOEF39+q2PWXp+N23iKKdK8a2jMGIFUtpvOqmJZmwPvOqd19VkwOWXp+N23iKi:EF34va5Kk8EFUtpIJ/PL1D5f5Kk8bJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
MD5:	2543F29E81F4BA3DDE7BA82F8DF0D1D0
SHA1:	0550F32691EDF6B765769FC156045FF99CB44682
SHA-256:	0CDBA18278ACEB242FCF26315FA1118598E23B8591CE962ABC325541AB2E3396
SHA-512:	CE7D1706A8389BE7F48E8ABE0D57E914AC9776F20CBB91B33F1A1B708E05FC43942A1AEEDC915B6954ACAD5379F58072A0D5E532D929D5038CD65F4121D80F B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.226 1368 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/0 8/04-01:15:40.233 1368 Recovering log #3.2021/08/04-01:15:40.238 1368 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 Stateb (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advert ised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","support s_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":"1324854350 1454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.225221687570407
Encrypted:	false
SSDEEP:	6:mIOXX9+q2PWXp+N23iKKdKgXz4rRIFUtpvORJZmwPvOkD9VkwOWXp+N23iKKdKgi:6X4va5KkgXiuFUtpeJ/PHD5f5KkgX2J
MD5:	B76771DCB6461645F2F2CD8D52B6D669
SHA1:	A7A4ED4861992127A80E0D07662A77F36A7ACF65
SHA-256:	7058DA708A6F780A3CC7A8C027DA717C2FF7006046B5E0146315C762E421C715
SHA-512:	A12CA62D5549ECD993DDEF24F70FB88E70ADB77F1696D371D3D0629843B13F919434558B9D413C4AC3B823833EB9410916E164C91743DE0040CC209D156C069F
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.505 1368 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/ 08/04-01:15:40.507 1368 Recovering log #3.2021/08/04-01:15:40.508 1368 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Noti fications/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):	5.225221687570407
Encrypted:	false
SSDEEP:	6:mIOXX9+q2PWXp+N23iKKdKgXz4rRIFUtpvORJZmwPvOkD9VkwOWXp+N23iKKdKgi:6X4va5KkgXiuFUtpeJ/PHD5f5KkgX2J
MD5:	B76771DCB6461645F2F2CD8D52B6D669
SHA1:	A7A4ED4861992127A80E0D07662A77F36A7ACF65
SHA-256:	7058DA708A6F780A3CC7A8C027DA717C2FF7006046B5E0146315C762E421C715
SHA-512:	A12CA62D5549ECD993DDEF24F70FB88E70ADB77F1696D371D3D0629843B13F919434558B9D413C4AC3B823833EB9410916E164C91743DE0040CC209D156C069F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Preview:	2021/08/04-01:15:40.505 1368 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-01:15:40.507 1368 Recovering log #3.2021/08/04-01:15:40.508 1368 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):	5754
Entropy (8bit):	5.197500512295057
Encrypted:	false
SSDEEP:	96:nbCd359jUB/fcKIlok0JCKL8fk01YbOTQVuwn:nbCr9jgHcC4KSk0k
MD5:	B9496BF5B8A662309779DCF4A10E57E4
SHA1:	C8F53D3AA074C96DF7E6E0B7FE016E2BBFCC8259
SHA-256:	87E42905BD6FB8B4F8712EE0C1D024F3AB95DC9A769FFEDCE3727E2B67235863
SHA-512:	B9B4D25A1DFEFCA5CD18482BBF34B075EEBFEEDA314DDCA08886D9E0D8AEAA40BC00EDF3E9EC043D68601EAD5B98A81EF0F336CFD5AC698C17A07D240F9F C097
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272538540475030","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\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:	modified
Size (bytes):	20480
Entropy (8bit):	1.0040176314681757
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUbGiLhSK7:wIElwQF8mpcS5j
MD5:	A6490F9E160E7CCEEA5103090F02319D
SHA1:	757AC3FCA5AEEE7E090F13453A442A95E39EF0B8
SHA-256:	62AC33F4FF50AA756BAE6639CB606AFD400C57A2379D8397A1D3CC35CA55AE27
SHA-512:	234C62D264A9DBDF1180D195DFF4A9C672036D4AAD0F29DAB772CECC78AC3539BBE451E5B6EF06141D753D826BEE9516C0F4CBC149561BFC30A5E33C1BD80 74
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):	0.8235034998988683
Encrypted:	false
SSDEEP:	48:shWqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUl6:shWhIElwQF8mpcSk
MD5:	7BF13D565E7FA4591965A0919D8E6EA1
SHA1:	9F8977476C8B9CB6F95D839C05C95F7234732BD3
SHA-256:	23AFDE7CBDCE504EDF9AF3CFEBF43422EAFAB1498EEDA3B365D00B437838E9BB
SHA-512:	D0ECB324E1529DEC41E0D2A37C6EDC92F11432B8DADBA2C442F46AAFBB950B95A3A93050F52C3F6A3FF18DE0E057F4C061EC62A54B6B4ECBAF63AACBB02E 7461
Malicious:	false
Reputation:	low
Preview:	.... s...

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):	22595
Entropy (8bit):	5.536100595222747
Encrypted:	false
SSDEEP:	384:y/ftvLlahXt1kXqKf/pUZNCgVLH2HfDwrU9HGlnTqlsF4A:KLlGt1kXqKf/pUZNCgVLH2HfUrUhGlnz
MD5:	F170489B7BF225B96D7F5A4AD08A95AE
SHA1:	DFC07400A5F77DD44326E029C16EDE87274A5C15
SHA-256:	5E1E341998CD45B3F0859AD3ABF95FE2278D86E98989A8D7CC7C4888AF38577A
SHA-512:	55D4181C7F667BC9248C3CD4D03B58FCF75CD5C436AD5671E1E69EF1866358E5EC4DCA9EAA6A43DB3C08674EFD6849737C4205BB633356D6E8A65C053F8A2C3
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":"13272538540178986","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\Secure Preferencest (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):	24056
Entropy (8bit):	5.533918680747312
Encrypted:	false
SSDEEP:	384:y/ftvLlahXt1kXqKf/pUZNCgVLH2HfDwrU7HG9HGxnTqlCF4A:KLlGt1kXqKf/pUZNCgVLH2HfUrULGhGz
MD5:	789E3946C3F97E4B52585E10578E106F
SHA1:	AE680D0EF79B455FF14D020F8B6A96BAD920F281
SHA-256:	7D05B079ED3F0C96383113D8B4AFED11D1AC0132A6643E1909F7671BB3695B28
SHA-512:	7132DC16D263C63780FAA3A3BC71AB2D8DD488F66B8FE1BA39C5D49300070AF9CEAA3CD6C4EC5A0D4EC608F86E097C689917CA6C103AF9CC4EB048FE872A7D8
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":"13272538540178986","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\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:	3:5ljljljljl: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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Size (bytes):	317
Entropy (8bit):	5.182071914288269
Encrypted:	false
SSDEEP:	6:mIOMhN+q2PWXp+N23iKKdKrQMxIFUtpvOMhQXWZmwPvOMhQiVkwOWXp+N23iKKd0:DhN+va5KkCFUtpTCW/PTBV5f5KktJ
MD5:	2E113B398A75F43EC1DF18C9D0CF3FD6
SHA1:	08710AE668F946F8E550F9E6DCB99BEBCBB5B331
SHA-256:	C8978A70AC400A3EF4372C81280590ABD6003259EEA18FF0AE01C5CBC67915E2
SHA-512:	52B365D22B84C561501C820C161EDAF58B3CEBEEE5F53FBD3832987F27AEBFB22092FDC620C3F110C05272C670684644B19570742B0E23B5501CBE629BBDFDB
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.436 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-01 :15:40.438 d5c Recovering log #3.2021/08/04-01:15:40.438 d5c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/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):	317
Entropy (8bit):	5.182071914288269
Encrypted:	false
SSDEEP:	6:mIOMhN+q2PWXp+N23iKKdKrQMxIFUtpvOMhQXWZmwPvOMhQiVkwOWXp+N23iKKd0:DhN+va5KkCFUtpTCW/PTBV5f5KktJ
MD5:	2E113B398A75F43EC1DF18C9D0CF3FD6
SHA1:	08710AE668F946F8E550F9E6DCB99BEBCBB5B331
SHA-256:	C8978A70AC400A3EF4372C81280590ABD6003259EEA18FF0AE01C5CBC67915E2
SHA-512:	52B365D22B84C561501C820C161EDAF58B3CEBEEE5F53FBD3832987F27AEBFB22092FDC620C3F110C05272C670684644B19570742B0E23B5501CBE629BBDFDB
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.436 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-01 :15:40.438 d5c Recovering log #3.2021/08/04-01:15:40.438 d5c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/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):	5.162938892457201
Encrypted:	false
SSDEEP:	6:mIOcQ+q2PWXp+N23iKKdK7Uh2ghZIFUtpvOfQgZmwPvOfQQVkwOWXp+N23iKKdKs:RVva5KklhHh2FUtpiQg/PiQI5f5KkIh9
MD5:	F3B1615099AD372FC1D56C9A4D159C3A
SHA1:	63D24031F497BFD719C033016DD27623D077FF8C
SHA-256:	119154730EFF30C0B3E2718D954A80B1434D50B12828190726020802FDBBF300
SHA-512:	5CCA9438B2D1AC40061ADCDA5EE661E3A1B701F421CAAD82B3F51A73A2D19251CE1D2F525885A4E804642D46FF8728BB987B0395D6B81DA6567351C51CD7CF 1
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.186 12f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/04-01:15:40.191 12f8 Recovering log #3.2021/08/04-01:15:40.191 12f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old,p (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.162938892457201
Encrypted:	false
SSDEEP:	6:mIOcQ+q2PWXp+N23iKKdK7Uh2ghZIFUtpvOfQgZmwPvOfQQVkwOWXp+N23iKKdKs:RVva5KklhHh2FUtpiQg/PiQI5f5KkIh9
MD5:	F3B1615099AD372FC1D56C9A4D159C3A
SHA1:	63D24031F497BFD719C033016DD27623D077FF8C
SHA-256:	119154730EFF30C0B3E2718D954A80B1434D50B12828190726020802FDBBF300
SHA-512:	5CCA9438B2D1AC40061ADCDA5EE661E3A1B701F421CAAD82B3F51A73A2D19251CE1D2F525885A4E804642D46FF8728BB987B0395D6B81DA6567351C51CD7CF 1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old,p (copy)	
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.186 12f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/04-01:15:40.191 12f8 Recovering log #3.2021/08/04-01:15:40.191 12f8 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\11fae294-3638-4c77-a790-0ce235b0dfc9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.240238014273351
Encrypted:	false
SSDEEP:	6:mIOM0+q2PWXp+N23iKKdKusNpV/2jMGIFUtpvOM00ZmwPvOcnVkwOWXp+N23iKKZ:DJva5KkFFUtpT1/P5V5f5KkOJ
MD5:	C0BA8C31BA4E3AF7D48BD2E5DFE8A64B
SHA1:	9498168EC059BBC0B2A77A172A8A080C345A8759
SHA-256:	A29F050EA3145BE7A4FEB1E709B8B155D9E6AF3478DA38D843B13B55F8864DA0
SHA-512:	E296A4CFFAC222D1F743F5E876444AF5606951019068C2AD012DD3306C8BF7F082258A1E920AB0066A82EAAF36B437475D7C07DB567AD0997618CED59B783DC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.438 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:15:40.439 508 Recovering log #3.2021/08/04-01:15:40.440 508 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.240238014273351
Encrypted:	false
SSDEEP:	6:mIOM0+q2PWXp+N23iKKdKusNpV/2jMGIFUtpvOM00ZmwPvOcnVkwOWXp+N23iKKZ:DJva5KkFFUtpT1/P5V5f5KkOJ
MD5:	C0BA8C31BA4E3AF7D48BD2E5DFE8A64B
SHA1:	9498168EC059BBC0B2A77A172A8A080C345A8759
SHA-256:	A29F050EA3145BE7A4FEB1E709B8B155D9E6AF3478DA38D843B13B55F8864DA0
SHA-512:	E296A4CFFAC222D1F743F5E876444AF5606951019068C2AD012DD3306C8BF7F082258A1E920AB0066A82EAAF36B437475D7C07DB567AD0997618CED59B783DC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.438 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:15:40.439 508 Recovering log #3.2021/08/04-01:15:40.440 508 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
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):	5.256081454772514
Encrypted:	false
SSDEEP:	12:UkDM+va5KkmiuFUtpMg/PDDMV5f5Kkm2J:Uma5KkSgmf5Kkr
MD5:	5C2A190C04777170E7E90712958B8307
SHA1:	CF3410080CE4028D5CC1D26E001EC1099A7E17AA
SHA-256:	6FB95161BC9D230EC155DD3C6DF13821DE35D6F894C68A060B4088978875D825
SHA-512:	E3DA2BCCDC30FA55A9DB909BB872AB5E3F0DA48BEA7836B5F1F17707A8503DE74612A11D2B4B5FC5AC8BC635832DC6E23C2935C6D5C861AE4BC6F92ED1FF815
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.504 15fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/04-01:15:40.507 15fc Recovering log #3.2021/08/04-01:15:40.508 15fc 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):	5.256081454772514
Encrypted:	false
SSDEEP:	12:UkDM+va5KkmiuFUtpMg/PDDMV5f5Kkm2J:Uma5KkSgmf5Kkr
MD5:	5C2A190C04777170E7E90712958B8307
SHA1:	CF3410080CE4028D5CC1D26E001EC1099A7E17AA
SHA-256:	6FB95161BC9D230EC155DD3C6DF13821DE35D6F894C68A060B4088978875D825

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
SHA-512:	E3DA2BCCDC30FA55A9DB909BB872AB5E3F0DA48BEA7836B5F1F17707A8503DE74612A11D2B4B5FC5AC8BC635832DC6E23C2935C6D5C861AE4BC6F92ED1FF(815
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.504 15fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/04-01:15:40.507 15fc Recovering log #3.2021/08/04-01:15:40.508 15fc Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.281043386880695
Encrypted:	false
SSDEEP:	6:mILc+q2PWXp+N23iKKdKusNpZQMxIFUtpvL+0ZmwPvL2VtVkwOWXp+N23iKKdKuG:zhva5KkMFUtpD+0/PDS5f5KkTJ
MD5:	26F522065997E78E3DCB577EB9D1EC4E
SHA1:	49341E384345476F076687E78DFD70F89B932393
SHA-256:	C1E55E9CA943D834724A6D40AFCD5155441B436CB094B3E1BECB56107C61FB63
SHA-512:	6B8C434D7604AF6AB00CC2B50311A338BF0AF10D020305B91C933E95617FB236B70C81F77F2D0C9CD07FC337C89D6A4ABDD3842FB2034D4A831ACD9B3DAA70 C
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:56.707 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Session Storage/MANIFEST-000001.2021/08/04-01:15:56.708 508 Recovering log #3.2021/08/04-01:15:56.709 508 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.olde/ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.281043386880695
Encrypted:	false
SSDEEP:	6:mILc+q2PWXp+N23iKKdKusNpZQMxIFUtpvL+0ZmwPvL2VtVkwOWXp+N23iKKdKuG:zhva5KkMFUtpD+0/PDS5f5KkTJ
MD5:	26F522065997E78E3DCB577EB9D1EC4E
SHA1:	49341E384345476F076687E78DFD70F89B932393
SHA-256:	C1E55E9CA943D834724A6D40AFCD5155441B436CB094B3E1BECB56107C61FB63
SHA-512:	6B8C434D7604AF6AB00CC2B50311A338BF0AF10D020305B91C933E95617FB236B70C81F77F2D0C9CD07FC337C89D6A4ABDD3842FB2034D4A831ACD9B3DAA70 C
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:56.707 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Session Storage/MANIFEST-000001.2021/08/04-01:15:56.708 508 Recovering log #3.2021/08/04-01:15:56.709 508 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\18f823a0-e59c-4d90-b26a-34f1a35bf16e.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"},{"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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
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):	5.190028099482578
Encrypted:	false
SSDEEP:	12:uDM+va5KkkGHArBFUtpMg/PqSDMV5f5KkkGHAryJ:wa5KkkGgPgmXf5KkkGga
MD5:	EF92436C86E5B68EE72EA1ACD94A3DD5
SHA1:	2FCC0998F535A569275E9DF31B1598FA87E1ACFD
SHA-256:	7E2B4291184E2315C0A03F423198E3823EDF80B4EEB6E736C63F5F38EBBEF01E
SHA-512:	9480288C5B6DFD4E4E702D3B25E003FD0E0A90C313F37154D71F6711435639244C0EC923B92DAA0157C474488B3C71D9B090E0AEBDB2001C02C6CF084111D48
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:48.130 15fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:15:48.132 15fc Recovering log #3.2021/08/04-01:15:48.133 15fc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.190028099482578
Encrypted:	false
SSDEEP:	12:uDM+va5KkkGHArBFUtpMg/PqSDMV5f5KkkGHAryJ:wa5KkkGgPgmXf5KkkGga
MD5:	EF92436C86E5B68EE72EA1ACD94A3DD5

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

SHA1:	2FCC0998F535A569275E9DF31B1598FA87E1ACFD
SHA-256:	7E2B4291184E2315C0A03F423198E3823EDF80B4EEB6E736C63F5F38EBBEF01E
SHA-512:	9480288C5B6DFD4E4E702D3B25E003FD0E0A90C313F37154D71F6711435639244C0EC923B92DAA0157C474488B3C71D9B090E0AEBDB2001C02C6CF084111D48
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:48.130 15fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-01:15:48.132 15fc Recovering log #3.2021/08/04-01:15:48.133 15fc 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 Statemp (cop y)

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\Platform Notifications\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.223130887440989
Encrypted:	false
SSDEEP:	12:H+va5KkkGHArqiuFUtpDiW/PDhV5f5KkkGHArq2J:8a5KkkGgCglikhf5KkkGg7
MD5:	53CCED421417FE1AAF89044789622114
SHA1:	CA2F5CC310EDEA5588018B1894568FE013F31AE9
SHA-256:	80FC620CD013E2E6F5997DA3D0EB66D5C17EBA5C34A6670D385AB37009DF1646
SHA-512:	8E5DC7DBD0D5AF56C6DB5434890B4932C11BBA99F9C9EB06149984C2A9256866DA86F16059AA3836D1461FB29C3402D60E1FECCD322DE480171A1725371FCB6
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:48.159 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Platform Notifications/MANIFEST-000001.2021/08/04-01:15:48.162 d5c Recovering log #3.2021/08/04-01:15:48.162 d5c 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):	429
Entropy (8bit):	5.223130887440989
Encrypted:	false
SSDEEP:	12:H+va5KkkGHArqiuFUtpDiW/PDhV5f5KkkGHArq2J:8a5KkkGgCglikhf5KkkGg7
MD5:	53CCED421417FE1AAF89044789622114
SHA1:	CA2F5CC310EDEA5588018B1894568FE013F31AE9
SHA-256:	80FC620CD013E2E6F5997DA3D0EB66D5C17EBA5C34A6670D385AB37009DF1646
SHA-512:	8E5DC7DBD0D5AF56C6DB5434890B4932C11BBA99F9C9EB06149984C2A9256866DA86F16059AA3836D1461FB29C3402D60E1FECCD322DE480171A1725371FCB6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
Preview:	2021/08/04-01:15:48.159 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/04-01:15:48.162 d5c Recovering log #3.2021/08/04-01:15:48.162 d5c 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):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Reputation:	low
Preview:	..&f.....&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):	415
Entropy (8bit):	5.180165951906452
Encrypted:	false
SSDEEP:	6:mI93+q2PWXp+N23iKKdKkGckArZQMxIFUtpvOZmwPv/VkwOWXp+N23iKKdKkGcki:wva5KkkGHArAFUtpW/P15f5KkkGHArfJ
MD5:	532F3BAF462147F9AE9ED348CC875CE9
SHA1:	4F9C6F9AF95B316103E2886EE80249C575D878D5
SHA-256:	416CDA20F76875327AF297AD5CB13F5F3F571641A0C916845FDE11073F2BD634
SHA-512:	3F246EBFB70AF053168E55BFF61B2043E40655110EB92ACA5C6AAA5BB66C275C0BCFCA4A324B05C43BA13F879ED817749AA6A1AA5CC6FE6265977A3C8BF9D67B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:16:03.411 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/04-01:16:03.412 508 Recovering log #3.2021/08/04-01:16:03.413 508 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.180165951906452
Encrypted:	false
SSDEEP:	6:mI93+q2PWXp+N23iKKdKkGckArZQMxIFUtpvOZmwPv/VkwOWXp+N23iKKdKkGcki:wva5KkkGHArAFUtpW/P15f5KkkGHArfJ
MD5:	532F3BAF462147F9AE9ED348CC875CE9
SHA1:	4F9C6F9AF95B316103E2886EE80249C575D878D5
SHA-256:	416CDA20F76875327AF297AD5CB13F5F3F571641A0C916845FDE11073F2BD634
SHA-512:	3F246EBFB70AF053168E55BFF61B2043E40655110EB92ACA5C6AAA5BB66C275C0BCFCA4A324B05C43BA13F879ED817749AA6A1AA5CC6FE6265977A3C8BF9D67B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:16:03.411 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/04-01:16:03.412 508 Recovering log #3.2021/08/04-01:16:03.413 508 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.235719180493192
Encrypted:	false
SSDEEP:	6:mIOCq2PWXp+N23iKKdKpIFUtpvOPZmwPvOrFfVFkwOWXp+N23iKKdKa/WLJ:/va5KkmFUtpe/PCFfVF5f5KkaUJ
MD5:	3B217829C64C35E62DD108809FA72A9E
SHA1:	7490E219D2F16EFB08CEC9FA1BFCD16ECA3974F4
SHA-256:	9222886F461AC1419C77163AE235FACF42C528CE56C4000F4B3AD782543340C1
SHA-512:	1B7861EB159FC95F25465E7F2610D7116F1DF4E3DCC3FF94CD73F8FE17CBE87061D8732925963EC7A4A6628D4B21BE8EB3F746CC50D50CFF9BBA48CBFE85D1 3
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.183 660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-01:15:40.187 660 Recovering log #3.2021/08/04-01:15:40.190 660 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.235719180493192
Encrypted:	false
SSDEEP:	6:mIOCq2PWXp+N23iKKdKpIFUtpvOPZmwPvOrFfVFkwOWXp+N23iKKdKa/WLJ:/va5KkmFUtpe/PCFfVF5f5KkaUJ
MD5:	3B217829C64C35E62DD108809FA72A9E
SHA1:	7490E219D2F16EFB08CEC9FA1BFCD16ECA3974F4
SHA-256:	9222886F461AC1419C77163AE235FACF42C528CE56C4000F4B3AD782543340C1
SHA-512:	1B7861EB159FC95F25465E7F2610D7116F1DF4E3DCC3FF94CD73F8FE17CBE87061D8732925963EC7A4A6628D4B21BE8EB3F746CC50D50CFF9BBA48CBFE85D1 3
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:40.183 660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-01:15:40.187 660 Recovering log #3.2021/08/04-01:15:40.190 660 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):	399
Entropy (8bit):	5.330044118780552
Encrypted:	false
SSDEEP:	6:mIaAt+q2PWXp+N23iKKdKks8Y5JKKhdIFUtpv00ZmwPv0UVkwOWXp+N23iKKdKk0:pova5KkkOrsFUtpc0/Pc05f5KkkOrzJ
MD5:	3AC4F0F587A8EF2EFCB9003D00A60919
SHA1:	1BAFA5577F946B4D59D9F949793423455A2AAE16
SHA-256:	98E73D3D6AC4489206A068CE7933C35698ABB3EA65DAB6F671E1418B3BE4AA4E
SHA-512:	B5C267E7E410FFFAA519FD7751FD88DD405DF96241511EB85348668C33DAA76E44683340C090C4FEE78D1898BBC57319EF612F7D275A7714DCA376B7E0E9AFC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Preview:	2021/08/04-01:15:49.151 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/04-01:15:49.153 508 Recovering log #3.2021/08/04-01:15:49.153 508 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):	399
Entropy (8bit):	5.330044118780552
Encrypted:	false
SSDEEP:	6:mIaAt+q2PWXp+N23iKKdKks8Y5JKKhdIFUtpv00ZmwPv0UVkwOWXp+N23iKKdKk0:pova5KkkOrsFUtpc0/Pc05f5KkkOrzJ
MD5:	3AC4F0F587A8EF2EFCB9003D00A60919
SHA1:	1BAFA5577F946B4D59D9F949793423455A2AAE16
SHA-256:	98E73D3D6AC4489206A068CE7933C35698ABB3EA65DAB6F671E1418B3BE4AA4E
SHA-512:	B5C267E7E410FFFAA519FD7751FD88DD405DF96241511EB85348668C33DAA76E44683340C090C4FEE78D1898BBC57319EF612F7D275A7714DCA376B7E0E9AFC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:49.151 508 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/04-01:15:49.153 508 Recovering log #3.2021/08/04-01:15:49.153 508 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.566210022658869
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvtP7wU5RUenHQ:YI6UUhVseKUewqPeUer2UefxwUfUenw
MD5:	43098F2E2FDAE70C41ED593A8A5199B0
SHA1:	147DEFD8D0B5FBCFAE3294D10954B7A7019A26CB
SHA-256:	ACE1E54E64A6F8EFA77593EB1CE7205CBA12F12DFDF932B2BA9100E076FD6734
SHA-512:	178C362528C1B7FDEDCAB5A0231012C1A0B083BD9C3F811B4DE1204568A36F03C69785B4C44DBC0C8983616516D1E89F09F2DB5C27BB802AF39A8A0C347CADE
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":1659600945.004806,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628064945.004809},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

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:b8oV:b5V
MD5:	EFEB7D2B3A1603BCC6178499F456F3A9
SHA1:	EA1719CCB18DA7354291E45236AD621E9641CE79
SHA-256:	42342BD02EAAEF61878C3B07566458B49F0B8C2FA83EF876EA1D30A2A282F8B1
SHA-512:	7B6C9B5247B0FB3CDBC2B0119B82909BFBD09CC136AA0ACB1C931BC64887AC2490727F2AEDDF76B96D712A8A91BF6B5C9881F8A4290B293228CBAF2165AC37FA
Malicious:	false
Reputation:	low
Preview:	.....*M.U

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\378df481-0f11-4daf-a4b6-eacd2e92fe75.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\378df481-0f11-4daf-a4b6-eacd2e92fe75.tmp	
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E....I...k}....{.m.t.CP.....E...\.....=H..,A..,J..;P.....nn p}nnp}.....~~~.....!...!---2---2... .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P.. .Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e..... ....nnnzXXXa.....RRR\.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168B6
Malicious:	false
Reputation:	low
Preview:	F.....r...(R..

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
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\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):	4.388021910636348
Encrypted:	false
SSDEEP:	3:tUK6NUJLxW4VSgZmwv3INUJLW/L1V8sINUJL2+FJ1WGv:mIDW7gZmwPvI5Vvvphtv
MD5:	7041DD57F58CE5BE8B97D26904733712
SHA1:	B292401B9232E24CAFE2FB0FDE59F76EBF421053
SHA-256:	CCA686BE65B48BD2E14A0236D8743759F0A4CC8DC3702A84EB93639075C47AEF
SHA-512:	186245860838CFCA75536DB9EB40D7F37EF7CDAE10504528D9392E28FEED485DB71547109CD11C71CCA862077654E18C5B6887E5BFB648BA42985D7A982AE63
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.423 1200 Recovering log #3.2021/08/04-01:15:47.523 1200 Delete type=0 #3.2021/08/04-01:15:47.524 1200 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):	4.388021910636348
Encrypted:	false
SSDEEP:	3:tUK6NUJLxW4VSgZmwv3INUJLW/L1V8sINUJL2+FJ1WGv:mIDW7gZmwPvI5Vvvphtv
MD5:	7041DD57F58CE5BE8B97D26904733712
SHA1:	B292401B9232E24CAFE2FB0FDE59F76EBF421053
SHA-256:	CCA686BE65B48BD2E14A0236D8743759F0A4CC8DC3702A84EB93639075C47AEF
SHA-512:	186245860838CFCA75536DB9EB40D7F37EF7CDAE10504528D9392E28FEED485DB71547109CD11C71CCA862077654E18C5B6887E5BFB648BA42985D7A982AE63
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.423 1200 Recovering log #3.2021/08/04-01:15:47.523 1200 Delete type=0 #3.2021/08/04-01:15:47.524 1200 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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	5.235236536688398
Encrypted:	false
SSDEEP:	6:mIWFCq2PWXp+N23iKKdKfrzAdIFUtpvvBZmwPvUFbFkwOWXp+N23iKKdKfrzILJ:+FCva5Kk9FUtpR/PA5f5Kk2J
MD5:	1A149354CC63FA3CF407D7EF3E27A95B
SHA1:	E7378D1A94773641EF81954445DDB8BF8A131B55
SHA-256:	9A60AA3B7E6A9C4C1C48E7CF1250F7F8E4465E1F0F616EF1E614BC5B19FAF2D6
SHA-512:	54584A1FB4AC77FDC30DDFCABDFD198068DB9DE5A46A255EEF8778A6D4E92FE7890ED5DB9F991630B72617190B501D046B0569BAD30294A74A5EA463AACC201E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.834 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/04-01:15:47.835 15b0 Recovering log #3.2021/08/04-01:15:47.836 15b0 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):	5.235236536688398
Encrypted:	false
SSDEEP:	6:mIWFCq2PWXp+N23iKKdKfrzAdIFUtpvvBZmwPvUFbFkwOWXp+N23iKKdKfrzILJ:+FCva5Kk9FUtpR/PA5f5Kk2J
MD5:	1A149354CC63FA3CF407D7EF3E27A95B
SHA1:	E7378D1A94773641EF81954445DDB8BF8A131B55
SHA-256:	9A60AA3B7E6A9C4C1C48E7CF1250F7F8E4465E1F0F616EF1E614BC5B19FAF2D6
SHA-512:	54584A1FB4AC77FDC30DDFCABDFD198068DB9DE5A46A255EEF8778A6D4E92FE7890ED5DB9F991630B72617190B501D046B0569BAD30294A74A5EA463AACC201E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-01:15:47.834 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/04-01:15:47.835 15b0 Recovering log #3.2021/08/04-01:15:47.836 15b0 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
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):	174336
Entropy (8bit):	6.079345199189187
Encrypted:	false
SSDEEP:	3072:31/GaYTJQE+mugy9+QV1T7IRwdfLSNPWFcbXafIB0u1GOJmA3iuRL:FOxaV+QfT7GSmh8aqfIlUOoSiuRL
MD5:	4D85AC6BC3F81ABA9AAC70F614FFDD16
SHA1:	677EE75482F0911DCDE1F3660244745472FBEDA1
SHA-256:	883C865883D686C0BDAE6AD6BECAB1E9CD83D7A3B48E22EF037E1D7629D07FED
SHA-512:	07ECB95F70B043BDE86AFD5182C5CCDB7814BCBAEA8C64589DFB412FA18D36D75CE0189C72862ABF147CA1CE9174136E732FCEFFFABD3C0922B6C700BA3B6B54
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":1.628064943269636e+12,"network":1.628032544e+12,"ticks":5759005818.0,"uncertainty":4684117.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7489538170141197
Encrypted:	false
SSDEEP:	384:nPRumYbdEwf65Nmrzv6y3RqgtHIRGtkrPM+QxBkU03r/GmzQf8eKCZOkIKNH1OPA:LeZRKoJ5AenAiocvjGaKACKJz
MD5:	402A499FC2C8AAD06C9827650C0838A3
SHA1:	9D0A487664DE108EC93700C68756A5E574025579
SHA-256:	E20B05DDD4BF4B8F12548DCA269D9086C1EE5D86433348AF22AB7BD28B5D033C
SHA-512:	4CD23341C39ABF0B219A827623D1E50F49B829A274759CB7B265F2D59E0AC69A85C4B5455FDBF62ABA63791147305F568B38B4EBAECD4A634A1C1ACD88A5E385
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\c534f1ad-152d-4067-9acf-27e8a2b2e26f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174336
Entropy (8bit):	6.079345761837566
Encrypted:	false
SSDEEP:	3072:38PGaYTJQE+mugy9+QV1T7IRwdfLSNPWFcbXafIB0u1GOJmA3iuRL:M+xaV+QfT7GSmh8aqfIlUOoSiuRL
MD5:	034D15902678D021BB2FC1F1453C8C8D
SHA1:	6D9D2AD5E39A1ADF29B6249B80B3C511E221C16B
SHA-256:	691F36587474197603660ACB1B505C1D86360C73576212CDCA7EA2E10FDFC62C
SHA-512:	EA41F1E62785E84FD5E36EC30E386F3B3AB5143EE6C6AD8FD1546B9E7811A84F4192C8BD0FCEA79E4D0EBE7C48770C0DF8403881A4AA2CE1B8586D94599B93 7
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":1.628064943269636e+12,"network":1.628032544e+12,"ticks":5759005818.0,"uncertainty":4684117.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Temp\02f74514-3293-4814-afbd-8570dd6d99ee.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L]....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

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 01:15:44.325339079 CEST	192.168.2.3	8.8.8.8	0x7f19	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.329865932 CEST	192.168.2.3	8.8.8.8	0x1aac	Standard query (0)	securecloud-oauth.herokuapp.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.333791971 CEST	192.168.2.3	8.8.8.8	0xb9f3	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:47.279783964 CEST	192.168.2.3	8.8.8.8	0xd402	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 01:15:44.364325047 CEST	8.8.8.8	192.168.2.3	0x1aac	No error (0)	securecloud-oauth.herokuapp.com		3.232.85.60	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.364325047 CEST	8.8.8.8	192.168.2.3	0x1aac	No error (0)	securecloud-oauth.herokuapp.com		34.230.212.197	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.364325047 CEST	8.8.8.8	192.168.2.3	0x1aac	No error (0)	securecloud-oauth.herokuapp.com		3.221.43.225	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.364325047 CEST	8.8.8.8	192.168.2.3	0x1aac	No error (0)	securecloud-oauth.herokuapp.com		34.199.140.75	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.364325047 CEST	8.8.8.8	192.168.2.3	0x1aac	No error (0)	securecloud-oauth.herokuapp.com		54.156.27.150	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.364325047 CEST	8.8.8.8	192.168.2.3	0x1aac	No error (0)	securecloud-oauth.herokuapp.com		3.219.126.122	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.364325047 CEST	8.8.8.8	192.168.2.3	0x1aac	No error (0)	securecloud-oauth.herokuapp.com		3.223.221.167	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.364325047 CEST	8.8.8.8	192.168.2.3	0x1aac	No error (0)	securecloud-oauth.herokuapp.com		34.237.27.35	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.369262934 CEST	8.8.8.8	192.168.2.3	0x7f19	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 01:15:44.369262934 CEST	8.8.8.8	192.168.2.3	0x7f19	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:44.374644041 CEST	8.8.8.8	192.168.2.3	0xb9f3	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 4, 2021 01:15:47.323169947 CEST	8.8.8.8	192.168.2.3	0xd402	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 01:15:47.323169947 CEST	8.8.8.8	192.168.2.3	0xd402	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

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 01:15:44.642416954 CEST	3.232.85.60	443	192.168.2.3	49716	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		
Aug 4, 2021 01:15:44.644967079 CEST	3.232.85.60	443	192.168.2.3	49715	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: 3484 Parent PID: 4864

General

Start time:	01:15:39
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'
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: 5608 Parent PID: 3484

General

Start time:	01:15:40
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=1560,3241909227358404563,10164897485226726443,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1716 /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