ID: 458931
Cookbook: browseurl.jbs
Time: 22:04:25
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

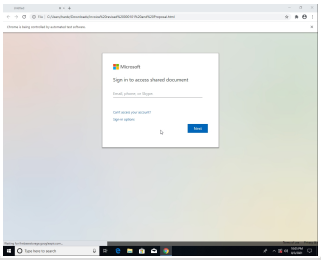
Windows Analysis Report https://ballardagency-my.sha…

Overview

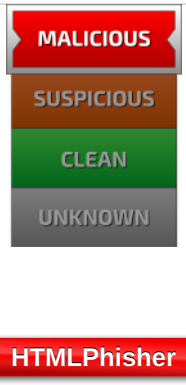
General Information

Sample URL:	http://https://ballardagency-my.sharepoint.com/:u:/p/linda_davidson/EUJ1_psy-lhNg86-55dcNsUB8Ohn7k8q2Vtm1Wl6wQekUA?download=1
Analysis ID:	458931
Infos:	

Most interesting Screenshot:



Detection



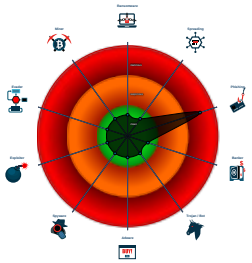
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish44
- Phishing site detected (based on log…
- No HTML title found
- None HTTPS page querying sensitiv…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 1200 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://ballardagency-my.sharepoint.com/:u:/p/linda_davidson/EUJ1_psy-lhNg86-55dcNsUB8Ohn7k8q2Vtm1Wl6wQekUA?download=1' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3560 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,18194422631878575160,1734107580143613396,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1752 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6436 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=quarantine.mojom.Quarantine --field-trial-handle=1544,18194422631878575160,1734107580143613396,131072 --lang=en-US --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=4964 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Downloads\37341020-383d-44e0-be87-80eb5cb51d67.tmp	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Phishing:

Phishing site detected (based on favicon image match)

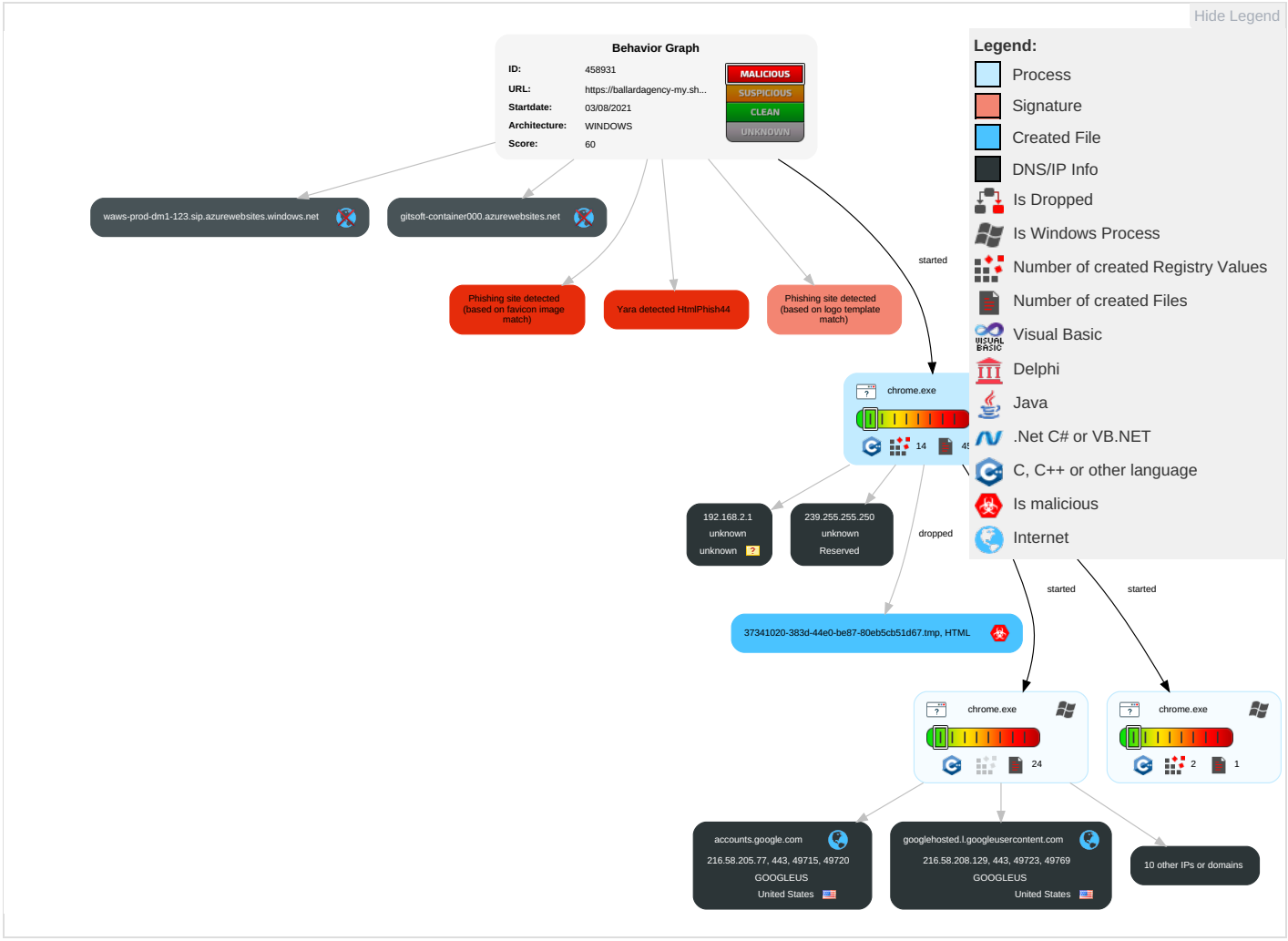
Yara detected HtmlPhish44

Phishing site detected (based on logo template match)

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

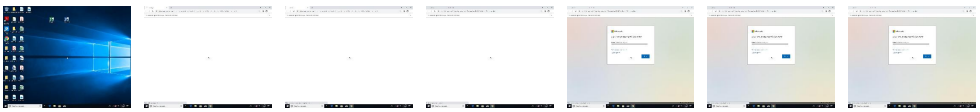
Behavior Graph

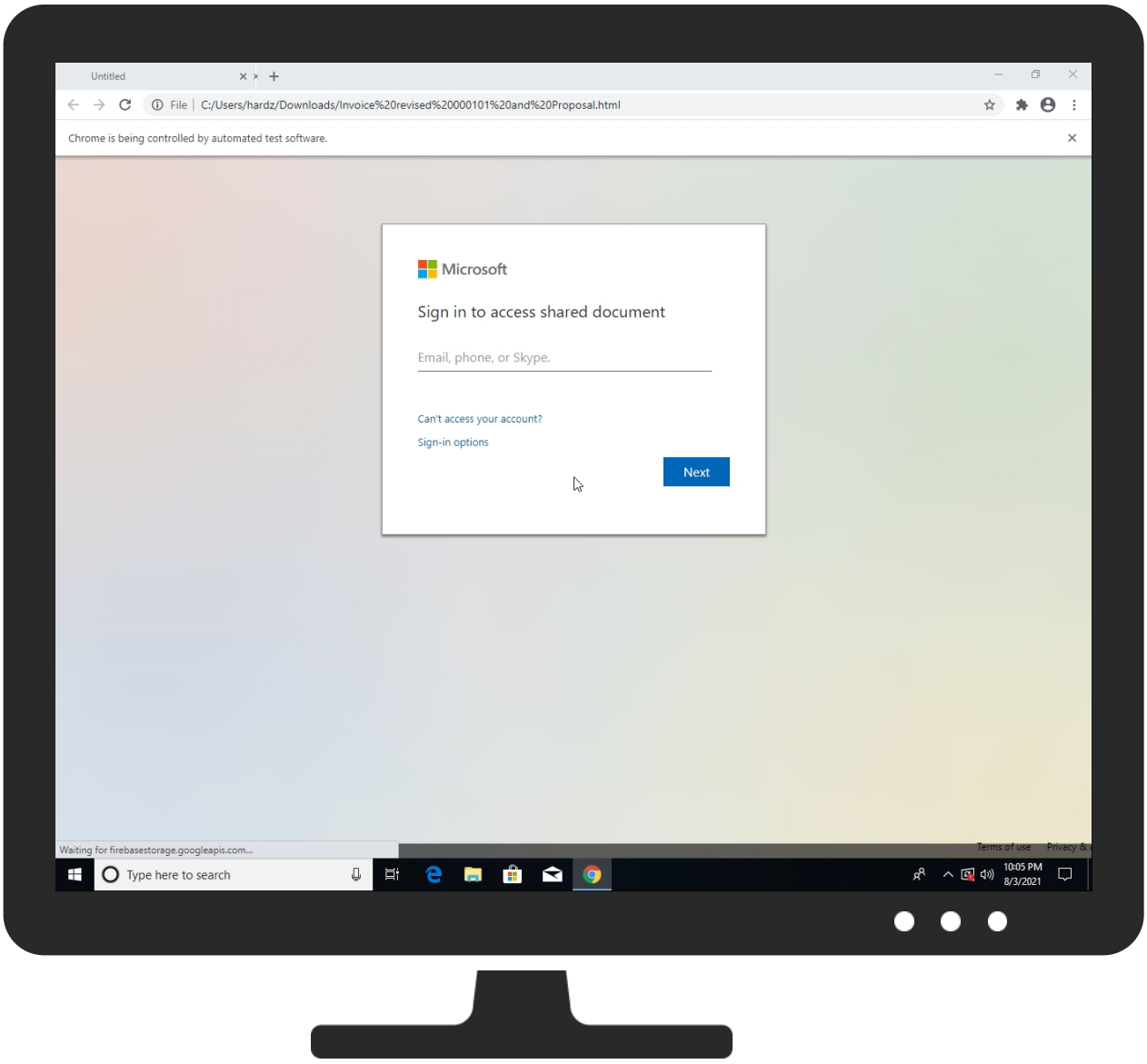


Screenshots

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://ballardagency-my.sharepoint.com/:u:/p/linda_davidson/EUJ1_psy-lhNg86-55dcNsUB8Ohn7k8q2Vtm1Wl6wQekUA?download=1	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ballardagency-my.sharepoint.com	0%	Virustotal		Browse
gitsoft-container000.azurewebsites.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://ballardagency-my.sharepoint.com/:u:/p/linda_davidson/EUJ1_psy-lhNg86-55dcNsUB8Ohn7k8q2Vtm1Wl	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://ballardagency-my.sharepoint.com/personal/linda_davidson_ballardagency_com/Documents/Invoice%	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://ballardagency-my.sharepoint.com	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	
http://https://gitsoft-container000.azurewebsites.net/favicon623e44eff7.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.205.77	true	false		high
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
ballardagency-my.sharepoint.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high
gitsoft-container000.azurewebsites.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Downloads/Invoice%20revised%20000101%20and%20Proposal.html	true		low

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
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:	458931
Start date:	03.08.2021
Start time:	22:04:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 53s
Hypervisor based Inspection enabled:	false

Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://ballardagency-my.sharepoint.com/:u:/p/linda_davidson/EUJ1_psy-lhNg86-55dcNsUB8Ohn7k8q2Vtm1Wl6wQekUA?download=1
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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.win@37/222@6/6
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):	451619

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Entropy (8bit):	5.009890973226876
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4pr:NfOCzvRKhGvwk
MD5:	91E20E3DB3D3EEB8326208B5C96669FB
SHA1:	2DAD9972680D8BA2C4076CF0D4DECBEC01844657
SHA-256:	718BED0783D98465D9EBD58D13DE72DC7D4C33DBFBCEFDBAB4CF7BB4416EA784
SHA-512:	9CE77BE15D12C720FA7B65EF7AC390F8BDFEC423636F403E92D4440D72DC427A60496B1720B5FB2BA6E86D6FE2618ED7C5D780AA77820CA5F39A389F61DFD0A
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\2342856e-5376-43d8-8947-a38cad4044ee.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):	174334
Entropy (8bit):	6.0793136935586265
Encrypted:	false
SSDEEP:	3072:rS6GaYTJQE+mugy9+QV1T7IRwdfLSNPDFcbXafIB0u1GOJmA3iuRV:W/xaV+QfT7GSmhRaqfllUOoSiuRV
MD5:	AB710B946022E77DF19AFE63530B0FD0
SHA1:	BB8E949F4AA5B48FAB95C11B32E031FE9125A37A
SHA-256:	EAE0157661D27F8A382BA097750A5246F5649A3D658877A901FC95C0C61F320B
SHA-512:	0715384AAC718989433E207F7E6AC4521643D557C2E52286F33C677B3820AE4C1F4529B61150F0F4D9E399B06E6F6D5356FE851997D8EDCBB62C9C4093EF1DD7
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":1.628053515445502e+12,"network":1.628021116e+12,"ticks":7292186725.0,"uncertainty":3674473.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016151097"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\26495167-b134-466e-865b-51887d7d2fdd.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	98812
Entropy (8bit):	3.7498613465038586
Encrypted:	false
SSDEEP:	384:/fktBRPkGn0HnVgmNMN1rmv5D3a9TWH3SGVeprE3dZxTCazb3ar4Rmwr0TddtqOR:T6+J9i8GGge7VIvsnLGnK5XlRw
MD5:	932D8AEF9BBA3BD30F7CE427DE876EB1
SHA1:	D44F78C099A87C4ECD51804F59ADA6A847B25834
SHA-256:	A7C134D85675802AA2CC6456C46E13C5F66C11C9894B4AF38ABD888DABEAAC92
SHA-512:	E5DC5246DC44AFDC5E2D701BF89A6EDE2CFADA3B022110EF28C3C2D935A531779A92980C89F8853C344CC6B269B6118E1F89083F4C881EE898664A291779896
Malicious:	false
Reputation:	low
Preview:	.....*...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\303f087b-9bf1-4a00-baf0-3e261a3bbb10.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):	174334
Entropy (8bit):	6.079314854363426

C:\Users\user\AppData\Local\Google\Chrome\User Data\303f087b-9bf1-4a00-baf0-3e261a3bbb10.tmp

Encrypted:	false
SSDEEP:	3072:1S6GaYTJQE+mugy9+QV1T7IRwdfLSNPDFcbXafIB0u1GOJmA3iuRV:8/xaV+QfT7GSmhRaqfIlUOoSiuRV
MD5:	C0CBF96C80E3DE23314140B972A54EE3
SHA1:	08B7200FE8F66DCCBB9268A2E04021AD1C908B7D
SHA-256:	3D861868255045047B3E824C411951A5568680AD7C7FD75D93BAC7E6AF6EC7A7
SHA-512:	CB098DAFAC8AB2807035096959ABC696C6D3DCA47D40A81D97A92BC2A0CD90AFD2B3E695749FC7396E10C955542B44EBE1F1E1CDAA75A68BA1187453576959
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":1.628053515445502e+12,"network":1.628021116e+12,"ticks":7292186725.0,"uncertainty":3674473.0}},"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\59788342-fead-42dd-9085-d7b7ab8462e6.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):	165961
Entropy (8bit):	6.049777170123203
Encrypted:	false
SSDEEP:	3072:NGaYTJQE+mugy9+QV1T7IRwdfLSNPDFcbXafIB0u1GOJmA3iuRV:oxaV+QfT7GSmhRaqfIlUOoSiuRV
MD5:	1CA572C22258816170285E6A345F41DB
SHA1:	795C4BB4F0885BD3EDFCA6D53C0D31CD15ACD97B
SHA-256:	0698A0CD53B8524AF3F4AE31F81463ED06A0351CA630E1F3B1AB9851FA04E503
SHA-512:	F43FF83980A01EF29E717EFC1C709C6E1937FC19A100880A81BCCF7C1A99EDF985265E19D1871D10465ED7AAE65BA6B8632ECF2011167F93B1FBE9DB9909F41
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":1.628053515445502e+12,"network":1.628021116e+12,"ticks":7292186725.0,"uncertainty":3674473.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016151097"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\5f6f2481-8ff8-433d-87f3-4c0787206635.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96828
Entropy (8bit):	3.7495287279348983
Encrypted:	false
SSDEEP:	384:9fktBRPkGDHANMN1rmv5D3a9TWH3SGVeprE3dZxTCazb3ar4Rmwr0TddtqOX3dNW:Q+J9i8GGge7VIvsnLGnK5XlRv
MD5:	175A7A060F4DD1582C15B18358AE26F1
SHA1:	2633FA86CCD62C9F8F5F062CEB34C889C5984191
SHA-256:	72C2C4D308DEAD748A64649E3195F80D0B27231985057E14AF454F7E816CE5C1
SHA-512:	B8CBC33A7D18C43630FE91E239030717DA297F182367FC6B652C603D2E6739756793EEA866E5D660E0BF560DD28BA71A0BC1C43B19D15E18B7EDD30A47AA768E
Malicious:	false
Reputation:	low
Preview:	8z.....*...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\6b5e0a33-e260-4c6d-84dc-1242d536e488.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):	165961
Entropy (8bit):	6.049777170123203

C:\Users\user\AppData\Local\Google\Chrome\User Data\6b5e0a33-e260-4c6d-84dc-1242d536e488.tmp	
Encrypted:	false
SSDEEP:	3072:NGaYTJQE+mugy9+QV1T7IRwdfLSNPDFcbXafIB0u1GOJmA3iuRV:oxaV+QfT7GSmhRaqfIlUOoSiuRV
MD5:	1CA572C22258816170285E6A345F41DB
SHA1:	795C4BB4F0885BD3EDFCA6D53C0D31CD15ACD97B
SHA-256:	0698A0CD53B8524AF3F4AE31F81463ED06A0351CA630E1F3B1AB9851FA04E503
SHA-512:	F43FF83980A01EF29E717EFC1C709C6E1937FC19A100880A81BCCF7C1A99EDF985265E19D1871D10465ED7AAE65BA6B8632ECF2011167F93B1FBE9DB9909F41
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":1.628053515445502e+12,"network":1.628021116e+12,"ticks":7292186725.0,"uncertainty":3674473.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016151097"},"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\000002.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Xv:1qIF/
MD5:	206702161F94C5CD39FADD03F4014D98
SHA1:	BD8BFC144FB5326D21BD1531523D9FB50E1B600A
SHA-256:	1005A525006F148C86EFCBFB36C6EAC091B311532448010F70F7DE9A68007167
SHA-512:	0AF09F26941B11991C750D1A2B525C39A8970900E98CBA96FD1B55DBF93FEE79E18B8AAB258F48B4F7BDA40D059629BC7770D84371235CDB1352A4F17F80E145
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000002.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2039
Entropy (8bit):	6.097483380031221
Encrypted:	false
SSDEEP:	24:KqX9Y8DPZu1jQc5NL62X9BzXj1k76Fm30X9Y8DPZu1jQc5NL62X9BzXj177lbn0h:KQxuBQW5k76A+xuBQW577lbnrbn624vH
MD5:	6ADE9A05C20066D05DAA7DC7681B7EBC
SHA1:	6C7C2D7451BA2416B9DD651F91DAF82DC92DF648
SHA-256:	E09FB87D2FF5890AB8571D16318EF43C65BDB9A479560D2FA365218DCBA10747
SHA-512:	4E91CB9F90610132AF374492AAB21B9F6802A80E0779ACF830FAA3C26E3988B5C3543FD456663F0EFABD30D2A475DB2A7FE38D195970DE7929FA62D235C4AE7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000003.log	
Preview:	.t.._...............-download,710d8785-46a6-459b-b53c-3471ee47e8b0......$710d8785-46a6-459b-b53c-3471ee47e8b0..............."...vhttps://ballardagency-my.sharepoint.com/:u:/p/linda_davidson/EUJ1_psy-lhNg86-55dcNsUB8Ohn7k8q2Vtm1Wl6wQekUA?download=1...https://ballardagency-my.sharepoint.com/personal/linda_davidson_ballardagency_com/Documents/Invoice%20revised%20000101%20and%20Proposal.html?originalPath=aHR0cHM6Ly9iYWxsYXJkYWdlbmN5LW15LnNoYXJlcG9pbnQuY29tLzp1Oi9wL2xpbmRhX2Rhdmlkc29uL0VVSjFfcHN5LWxoTmc4Ni01NWRjTnNVQjhPaG43azhxMlZ0bTFXbDZ3UWVrVUE_cnRpbWU9bTVZM0E3cFcyVWc...."vhttps://ballardagency-my.sharepoint.com/:u:/p/linda_davidson/EUJ1_psy-lhNg86-55dcNsUB8Ohn7k8q2Vtm1Wl6wQekUA?download=1*.0.B*"{9BFE7542-FA32-4D58-83CE-BEE7975C36C5},1"J.Tue, 03 Aug 2021 19:25:03 GMTP.Z.text/htmlb.text/htmlj.........r.........x..7.W................-download,710d8785-46a6-459b-b53c-3471ee47e8b0......$710d8785-46a6-459b-b53c-3471ee47e8b0.............."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\091bdd2a-4868-44f6-b777-0c08a4a17890.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):	5502
Entropy (8bit):	5.185380280129326
Encrypted:	false
SSDEEP:	96:nmC2Tt95QmMrvcKIHok0JCKL8LbOTQVuwn:nmCS9Gjco4K8
MD5:	0E2E95FA2C91C04B6AD501B15CBF694F
SHA1:	AFD9CBD82854244A21DC832ED0D3268AF246C277
SHA-256:	F1BAD84E9CF98A1FD5A00BA5285D80744B11F3692A30D3DDCE998617D0466DA0
SHA-512:	58D1A8FBC7B53AE6E20888FEE97739A3338B309C5A0037749722CF1BD4A6772846BF5FC0C1EEE31ADF4C8D6E1B22C01032F5F2A36AD41299627E5CD7266119F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272527113400851","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\236ef2f3-ec28-41f8-ab4f-df480ebb3f97.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\37a75690-c891-4ee7-bbdb-79f995aa8d57.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22594
Entropy (8bit):	5.535320755351335
Encrypted:	false
SSDEEP:	384:iEvntwLlLFX+1kXqKf/pUZNCgVLH2HfDerUyHGLnTLOZ9P4R:eLld+1kXqKf/pUZNCgVLH2HfyrUyGLnv
MD5:	8247ED0691CC36D0FC360560D44C5852
SHA1:	A217D80E81F503AC818B049D66710BE50A1A0D4D
SHA-256:	414EF02B7D8545BD8DEF740DCDA2EE2D9D90E9C188441EC4EE031E00C9E8930C
SHA-512:	DE317E0DDA1D133E0A4BE0AB33FC1D3CF5FC786F5930A0185B258C5A5046139ED54185EF97EBC5CB45A6FD850639E88D6AF79094430CEF3046570187E3D0A86
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\37a75690-c891-4ee7-bbdb-79f995aa8d57.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272527113143131","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\596634fa-2fb1-445a-8b42-bf45619ff6e8.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):	2369
Entropy (8bit):	4.89521948478653
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5s8RLswTsDsSers4yKsK3zsuuzsyMHPpYhbD:JTnOCXGDHzPr75tTrOGP2hH
MD5:	492415A68B46C96E02F42DA89C281FB4
SHA1:	74B9C8E4B29B00AF2D4539E36105F65ECF8437F7
SHA-256:	C21A5FB2FFF87A24853557FC502D3EE67FC668C281BF07E288C18402FCE6982E
SHA-512:	8BDD099FE263A3F91CFC1D52180AA2D2252CD943C4305E5FE47B01B8DAFBFFE8EF832B22D2DE7B383AF0FC567A4CAFB31510AB69488C6E3F4752F82C04EB91 43
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275119116654373","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275119116702849","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5dd3cf20-761b-4f26-9b59-86b8f081c743.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):	5476
Entropy (8bit):	5.1828268257789265
Encrypted:	false
SSDEEP:	96:nmC2qt95QmMrvcKIHok0JCKL8VbOTQVuwn:nmCN9Gjco4K6
MD5:	8F8DDD40CA69745F07479AAF79F860E3
SHA1:	176E1319B576E9AC16821957D5E0EEF4E8904FC0
SHA-256:	ECDF533780F51DE6F847926F53DCE5E8F4164E9284425DE40D38C4E5A9E30AB1
SHA-512:	E48E0F46486FA71773468DA4DE60EA73B6AB837D5B4E277BDA03695CF3A495BA0AB3952AB4FCE9AEFB1EA3BE7F4EEE332FF0E595D13BA71062F7C9E0DA3E7 019
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272527113400851","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\6456bb93-f7e6-4adb-92df-56b0c81d75f5.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 F21
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6456bb93-f7e6-4adb-92df-56b0c81d75f5.tmp	
Preview:	.

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):	5.258079172956519
Encrypted:	false
SSDEEP:	6:m/rq2PWXp+N23iKKdK9RXXTZIFUtp38XZmwP38FkwOWXp+N23iKKdK9RXX5LJ:yrva5Kk7XT2FUtp38X/P38F5f5Kk7XVJ
MD5:	2EC5D8133878A2707C508B53A8EC832B
SHA1:	2DB727AF547626A35FCAB94847AD59B8A1293C1E
SHA-256:	BC716EB0963F723C557C5A2EB714E2421E00548AC42EA02E0923AF6DC3ACE584
SHA-512:	E8BEFE0E7B89F41FDF684669E94526DC0999E93A91FDFDFA43DE050DF8D9B2A12E9971E1E4AF7CA162F0B7FCF5F11FFAA9902EB5EDDD661EADD3CAD0FE7EA624
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.798 1914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-22:05:18.799 1914 Recovering log #3.2021/08/03-22:05:18.799 1914 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):	5.258079172956519
Encrypted:	false
SSDEEP:	6:m/rq2PWXp+N23iKKdK9RXXTZIFUtp38XZmwP38FkwOWXp+N23iKKdK9RXX5LJ:yrva5Kk7XT2FUtp38X/P38F5f5Kk7XVJ
MD5:	2EC5D8133878A2707C508B53A8EC832B
SHA1:	2DB727AF547626A35FCAB94847AD59B8A1293C1E
SHA-256:	BC716EB0963F723C557C5A2EB714E2421E00548AC42EA02E0923AF6DC3ACE584
SHA-512:	E8BEFE0E7B89F41FDF684669E94526DC0999E93A91FDFDFA43DE050DF8D9B2A12E9971E1E4AF7CA162F0B7FCF5F11FFAA9902EB5EDDD661EADD3CAD0FE7EA624
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.798 1914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-22:05:18.799 1914 Recovering log #3.2021/08/03-22:05:18.799 1914 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):	5.258750275892141
Encrypted:	false
SSDEEP:	6:me0rq2PWXp+N23iKKdKyDZIFUtpRFkZmwPLkwOWXp+N23iKKdKyJLJ:wva5Kk02FUtpc/PL5f5KkWJ
MD5:	E4E4187C750F325FDFE4809B432053A6
SHA1:	C43C22BE8DB1BD78A574B4177922B31CF131D901
SHA-256:	4BF57072824C31920FD4AA70A5B96E03FCEADE85627AF3D2602A42526EA5DFDE
SHA-512:	304A6463A8E4E280EB79365035E00184E524AB105F5F479B805E2711CC96AF727004BFAF09A8870AFAFEFCD59FE0379F39FE29566EA75CE39A83A719CA0F6563
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.679 1914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-22:05:18.683 1914 Recovering log #3.2021/08/03-22:05:18.684 1914 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.258750275892141

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old (copy)	
Encrypted:	false
SSDEEP:	6:me0rq2PWXp+N23iKKdKyDZIFUtpRFkZmwPLkwOWXp+N23iKKdKyJLJ:wva5Kk02FUtpc/PL5f5KkWJ
MD5:	E4E4187C750F325FDFE4809B432053A6
SHA1:	C43C22BE8DB1BD78A574B4177922B31CF131D901
SHA-256:	4BF57072824C31920FD4AA70A5B96E03FCEADE85627AF3D2602A42526EA5DFDE
SHA-512:	304A6463A8E4E280EB79365035E00184E524AB105F5F479B805E2711CC96AF727004BFAF09A8870AFAFEFCD59FE0379F39FE29566EA75CE39A83A719CA0F6563
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.679 1914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-22:05:18.683 1914 Recovering log #3.2021/08/03-22:05:18.684 1914 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\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//Xv:1qIF/
MD5:	206702161F94C5CD39FADD03F4014D98
SHA1:	BD8BFC144FB5326D21BD1531523D9FB50E1B600A
SHA-256:	1005A525006F148C86EFCBFB36C6EAC091B311532448010F70F7DE9A68007167
SHA-512:	0AF09F26941B11991C750D1A2B525C39A8970900E98CBA96FD1B55DBF93FEE79E18B8AAB258F48B4F7BDA40D059629BC7770D84371235CDB1352A4F17F80E145
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000002.

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):	1.8691884774122303
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7UBqrHtJrlya0MYvqHazP5lsc:dNw4rHtRIa0bvq6zBlsc
MD5:	4949F8E15DA68EA77F08B7969806381F
SHA1:	7ABECACEB945BB2EC940B82C001CFA7DC48CD384
SHA-256:	14CE76579DD7F67610A3D4E86BF800183ACD9FC262C1B9BE1202703DB07C36C0
SHA-512:	FAC9F52764F442B68F3F881FBED0507A555C44218DDF42BB58A7D02953F9F3A936CD3147A75814D4647EF23523F2C22F3CE31086B9122A4E770FA060D2F9B934
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):	0.9686218256555883
Encrypted:	false
SSDEEP:	24:VcLgAZOZD/rqLbJLbXaFpEO5bNmISHn06Uwh8:V8NOZrq5LLOpEO5J/Kn7UO8
MD5:	3F5E2D142B72600710F0304966B9E2BE
SHA1:	BC809AD7A7C4346BB29DBFCF613B5DA8391635EC
SHA-256:	7A5680DA707B790A5F6574DE1CAE9C04A7C20909B337977AC67BBA3CF4D6F3C6
SHA-512:	039CE3D8C3681B6B2F2156D93589D8D8991F4BE5775014CF51321B8CE0CF25AF66E07AF97394AEB057C2F58A2BD171CCAEB1216E3FE8A87F284A4BE540483A8
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1738
Entropy (8bit):	3.4375358079054568
Encrypted:	false
SSDEEP:	24:34S2OlrlA/tZm5VwLHlXx+NgZu1we0h1LasQ1VHBL3S6jb6t+NgZu10bPlL:34axn5SQNEuM3BQ1Vd3S8NEuqJL
MD5:	9B6B76AB692D04AE8409D42B478C0818
SHA1:	5A137D7E47C8F94DA0938C0BA6DE193E86ACD77E
SHA-256:	5261E7E0CBDC623691DB627B4ADCD4AD22D04FF77153032A5B2C6E1A7F378DFD
SHA-512:	0C029501D23C3C4BD0258AF26C5034AFA841BCCE9800D35C0D5344D0D1CC6AA5DA7DDC1AEA47342B5C704ED1E34E387F0EC2E83F70564A6DD3C260C42DE3 D8
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...34507e19_ea7d_4604_be00_35c657d3dea6..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....!.....1.,.....$...9aac2de2_9297_484c_aad4 _8374825bfd65.....Bc.....Q...file:///C:/Users/user/Downloads/Invoice%20revised%20000101%20and%20Proposal.html.....S.i. g.n. .i.n.....h.....`.....B.....C.....Q...f.i.l.e.:././/.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.o.w.n. l.o.a.d.s./.l.n.v.o.i.c.e.%.2.0.r.e.v.i.s.e.d.%.2.0.0.0.0.1.0.1.%.2.0.a.n.d.%.2.0.P.r.o.p.o.s.a.l...h.t.m.l.....@.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Entropy (8bit):	5.179934379345752
Encrypted:	false
SSDEEP:	6:mGzu4q2PWXp+N23iKKdK8aPrqIFUtpTSDZZmwPTSDzkwOWXp+N23iKKdK8amLJ:DzNva5KkL3FUtpTOZ/PTOz5f5KkQJ
MD5:	820D3CADA1332AF5BD38CE6F38C7BF27
SHA1:	0B2A82C45878AE60BB6D4DCDBBA262949C1AD8D0
SHA-256:	BD95B617D02B863A69BD1D56EFF9BB4086A04E0AFDB9BC4E572FFF50C8B5507F
SHA-512:	0D72C9452C3EC0F5526C1A3499F77B1EDFAAC7D9E671743F55E9B4E84C84F70D4863DE16C05A7A34CD602DCA3BCB5C79715AC13190555CDDB33652D91E034A F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.409 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-22 :05:13.410 3e4 Recovering log #3.2021/08/03-22:05:13.410 3e4 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):	317
Entropy (8bit):	5.179934379345752
Encrypted:	false
SSDEEP:	6:mGzu4q2PWXp+N23iKKdK8aPrqIFUtpTSDZZmwPTSDzkwOWXp+N23iKKdK8amLJ:DzNva5KkL3FUtpTOZ/PTOz5f5KkQJ
MD5:	820D3CADA1332AF5BD38CE6F38C7BF27
SHA1:	0B2A82C45878AE60BB6D4DCDBBA262949C1AD8D0
SHA-256:	BD95B617D02B863A69BD1D56EFF9BB4086A04E0AFDB9BC4E572FFF50C8B5507F
SHA-512:	0D72C9452C3EC0F5526C1A3499F77B1EDFAAC7D9E671743F55E9B4E84C84F70D4863DE16C05A7A34CD602DCA3BCB5C79715AC13190555CDDB33652D91E034A F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.409 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-22 :05:13.410 3e4 Recovering log #3.2021/08/03-22:05:13.410 3e4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....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):	5.179756049881876
Encrypted:	false
SSDEEP:	6:m4XdXVN4q2PWXp+N23iKKdK8NIFUtpjX8v3JZmwPjXtyDkwOWXp+N23iKKdK8+ed:rN4va5KkpFUtpyJ/PZyD5f5KkqJ
MD5:	F5564CCD9A29A32748FF61D7DFE1E7B9
SHA1:	A92D5E0EE57BB05B930CCD8618E831C388EECEB6
SHA-256:	E8822B0BD3C6C5A75E52438D8A2F38DCAB09A92A91AC543E86FEE8C5DBB87661
SHA-512:	80BC108209C57C8F4A38D5E9E0E8F369317C018923D6CDC42BBBF5C6BC9AD254CAC4CE95EEBBD152CD4F3AC10AF6EFE93590241AFF0699B2751EB69B44373 E6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:16.326 1320 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-22:05:16.327 1320 Recovering log #3.2021/08/03-22:05:16.329 1320 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.oldS (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.179756049881876
Encrypted:	false
SSDEEP:	6:m4XdXVN4q2PWXp+N23iKKdK8NIFUtpjX8v3JZmwPjXtyDkwOWXp+N23iKKdK8+ed:rN4va5KkpFUtpyJ/PZyD5f5KkqJ
MD5:	F5564CCD9A29A32748FF61D7DFE1E7B9
SHA1:	A92D5E0EE57BB05B930CCD8618E831C388EECEB6
SHA-256:	E8822B0BD3C6C5A75E52438D8A2F38DCAB09A92A91AC543E86FEE8C5DBB87661
SHA-512:	80BC108209C57C8F4A38D5E9E0E8F369317C018923D6CDC42BBBF5C6BC9AD254CAC4CE95EEBBD152CD4F3AC10AF6EFE93590241AFF0699B2751EB69B44373E6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:16.326 1320 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-22:05:16.327 1320 Recovering log #3.2021/08/03-22:05:16.329 1320 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
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):	16384
Entropy (8bit):	1.386557222932722
Encrypted:	false
SSDEEP:	48:yBmw6fUoNEuSusa3P9a186/gta7gNEuA9:yBCfNFyE9IV0NFa
MD5:	7215CFF6657A147406D4562DAF116CBC
SHA1:	A69D7D56CAC067D9DDD24FA34F253213B79F9854
SHA-256:	C2A2275F19B2A58993156426E77BEBE1F89CAA080EB0B2E9F26E458B02F52943
SHA-512:	4669FC53352B7BAD681CBD27D8AD88043D38C9D0C274F2F8FE8AD5A1AADA32A214017F541BEC4E8AF3FDFC26A0997E921CB2B39A406D26062BAF6BAD5C29B59
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.778375471873636
Encrypted:	false
SSDEEP:	24:GzSyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwycM3n:oSdBmw6fU33n
MD5:	C88DB68DC81205DB7E81435A5A3D797C
SHA1:	E47C0193D78AE0660D9E3CA34F7C62B8F397AA1E
SHA-256:	1635DC512E395F99B1B34B5B6141A5B5A1972226EA1E2F049A65CF25948FB2E6
SHA-512:	B24936A6C1212D9A3B74B2702A93E6A7BF8A6D7B2A4CB00FDCE2BAB01DC09E3CB8CA63A37358EE099D2B4328BB1A77C54AC6D58610515154B1485E2EDD0A4B5F
Malicious:	false
Reputation:	low
Preview:	.....8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.29306551151048
Encrypted:	false
SSDEEP:	6:mNcZq2PWXp+N23iKKdK25+Xqx8chI+IFUtp0ZZmwPTkwOWXp+N23iKKdK25+Xqx7:6cZva5KkTXfchI3FUtpI/PT5f5KkTXfE
MD5:	6717AD8CAAF6F7B0AAA77A72FDEE427E
SHA1:	FE9232F3F310ABBDC0153AF838E4605EBB44B80E
SHA-256:	7C0A15AA04F09DDA63584F20B9D4084B5B3A5DEEA860D57A05049AE6631FAE1C
SHA-512:	6EDBBC2E5944FA253F9FA2D76D256B73EF167B9CF60FED59D736AB8ADCCE76C5416805747D94FF27505A114C6D88A9D431376FE171A6B7A9F798A65678A9E94
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.661 1914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-22:05:18.665 1914 Recovering log #3.2021/08/03-22:05:18.666 1914 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.oldN (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.29306551151048
Encrypted:	false
SSDEEP:	6:mNcZq2PWXp+N23iKKdK25+Xqx8chI+IFUtp0ZZmwPTkwOWXp+N23iKKdK25+Xqx7:6cZva5KkTXfchI3FUtpI/PT5f5KkTXfE
MD5:	6717AD8CAAF6F7B0AAA77A72FDEE427E
SHA1:	FE9232F3F310ABBDC0153AF838E4605EBB44B80E
SHA-256:	7C0A15AA04F09DDA63584F20B9D4084B5B3A5DEEA860D57A05049AE6631FAE1C
SHA-512:	6EDBBC2E5944FA253F9FA2D76D256B73EF167B9CF60FED59D736AB8ADCCE76C5416805747D94FF27505A114C6D88A9D431376FE171A6B7A9F798A65678A9E94
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.661 1914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-22:05:18.665 1914 Recovering log #3.2021/08/03-22:05:18.666 1914 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):	5.249832520565134
Encrypted:	false
SSDEEP:	6:maojlq2PWXp+N23iKKdK25+XuoIFUtpDyZmwPDJFzkwOWXp+N23iKKdK25+XuxWd:cjlva5KkTXYFUtpe/PFF5f5KkTXHJ
MD5:	7B69C0428B1C3DE258E9B184E34B4C97
SHA1:	D744F8CFEA97B9C33CA0774A7E68F6E62485FEF1
SHA-256:	B4CDF39AA25587DAF05E78AC3DB782147DA45AF361B8655F0D83C0675C77AB03
SHA-512:	2AF175EBB7E399C7F445ABA7903DC70AA42D5A6FA93257BED8EEDF51BE19ADD74B05FAADF7E763CF9BC86CA7EB58EDF262B9A4D30DC743BED548070152B74DFF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.632 1914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-22:05:18.634 1914 Recovering log #3.2021/08/03-22:05:18.635 1914 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.249832520565134
Encrypted:	false
SSDEEP:	6:maojlq2PWXp+N23iKKdK25+XuoIFUtpDyZmwPDJFzkwOWXp+N23iKKdK25+XuxWd:cjlva5KkTXYFUtpe/PFF5f5KkTXHJ
MD5:	7B69C0428B1C3DE258E9B184E34B4C97
SHA1:	D744F8CFEA97B9C33CA0774A7E68F6E62485FEF1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
SHA-256:	B4CDF39AA25587DAF05E78AC3DB782147DA45AF361B8655F0D83C0675C77AB03
SHA-512:	2AF175EBB7E399C7F445ABA7903DC70AA42D5A6FA93257BED8EEDF51BE19ADD74B05FAADF7E763CF9BC86CA7EB58EDF262B9A4D30DC743BED548070152B74DFF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.632 1914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-22:05:18.634 1914 Recovering log #3.2021/08/03-22:05:18.635 1914 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):	5.257396017802679
Encrypted:	false
SSDEEP:	6:mweOq2PWXp+N23iKKdKWT5g1IdqIFUtpXZZmwPvFEkwOWXp+N23iKKdKWT5g1I3e:lrva5Kkg5gSRFUtpXZ/Pq5f5Kkg5gS3e
MD5:	8922BA0FC05A6D9FA08BCABA82036187
SHA1:	65F3BB301320ACCA9C6D90C2C6252A5D42304B51
SHA-256:	79D9873E2413D72AF69FCA3BCFFD6AE07DF7DE3761ED1F03373B0ADEE63DE997
SHA-512:	4DB627E501A8D3BBAEA97B66A52AFC1F7E888B197D206E00B32A0DAC136D0DF5F5A67DB8F520D85788571783C99DACC6D28A14D6CDF47EAB28AB8D655BCFD91E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.621 1914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-22:05:18.622 1914 Recovering log #3.2021/08/03-22:05:18.623 1914 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.oldn (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.257396017802679
Encrypted:	false
SSDEEP:	6:mweOq2PWXp+N23iKKdKWT5g1IdqIFUtpXZZmwPvFEkwOWXp+N23iKKdKWT5g1I3e:lrva5Kkg5gSRFUtpXZ/Pq5f5Kkg5gS3e
MD5:	8922BA0FC05A6D9FA08BCABA82036187
SHA1:	65F3BB301320ACCA9C6D90C2C6252A5D42304B51
SHA-256:	79D9873E2413D72AF69FCA3BCFFD6AE07DF7DE3761ED1F03373B0ADEE63DE997
SHA-512:	4DB627E501A8D3BBAEA97B66A52AFC1F7E888B197D206E00B32A0DAC136D0DF5F5A67DB8F520D85788571783C99DACC6D28A14D6CDF47EAB28AB8D655BCFD91E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.621 1914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-22:05:18.622 1914 Recovering log #3.2021/08/03-22:05:18.623 1914 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	296
Entropy (8bit):	0.4481240366544235
Encrypted:	false
SSDEEP:	3:8EflA:81
MD5:	61EFE25511775F0C64C5A5D883AFA171
SHA1:	0BC3916B2B4EAB8859F5337F69093A98B468625C
SHA-256:	A9A694FCC1C0F85AB1C88DFB40374DD55775C8B5652E889133B78BA1AD565794
SHA-512:	6C4040BB694CE72C04CDBD0AAF0DE45295BAC9B6A4E9D6B0F58346BBC7935569428C3F966DCE9A45AAE3CC65F7430E5D6319B5AC2417063ACA3B9141563880B
Malicious:	false
Reputation:	low
Preview:	.'..(.....A..K'/ .....

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):	45056
Entropy (8bit):	0.3515382763288945
Encrypted:	false
SSDEEP:	24:TLxbR4kyW4ky1uX9vEN6CDPZu1jQc5NL6EX9RX5V+NgZu1MZuxR+NgZu10:TVGFSGN6MuBQoD5cNEutxgNEuK
MD5:	18BDA54D19511AAE93ED963E2AE13026
SHA1:	8714483E827442302863C19F3744CAC2DA5F4586
SHA-256:	F7BDBAB207EC370221D3DDEB77CA13F85BBBFB79115848C4CFA035D331465706
SHA-512:	603B55DD3980824CA8742F5EC3A4C9CCB98765C50881B0A1E6CE262ADE016821117F2696C3ADAD88461953543C47D25A4A0075581777B3F387D93132B03A4FC3
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

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):	54912
Entropy (8bit):	0.10154081527827694
Encrypted:	false
SSDEEP:	12:hlil9zlu3lkl+WqLBj/Pt7lCSj30aGS0sB4nMWQA9LfBQZ8fOFn:2llqLBPthnqbNfTfln
MD5:	8191EFDDE6567A9883C307D2AFD0C76C
SHA1:	5B4F0BE175FF902E1EADA44DE544D3B09D33956D
SHA-256:	343318592F47702D624015CD8929031F55582A76E767E047DD76A381C347E405
SHA-512:	D3BF98C7A738AA183E369776A0192FCF9FB6A4A7215C76D7EF6BE4FD2B3914E323DD2C4580E68AC163D00F45426A24EE14759D2D869755D5274938C928E3E5A1
Malicious:	false
Reputation:	low
Preview:	.....).4<..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.266977196801593
Encrypted:	false
SSDEEP:	3:tUK6c+l7WFv:ma+hg
MD5:	8D8A70AC9A876BBB5CF04BCF7A4B725D
SHA1:	608AA06FAD9132660B4EB127E0CF9C3BD97CAC46
SHA-256:	F6065C19675E8A5A99376B021CE26CC47B662EED7AD132D58FC0B21DA9CA3469
SHA-512:	EF05932E7A56C2011917C29C04780A76C07A7551E074C2E9E13DD9841E15D8B503757C255FE616E1D86E4BFC3482EA29294C2E92CC9B07E69D686F93BEE05C0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:17.238 d5c Delete type=3 #1.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session` (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1738
Entropy (8bit):	3.4375358079054568
Encrypted:	false
SSDEEP:	24:34S2OlrlA/tZm5VwLHlXx+NgZu1we0h1LasQ1VHBL3S6jb6t+NgZu10bPlL:34axn5SQNEuM3BQ1Vd3S8NEuqJL
MD5:	9B6B76AB692D04AE8409D42B478C0818
SHA1:	5A137D7E47C8F94DA0938C0BA6DE193E86ACD77E
SHA-256:	5261E7E0CBDC623691DB627B4ADCD4AD22D04FF77153032A5B2C6E1A7F378DFD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session` (copy)	
SHA-512:	0C029501D23C3C4BD0258AF26C5034AFA841BCCE9800D35C0D5344D0D1CC6AA5DA7DDC1AEA47342B5C704ED1E34E387F0EC2E83F70564A6DD3C260C42DE3 D8
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...34507e19_ea7d_4604_be00_35c657d3dea6..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....!.....1.,.....$...9aac2de2_9297_484c_aad4 _8374825bfd65.....Bc.....Q...file:///C:/Users/user/Downloads/Invoice%20revised%20000101%20and%20Proposal.html.....S.i. g.n. .i.n.....h.....`.....B.....C.....Q...f.i.l.e.:././/.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.o.w.n. l.o.a.d.s./.l.n.v.o.i.c.e.%.2.0.r.e.v.i.s.e.d.%.2.0.0.0.0.1.0.1.%.2.0.a.n.d.%.2.0.P.r.o.p.o.s.a.l...h.t.m.l.....@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last TabsOG (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):	5.45557446133023
Encrypted:	false
SSDEEP:	48:hA1sGo0wkna7znMPq8db357L+bQSefgGPNrS0U9RdiN9pX:+oLkna7znMPpdb357L+bQ5fgG1rS0L
MD5:	538183B9650EFA0DDA0C91F2902931D7
SHA1:	3947921F53FD1AAE580E74181FA21B61211DF9C1
SHA-256:	A944582A5B6CB9E71246BB6FB9CDC147010C372A90BFFC9A3042DBB894E8E300
SHA-512:	C502BD0B6743B5B99DE353AA5E1567660B7EAD32E7E1B774B9985E1FC5EBE39E9C7E34F72F4991A805DA0D5FDF74944849F0694B6E382666B0900111879BCFA6
Malicious:	false
Reputation:	low
Preview:	<x.....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutS inkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast. RequestIdGenerator..337089000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 22:05:20.30][INFO][mr.Init] MR instance ID: 47900605-1f8c-4dc6-bcfe-7d1603517e82\n","[2021-08-03 22:05:20.30][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 22:05:20.30][INFO][m r.Init] Native Mirroring Service is enabled.\n","[2021-08-03 22:05:20.30][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 22:05 :20.30][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 22:05:20.30][INFO][mr.CastProvider] Query enabled: true\n","[2021- 08-03 22:05:20.30][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):	329
Entropy (8bit):	5.195975977909585
Encrypted:	false
SSDEEP:	6:mGpq2PWXp+N23iKKdK8a2jMGIFUtpTlZmwPTuFPkwOWXp+N23iKKdK8a2jMmLJ:Dpva5Kk8EFUtpTl/PTuh5f5Kk8bJ
MD5:	D89CA1B042A35FF2A2DE7E14C2102C41
SHA1:	AD1F29D755C62A8841CA3591618F2518F5F9B3BD
SHA-256:	13C287ED9B352DF4F9999DEE32EB91AAE5402518B8183FC746E0F090B6898CCF
SHA-512:	A7D57CE6AAE4BA44E34B1CC7BDB3D882A6696C8FD3F22932EAB4C0A8DC78312828ECB03C0FC5780E096C36440B5168BAF5D656AFC4E78A7E07CFF904145B1A 79
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Preview:	2021/08/03-22:05:13.188 d44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:05:13.189 d44 Recovering log #3.2021/08/03-22:05:13.191 d44 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):	329
Entropy (8bit):	5.195975977909585
Encrypted:	false
SSDEEP:	6:mGpq2PWXp+N23iKKdK8a2jMGIFUtpTlZmwPTuFPkwOWXp+N23iKKdK8a2jMmLJ:Dpva5Kk8EFUtpTl/PTuh5f5Kk8bJ
MD5:	D89CA1B042A35FF2A2DE7E14C2102C41
SHA1:	AD1F29D755C62A8841CA3591618F2518F5F9B3BD
SHA-256:	13C287ED9B352DF4F9999DEE32EB91AAE5402518B8183FC746E0F090B6898CCF
SHA-512:	A7D57CE6AAE4BA44E34B1CC7BDB3D882A6696C8FD3F22932EAB4C0A8DC78312828ECB03C0FC5780E096C36440B5168BAF5D656AFC4E78A7E07CFF904145B1A79
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.188 d44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:05:13.189 d44 Recovering log #3.2021/08/03-22:05:13.191 d44 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\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAIxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C235B
Malicious:	false
Reputation:	low
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\MANIFEST-000002	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	4.948758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVqU0blS:oO7iblS
MD5:	22BF0E81636B1B45051B138F48B3D148
SHA1:	56755D203579AB356E5620CE7E85519AD69D614A
SHA-256:	E292F241DAAFC3DF90F3E2D339C61C6E2787A0D0739AAC764E1EA9BB8544EE97
SHA-512:	A4CF1F5C74E0DF85DDA8750BE9070E24E19B8BE15C6F22F0C234EF8423EF9CA3DB22BA9EF777D64C33E8FD49FADA6FCCA26C1A14BA18E8472370533A1C65DD0
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State. (copy)	
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\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):	2369
Entropy (8bit):	4.89521948478653
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5s8RLswTsDsSers4yKsK3zsuuzsyMHPpYhbD:JTnOCXGDHzPr75tTrOGP2hH
MD5:	492415A68B46C96E02F42DA89C281FB4
SHA1:	74B9C8E4B29B00AF2D4539E36105F65ECF8437F7
SHA-256:	C21A5FB2FFF87A24853557FC502D3EE67FC668C281BF07E288C18402FCE6982E
SHA-512:	8BDD099FE263A3F91CFC1D52180AA2D2252CD943C4305E5FE47B01B8DAFBFFE8EF832B22D2DE7B383AF0FC567A4CAFB31510AB69488C6E3F4752F82C04EB9143
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275119116654373","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275119116702849","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.200369503449517
Encrypted:	false
SSDEEP:	6:mGXYVq2PWXp+N23iKKdKgXz4rRIFUtpTSSgZmwPTSSIkwOWXp+N23iKKdKgXz4qG:DQva5KkgXiuFUtpTSX/PTSF5f5KkgX2J
MD5:	317E90DFBCE7DA97A1F31E17268057B7
SHA1:	54D0914860A416048C463AF1D2052CB12D695CCE
SHA-256:	11ED7CDAECE1BCD6738E551D699DCD3192F6BE2F6535870A3E38C5F262195AED
SHA-512:	17824A75512F5CD5A8F6696BDC4B0B8BCEF0F8545DDDF713789296BFDCE6711E847B5304835806F7008970EF0C10355EC2438B72140A17799EABA1FBBAC322A5
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.435 ff0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-22:05:13.436 ff0 Recovering log #3.2021/08/03-22:05:13.436 ff0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.200369503449517
Encrypted:	false
SSDEEP:	6:mGXYVq2PWXp+N23iKKdKgXz4rRIFUtpTSSgZmwPTSSIkwOWXp+N23iKKdKgXz4qG:DQva5KkgXiuFUtpTSX/PTSF5f5KkgX2J
MD5:	317E90DFBCE7DA97A1F31E17268057B7
SHA1:	54D0914860A416048C463AF1D2052CB12D695CCE
SHA-256:	11ED7CDAECE1BCD6738E551D699DCD3192F6BE2F6535870A3E38C5F262195AED
SHA-512:	17824A75512F5CD5A8F6696BDC4B0B8BCEF0F8545DDDF713789296BFDCE6711E847B5304835806F7008970EF0C10355EC2438B72140A17799EABA1FBBAC322A5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.435 ff0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-22:05:13.436 ff0 Recovering log #3.2021/08/03-22:05:13.436 ff0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notific ations/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):	5502
Entropy (8bit):	5.185380280129326
Encrypted:	false
SSDEEP:	96:nmC2Tt95QmMrvcKIHok0JCKL8LbOTQVuwn:nmCS9Gjco4K8
MD5:	0E2E95FA2C91C04B6AD501B15CBF694F
SHA1:	AFD9CBD82854244A21DC832ED0D3268AF246C277
SHA-256:	F1BAD84E9CF98A1FD5A00BA5285D80744B11F3692A30D3DDCE998617D0466DA0
SHA-512:	58D1A8FBC7B53AE6E20888FEE97739A3338B309C5A0037749722CF1BD4A6772846BF5FC0C1EEE31ADF4C8D6E1B22C01032F5F2A36AD41299627E5CD7266119F
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272527113400851","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.1211183826243067
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU1UQ0rsGoTRsCH:wIElwQF8mpcSxAYVSYTc8cIl1
MD5:	76A59C1D65F588DE984D61B03CEA13B7
SHA1:	9877ADC79BBEDFAF031EBCA8F93FF48C2FD9BF23
SHA-256:	9237E007BD71F88B6D6B35CC1FF95BA4E10DDAF150D86219314485B288E8FD89
SHA-512:	4CD69D2D339E069AD1A39CAC9B7106C385DF327C9A6FFE6D6AAB00CE303FE1645425477F91C4089610619399462784D76E7545629F67C9C1B92896DBC866E8D5
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):	29252
Entropy (8bit):	0.6285572987397579
Encrypted:	false
SSDEEP:	48:58qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU/4:58hIElwQF8mpcSU
MD5:	D1AE885CA9A31F1A259E5902D248CABD
SHA1:	25FB55C7F2B58095FEC23A9A359467A967C6DFD6
SHA-256:	770FCAAABB03C029A13760833C783847959C2877C9D77644DA4732B6440A06E8
SHA-512:	CF91682FF8D810E782F0F91CC28B4636DFC37368F2D95AC489B36CADB261126AEBA709290D335ABB71648DE7ED4436C1C9F0AB1448FF1E3D2812DFDBE1AC57 0
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):	22594
Entropy (8bit):	5.535320755351335
Encrypted:	false
SSDEEP:	384:iEvntwLlLFX+1kXqKf/pUZNCgVLH2HfDerUyHGLnTLOZ9P4R:eLld+1kXqKf/pUZNCgVLH2HfyrUyGLnv
MD5:	8247ED0691CC36D0FC360560D44C5852
SHA1:	A217D80E81F503AC818B049D66710BE50A1A0D4D
SHA-256:	414EF02B7D8545BD8DEF740DCDA2EE2D9D90E9C188441EC4EE031E00C9E8930C
SHA-512:	DE317E0DDA1D133E0A4BE0AB33FC1D3CF5FC786F5930A0185B258C5A5046139ED54185EF97EBC5CB45A6FD850639E88D6AF79094430CEF3046570187E3D0A86
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":"13272527113143131","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\Secure PreferencesTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535240768504845
Encrypted:	false
SSDEEP:	384:iEvntRLlLFX+1kXqKf/pUZNCgVLH2HfDerUyHGsnTLmEP4D:PLld+1kXqKf/pUZNCgVLH2HfyrUyGsnm
MD5:	F264EB198F1BB7A463EC7FF4D5D15311
SHA1:	12C2A0DBD18029EFF0EFD9B7927223BCBBC70055
SHA-256:	1506F88C37505609F1E946CA862EF3C7EB1174BF262579E9F842EB726966FF9F
SHA-512:	421CC4D275749DD3360BF62AA514E0E5BA4AE1E250160CE2232B4802BFB8B7DDCAE964F0B5D832466317FD697F641087011C5A132F9374C5C61BA9E2946828CI
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":"13272527113143131","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.198584438337386

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Encrypted:	false
SSDEEP:	6:mGRUVq2PWXp+N23iKKdKrQMxIFUtpTEgZmwPT8RSIkwOWXp+N23iKKdKrQMFLJ:DRsva5KkCFUtpTt/PTAF5f5KktJ
MD5:	FCC6906B2A24C7AE73188CE66C3B0AF1
SHA1:	51EFAD77841385634685D60E51302DF51F6FBFE6
SHA-256:	8AD6D29EC331DDFE0DDA93581673822EF1CD72B47C9E4505DAF01313546B0A2A
SHA-512:	C9462509F02F95DB985E59C45B7CE726BA634F426FEA1781A0FBEF31D5CCA305559CA726EA2A90BC802CCED6573DEBD6E9A3DE185AE69A7C43EE748FDA51ED9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.353 14b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-22:05:13.355 14b4 Recovering log #3.2021/08/03-22:05:13.356 14b4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.198584438337386
Encrypted:	false
SSDEEP:	6:mGRUVq2PWXp+N23iKKdKrQMxIFUtpTEgZmwPT8RSIkwOWXp+N23iKKdKrQMFLJ:DRsva5KkCFUtpTt/PTAF5f5KktJ
MD5:	FCC6906B2A24C7AE73188CE66C3B0AF1
SHA1:	51EFAD77841385634685D60E51302DF51F6FBFE6
SHA-256:	8AD6D29EC331DDFE0DDA93581673822EF1CD72B47C9E4505DAF01313546B0A2A
SHA-512:	C9462509F02F95DB985E59C45B7CE726BA634F426FEA1781A0FBEF31D5CCA305559CA726EA2A90BC802CCED6573DEBD6E9A3DE185AE69A7C43EE748FDA51ED9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.353 14b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-22:05:13.355 14b4 Recovering log #3.2021/08/03-22:05:13.356 14b4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.161172045318285
Encrypted:	false
SSDEEP:	6:mGgt4q2PWXp+N23iKKdK7Uh2ghZIFUtpTKVNJZmwPTKVNDkwOWXp+N23iKKdK7UT:DHva5KklhHh2FUtpTKVX/PTKVF5f5Kks
MD5:	A3051C54BAA8DF59398092E68FBB5939
SHA1:	E28753E86F70253F105B1F1905F09432499CC813
SHA-256:	E09A16D941223C2C0F70B4DF644A95C0F930B3C44DC8B8496CD95BDFF868433A
SHA-512:	0717D7F6D1735C23AD2FEE5570D3BFC0F1DEC5DCBAA80A9A55A936D66B5B1ECF44F014E71B19DFA9C406F2A753D607BB8251612901DFDCBE8C79A0FC08007FE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.167 1280 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-22:05:13.174 1280 Recovering log #3.2021/08/03-22:05:13.174 1280 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.161172045318285
Encrypted:	false
SSDEEP:	6:mGgt4q2PWXp+N23iKKdK7Uh2ghZIFUtpTKVNJZmwPTKVNDkwOWXp+N23iKKdK7UT:DHva5KklhHh2FUtpTKVX/PTKVF5f5Kks
MD5:	A3051C54BAA8DF59398092E68FBB5939
SHA1:	E28753E86F70253F105B1F1905F09432499CC813
SHA-256:	E09A16D941223C2C0F70B4DF644A95C0F930B3C44DC8B8496CD95BDFF868433A
SHA-512:	0717D7F6D1735C23AD2FEE5570D3BFC0F1DEC5DCBAA80A9A55A936D66B5B1ECF44F014E71B19DFA9C406F2A753D607BB8251612901DFDCBE8C79A0FC08007FE
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Reputation:	low
Preview:	2021/08/03-22:05:13.167 1280 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-22:05:13.174 1280 Recovering log #3.2021/08/03-22:05:13.174 1280 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\72c7e216-6d73-499a-9c36-3c23cd7335da.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.256003239338233
Encrypted:	false
SSDEEP:	6:mGHNVq2PWXp+N23iKKdKusNpV/2jMGIFUtpThNgZmwPThNIkwOWXp+N23iKKdKux:DHnva5KkFFUtpTE/PTk5f5KkOJ
MD5:	2E9E5E3AC551156F1CC678CF6CDCC156
SHA1:	6F9ED066FD6AFF89C689C69A6E0672AAE6275F10
SHA-256:	42C3A8211F2C037B5AB2C693984E8E749E81E91AFFF37B6D7F2E7B8828098C15
SHA-512:	940E9124D134686AB5461EAEB480146EB69AB2CBE8D166BFA226CD12420FC13E43823398E2BD5301DC0FEF4534462834B03C7B54B1BE9BED7DB7D7CFE9FD0F5
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.383 14b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:05:13.385 14b4 Recovering log #3.2021/08/03-22:05:13.385 14b4 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):	430
Entropy (8bit):	5.256003239338233
Encrypted:	false
SSDEEP:	6:mGHNVq2PWXp+N23iKKdKusNpV/2jMGIFUtpThNgZmwPThNIkwOWXp+N23iKKdKux:DHnva5KkFFUtpTE/PTk5f5KkOJ
MD5:	2E9E5E3AC551156F1CC678CF6CDCC156
SHA1:	6F9ED066FD6AFF89C689C69A6E0672AAE6275F10
SHA-256:	42C3A8211F2C037B5AB2C693984E8E749E81E91AFFF37B6D7F2E7B8828098C15
SHA-512:	940E9124D134686AB5461EAEB480146EB69AB2CBE8D166BFA226CD12420FC13E43823398E2BD5301DC0FEF4534462834B03C7B54B1BE9BED7DB7D7CFE9FD0F5
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.383 14b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:05:13.385 14b4 Recovering log #3.2021/08/03-22:05:13.385 14b4 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):	429
Entropy (8bit):	5.269205309694056
Encrypted:	false
SSDEEP:	12:DM+va5KkmiuFUtpT36W/PT3pV5f5Kkm2J:Ra5KkSgF6AJf5Kkr
MD5:	778862E3B91B1F03B76F3C7071890D72
SHA1:	6D295BEE195271EAFD5393257FB81EA412F2F5E7
SHA-256:	3FF6B95FA5A320219D89CBE8DCF2A375C33B5DC44CBC68C908991D4615A0EA87
SHA-512:	DF3863D39490E939153FD87F98E2D40AB12D11390431A24150741104BD20493B6CACB3B294645D852F469D4253CBBB053D31C95C820EF17C09B01EADF1F0BCE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.438 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-22:05:13.440 d5c Recovering log #3.2021/08/03-22:05:13.440 d5c 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):	429
Entropy (8bit):	5.269205309694056
Encrypted:	false
SSDEEP:	12:DM+va5KkmiuFUtpT36W/PT3pV5f5Kkm2J:Ra5KkSgF6AJf5Kkr
MD5:	778862E3B91B1F03B76F3C7071890D72
SHA1:	6D295BEE195271EAFD5393257FB81EA412F2F5E7
SHA-256:	3FF6B95FA5A320219D89CBE8DCF2A375C33B5DC44CBC68C908991D4615A0EA87

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
SHA-512:	DF3863D39490E939153FD87F98E2D40AB12D11390431A24150741104BD20493B6CACB3B294645D852F469D4253CBBB053D31C95C820EF17C09B01EADF1F0BCE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.438 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-22:05:13.440 d5c Recovering log #3.2021/08/03-22:05:13.440 d5c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.213326312739877
Encrypted:	false
SSDEEP:	6:mN9+q2PWXp+N23iKKdKusNpZQMxIFUtp+XWZmwPyVkwOWXp+N23iKKdKusNpZQMT:Y+va5KkMFUtpqW/PyV5f5KkTJ
MD5:	CDBC038862BEC08B029D2F31494C8FC5
SHA1:	E3877FD984F48745DF0B42AD17D411393EB14823
SHA-256:	B97E0D4B5D1A6647AAFA38153CDBFE8DA321A6509C9F297D5C6A8981327C06F1
SHA-512:	3D571247EBB969E58CA04BB8F8A88C85F67CD57D20B389F3EC66D74B2068DA669026B43DFBF54DE5287501AFDDEB8AFE2469008546A762C60759079BB34A228
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:30.332 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-22:05:30.333 d5c Recovering log #3.2021/08/03-22:05:30.334 d5c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old90 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.213326312739877
Encrypted:	false
SSDEEP:	6:mN9+q2PWXp+N23iKKdKusNpZQMxIFUtp+XWZmwPyVkwOWXp+N23iKKdKusNpZQMT:Y+va5KkMFUtpqW/PyV5f5KkTJ
MD5:	CDBC038862BEC08B029D2F31494C8FC5
SHA1:	E3877FD984F48745DF0B42AD17D411393EB14823
SHA-256:	B97E0D4B5D1A6647AAFA38153CDBFE8DA321A6509C9F297D5C6A8981327C06F1
SHA-512:	3D571247EBB969E58CA04BB8F8A88C85F67CD57D20B389F3EC66D74B2068DA669026B43DFBF54DE5287501AFDDEB8AFE2469008546A762C60759079BB34A228
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:30.332 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-22:05:30.333 d5c Recovering log #3.2021/08/03-22:05:30.334 d5c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\4c8a4380-5343-41f8-8fc3-60b6cc642ecb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\4c8a4380-5343-41f8-8fc3-60b6cc642ecb.tmp	
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):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.2030068436804555
Encrypted:	false
SSDEEP:	12:VFva5KkkGHArBFUtpW/P3P5f5KkkGHAryJ:VJa5KkkGgPggf5KkkGga
MD5:	234CB87A4EB0D821405F310892274F69
SHA1:	302DFE501C1D00D017952FDD3D4CB0ADF9619015
SHA-256:	F66DDE028955DD2ADE40E2F48A2B70BC3FF409B403A29B682E9C3B6AB393A703
SHA-512:	231B492A44B79164481A8C7A70FC9FDB9A8CB0C19496058BE12311CB5CC7C0F7FF750C4844E38D104C862EA81208BDB943E90C28925EBE27DFBEB148B1D6044
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.743 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:05:18.747 3e4 Recovering log #3.2021/08/03-22:05:18.748 3e4 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):	427
Entropy (8bit):	5.2030068436804555
Encrypted:	false
SSDEEP:	12:VFva5KkkGHArBFUtpW/P3P5f5KkkGHAryJ:VJa5KkkGgPggf5KkkGga
MD5:	234CB87A4EB0D821405F310892274F69
SHA1:	302DFE501C1D00D017952FDD3D4CB0ADF9619015
SHA-256:	F66DDE028955DD2ADE40E2F48A2B70BC3FF409B403A29B682E9C3B6AB393A703
SHA-512:	231B492A44B79164481A8C7A70FC9FDB9A8CB0C19496058BE12311CB5CC7C0F7FF750C4844E38D104C862EA81208BDB943E90C28925EBE27DFBEB148B1D6044

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.743 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-22:05:18.747 3e4 Recovering log #3.2021/08/03-22:05:18.748 3e4 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\Network Persistent State.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.220534704517276
Encrypted:	false
SSDEEP:	12:ava5KkkGHArqiuFUtpp/PQD5f5KkkGHArq2J:ga5KkkGgCgYVf5KkkGg7
MD5:	DD90D311FE0754FA5AF190387ECFB50E
SHA1:	417497BFFE111936C18676E5C3E5232059390413
SHA-256:	DD1EFB7B29A005938DD7D08B2E9D9AE7E81C803EA5A57BF95C2F02701CA35C9D
SHA-512:	7B198957758BA166A008A665E27A32015D9756C1900B32E120716A48508A09A24F24C680C3D0CCBDE1477C0EFD46C4570D3BF612DA124401FC05BC062E71B8CD
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.745 da4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-22:05:18.747 da4 Recovering log #3.2021/08/03-22:05:18.748 da4 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):	5.220534704517276
Encrypted:	false
SSDEEP:	12:ava5KkkGHArqiuFUtpp/PQD5f5KkkGHArq2J:ga5KkkGgCgYVf5KkkGg7
MD5:	DD90D311FE0754FA5AF190387ECFB50E
SHA1:	417497BFFE111936C18676E5C3E5232059390413
SHA-256:	DD1EFB7B29A005938DD7D08B2E9D9AE7E81C803EA5A57BF95C2F02701CA35C9D
SHA-512:	7B198957758BA166A008A665E27A32015D9756C1900B32E120716A48508A09A24F24C680C3D0CCBDE1477C0EFD46C4570D3BF612DA124401FC05BC062E71B8CD
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:18.745 da4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-22:05:18.747 da4 Recovering log #3.2021/08/03-22:05:18.748 da4 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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.213426562451423
Encrypted:	false
SSDEEP:	12:Y9+va5KkkGHArAFUtp6W/PpV5f5KkkGHArfJ:YKa5KkkGgkgEKf5KkkGgV
MD5:	CEE418793AC9E8ACC28EB02FF7B71682
SHA1:	79F3D24A3896896A63F3CA955E36F30CF6EE450D
SHA-256:	48D128BF4B312A780EE6127E4BB8D3BF22EF64AA8BF426246586091A669717F2
SHA-512:	6CD6FFD2649132FC0198DD424353893C969FD2AD0B85E7DFA39899D68004C2B65B27A81506C88D427FED44612CF05F6C4EE127E140872DE0B10F297833F633EC
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:34.965 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-22:05:34.966 d5c Recovering log #3.2021/08/03-22:05:34.966 d5c 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):	5.213426562451423
Encrypted:	false
SSDEEP:	12:Y9+va5KkkGHArAFUtp6W/PpV5f5KkkGHArfJ:YKa5KkkGgkgEKf5KkkGgV
MD5:	CEE418793AC9E8ACC28EB02FF7B71682
SHA1:	79F3D24A3896896A63F3CA955E36F30CF6EE450D
SHA-256:	48D128BF4B312A780EE6127E4BB8D3BF22EF64AA8BF426246586091A669717F2
SHA-512:	6CD6FFD2649132FC0198DD424353893C969FD2AD0B85E7DFA39899D68004C2B65B27A81506C88D427FED44612CF05F6C4EE127E140872DE0B10F297833F633EC
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:34.965 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-22:05:34.966 d5c Recovering log #3.2021/08/03-22:05:34.966 d5c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.257803238279055
Encrypted:	false
SSDEEP:	6:mGaes3+q2PWXp+N23iKKdKpIFUtpTeNZmwPTces3VkwOWXp+N23iKKdKa/WLJ:Daedva5KkmFUtpTeN/PTYF5f5KkaUJ
MD5:	89C0F46F9D494103D6A4F930E1BA76FB
SHA1:	D1E624F0E027429A8C917FD7D3B8F82127ACE867
SHA-256:	3A7C14527EE61C719B878B99A2362108803AA48F1C4DC3A995012AF6E44B9387
SHA-512:	2EDE52F6DCCF86979EFA7930EDBB2044A446C009E284CAD5EAD2EC72EA4E29A60CA4109CE498BD8A9EE2BF1CEFE490478248DA243919206D8284A9445FDD1 AD
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.151 1498 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-22:05:13.155 1498 Recovering log #3.2021/08/03-22:05:13.157 1498 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.257803238279055
Encrypted:	false
SSDEEP:	6:mGaes3+q2PWXp+N23iKKdKpIFUtpTeNZmwPTces3VkwOWXp+N23iKKdKa/WLJ:Daedva5KkmFUtpTeN/PTYF5f5KkaUJ
MD5:	89C0F46F9D494103D6A4F930E1BA76FB
SHA1:	D1E624F0E027429A8C917FD7D3B8F82127ACE867
SHA-256:	3A7C14527EE61C719B878B99A2362108803AA48F1C4DC3A995012AF6E44B9387
SHA-512:	2EDE52F6DCCF86979EFA7930EDBB2044A446C009E284CAD5EAD2EC72EA4E29A60CA4109CE498BD8A9EE2BF1CEFE490478248DA243919206D8284A9445FDD1 AD
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:13.151 1498 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-22:05:13.155 1498 Recovering log #3.2021/08/03-22:05:13.157 1498 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):	5.287936336406459
Encrypted:	false
SSDEEP:	12:q+va5KkkOrsFUtpp2W/Pp9V5f5KkkOrzJ:La5Kk+gT2gVf5Kkn
MD5:	481AC37EFD0336F9C2F50A6D14F328DC
SHA1:	473A0480142FB6DB3822B905A512B02A690F529D
SHA-256:	983C790466CE6F6D62C8C474367BA2C9FC18AD384407DCB3427ADB8833BC36E4
SHA-512:	137F28E6AAC5CBE5A205D546CA8D5974FAC0B990801DE6885DCB7D73EE289FEE21BE723533DDE1AEFADC7C9C7B738EA717887599D3383C8CE38A296003C72 6E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:20.294 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-22:05:20.295 d5c Recovering log #3.2021/08/03-22:05:20.295 d5c 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.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\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old (copy)	
Size (bytes):	399
Entropy (8bit):	5.287936336406459
Encrypted:	false
SSDEEP:	12:q+va5KkkOrsFUtpp2W/Pp9V5f5KkkOrzJ:La5Kk+gT2gVf5Kkn
MD5:	481AC37EFD0336F9C2F50A6D14F328DC
SHA1:	473A0480142FB6DB3822B905A512B02A690F529D
SHA-256:	983C790466CE6F6D62C8C474367BA2C9FC18AD384407DCB3427ADB8833BC36E4
SHA-512:	137F28E6AAC5CBE5A205D546CA8D5974FAC0B990801DE6885DCB7D73EE289FEE21BE723533DDE1AEFADC7C9C7B738EA717887599D3383C8CE38A296003C72 6E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:20.294 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbm eomcjbeemfm/MANIFEST-000001.2021/08/03-22:05:20.295 d5c Recovering log #3.2021/08/03-22:05:20.295 d5c Reusing old log C:\Users\user\AppData\Local\Goog le\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):	1207
Entropy (8bit):	5.585379709632917
Encrypted:	false
SSDEEP:	24:YQUU6H0UhVsTG1KUerkq/HeUeXby2qUeXvh7wUQRUenHQ:YQUU6UUhVseKUewqPeUer2UefpwU0Uew
MD5:	542D8F6A3AD33622B410D6FA8DA25556
SHA1:	FFB3036C336264FF2C5D55E35A545EB41A6C94B9
SHA-256:	B753E5FB8CA51947C213E48A17A45FCEF041B33EA3A4729DEEA6109855BDA48D
SHA-512:	FF1F85C7C1EE3B8652662A479535D2E77D8BA81A5DE54E85212373DAF821288A80D7921708185843C67285E76FFF39DFBAB202929289B67768EC8CBA6231A06E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659589517.233009,"host":"LgR7jvaFNfmEH7iTmG2VL8JbNq6qMTR1Vco6SYJWsXU=","mode":"force-https","sts_include_subdomains" :false,"sts_observed":1628053517.233019},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_i nclude_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"forc e-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8k DM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho 8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659589516.654573,"host":"8/RrMm QlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","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):	3.0220552088742
Encrypted:	false
SSDEEP:	3:uVvhV:avD
MD5:	EC95E0A2F0079B294C2E4655AD3575CF
SHA1:	D6DA36FBD59F55ECCC29BE1FA00D23155BF3D1F7
SHA-256:	A61869297E23E501F7B01F11272925C08BDE56036A81FE70758C009B78836642
SHA-512:	58D35B4D02CBA26D53376D1958C47813EFDA2FBC3C500EB8D7C35F02264E5F6AF248884E9B824841D372949947026622785834663986818 1C4DCE6BCFC08A931
Malicious:	false
Reputation:	low
Preview:	.....]..p

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bceb9dcd-e1b5-4835-9a67-f4c453ddfebe.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):	1207
Entropy (8bit):	5.585379709632917
Encrypted:	false
SSDEEP:	24:YQUU6H0UhVsTG1KUerkq/HeUeXby2qUeXvh7wUQRUenHQ:YQUU6UUhVseKUewqPeUer2UefpwU0Uew
MD5:	542D8F6A3AD33622B410D6FA8DA25556
SHA1:	FFB3036C336264FF2C5D55E35A545EB41A6C94B9
SHA-256:	B753E5FB8CA51947C213E48A17A45FCEF041B33EA3A4729DEEA6109855BDA48D
SHA-512:	FF1F85C7C1EE3B8652662A479535D2E77D8BA81A5DE54E85212373DAF821288A80D7921708185843C67285E76FFF39DFBAB202929289B67768EC8CBA6231A06E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bceb9dcd-e1b5-4835-9a67-f4c453ddfebe.tmp	
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659589517.233009,"host":"LgR7jvaFNfmEH7iTmG2VL8JbNq6qMTR1Vco6SYJWsXU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628053517.233019},{"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":1659589516.654573,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c986afed-f683-4228-ba4a-7fd4f4d56ddd.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535240768504845
Encrypted:	false
SSDEEP:	384:iEvntRLlLFX+1kXqKf/pUZNCgVLH2HfDerUyHGsnTLmEP4D:PLld+1kXqKf/pUZNCgVLH2HfyrUyGsnm
MD5:	F264EB198F1BB7A463EC7FF4D5D15311
SHA1:	12C2A0DBD18029EFF0EFD9B7927223BCBBC70055
SHA-256:	1506F88C37505609F1E946CA862EF3C7EB1174BF262579E9F842EB726966FF9F
SHA-512:	421CC4D275749DD3360BF62AA514E0E5BA4AE1E250160CE2232B4802BFB8B7DDCAE964F0B5D832466317FD697F641087011C5A132F9374C5C61BA9E2946828C
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":"13272527113143131","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\cdb7244a-8ab8-401e-9247-3827665d6a84.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):	5476
Entropy (8bit):	5.1828268257789265
Encrypted:	false
SSDEEP:	96:nmC2qt95QmMrvcKIHok0JCKL8VbOTQVuwn:nmCN9Gjco4K6
MD5:	8F8DDD40CA69745F07479AAF79F860E3
SHA1:	176E1319B576E9AC16821957D5E0EEF4E8904FC0
SHA-256:	ECDF533780F51DE6F847926F53DCE5E8F4164E9284425DE40D38C4E5A9E30AB1
SHA-512:	E48E0F46486FA71773468DA4DE60EA73B6AB837D5B4E277BDA03695CF3A495BA0AB3952AB4FCE9AEFB1EA3BE7F4EEE332FF0E595D13BA71062F7C9E0DA3E7019
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272527113400851","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\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	136
Entropy (8bit):	4.592614579507851
Encrypted:	false
SSDEEP:	3:tUK6cno0GIyZmwv3Ict/HV8sIct/HWGv:manfgZmwPft/HVvft/Htv
MD5:	A16FCFED23332AD5CDE110EBCBA04879
SHA1:	6873FD566201803AA367B1476270ABD283FE89B0
SHA-256:	662F2888D190DBECB00ED22C984222B24E4620F1580AB4361A3D049FC587C238
SHA-512:	830A23A8C89BC8F90FA07F4AA6BCC93E59D7AB5AC50F23CD535462E49445BE8C83D0ADA40ECCA2B0852EB11A70EA7D0DB7107830F8271103AED9783BF5210AD0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-22:05:17.939 664 Recovering log #3.2021/08/03-22:05:17.998 664 Delete type=0 #3.2021/08/03-22:05:17.998 664 Delete type=3 #2.

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

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:05:16.158381939 CEST	192.168.2.3	8.8.8.8	0x72e8	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:05:16.162072897 CEST	192.168.2.3	8.8.8.8	0xadc8	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:05:16.166925907 CEST	192.168.2.3	8.8.8.8	0x1c1b	Standard query (0)	ballardagency-my.sharepoint.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:05:17.955707073 CEST	192.168.2.3	8.8.8.8	0x11ba	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:05:18.446641922 CEST	192.168.2.3	8.8.8.8	0x8c00	Standard query (0)	gitsoft-container000.azurewebsites.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:05:20.993709087 CEST	192.168.2.3	8.8.8.8	0x4521	Standard query (0)	gitsoft-container000.azurewebsites.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:05:16.198787928 CEST	8.8.8.8	192.168.2.3	0x72e8	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:05:16.198787928 CEST	8.8.8.8	192.168.2.3	0x72e8	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 22:05:16.206003904 CEST	8.8.8.8	192.168.2.3	0xadc8	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 22:05:16.213490009 CEST	8.8.8.8	192.168.2.3	0x1c1b	No error (0)	ballardagency-my.sharepoint.com	ballardagency.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:05:16.213490009 CEST	8.8.8.8	192.168.2.3	0x1c1b	No error (0)	ballardagency.sharepoint.com	784-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:05:16.213490009 CEST	8.8.8.8	192.168.2.3	0x1c1b	No error (0)	784-ipv4e.clump.prod.aa-rt.sharepoint.com	19244-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:05:16.213490009 CEST	8.8.8.8	192.168.2.3	0x1c1b	No error (0)	19244-ipv4e.farm.prod.aa-rt.sharepoint.com	19244-ipv4e.farm.prod.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:05:17.988184929 CEST	8.8.8.8	192.168.2.3	0x11ba	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:05:17.988184929 CEST	8.8.8.8	192.168.2.3	0x11ba	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)
Aug 3, 2021 22:05:18.541835070 CEST	8.8.8.8	192.168.2.3	0x8c00	No error (0)	gitsoft-container000.azurewebsites.net	waws-prod-dm1-123.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:05:18.541835070 CEST	8.8.8.8	192.168.2.3	0x8c00	No error (0)	waws-prod-dm1-123.sip.azurewebsites.windows.net	waws-prod-dm1-123.cloudapp.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:05:21.042068958 CEST	8.8.8.8	192.168.2.3	0x4521	No error (0)	gitsoft-container000.azurewebsites.net	waws-prod-dm1-123.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:05:21.042068958 CEST	8.8.8.8	192.168.2.3	0x4521	No error (0)	waws-prod-dm1-123.sip.azurewebsites.windows.net	waws-prod-dm1-123.cloudapp.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 1200 Parent PID: 3156

General

Start time:	22:05:12
Start date:	03/08/2021
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://ballardagency-my.sharepoint.com/:u:/p/linda_davidson/EUJ1_psy-lhNg86-55dcNsUB8Ohn7k8q2Vtm1Wl6wQekUA?download=1'
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: 3560 Parent PID: 1200

General

Start time:	22:05:13
Start date:	03/08/2021
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=1544,18194422631878575160,17341075801436133396,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1752 /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

Analysis Process: chrome.exe PID: 6436 Parent PID: 1200

General

Start time:	22:05:17
Start date:	03/08/2021
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=quarantine.mojom.Quarantine --field-trial-handle=1544,18194422631878575160,17341 07580143613396,131072 --lang=en-US --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=4964 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly