ID: 458989
Cookbook: browseurl.jbs
Time: 00:57:29
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

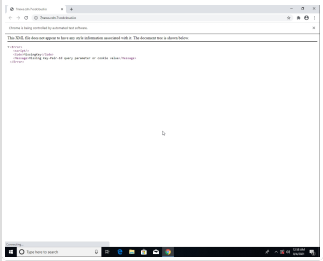
Windows Analysis Report http://7news.cdn.7vodcloud.io

Overview

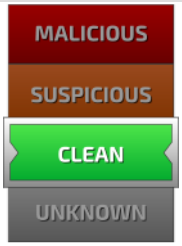
General Information

Sample URL:	http://7news.cdn.7vodcloud.io
Analysis ID:	458989
Infos:	

Most interesting Screenshot:



Detection

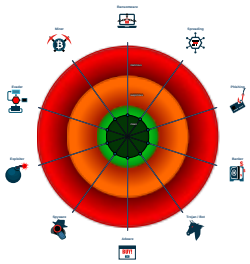


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5728 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://7news.cdn.7vodcloud.io' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 852 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,17392542265336455136,3443799518247237767,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1776 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

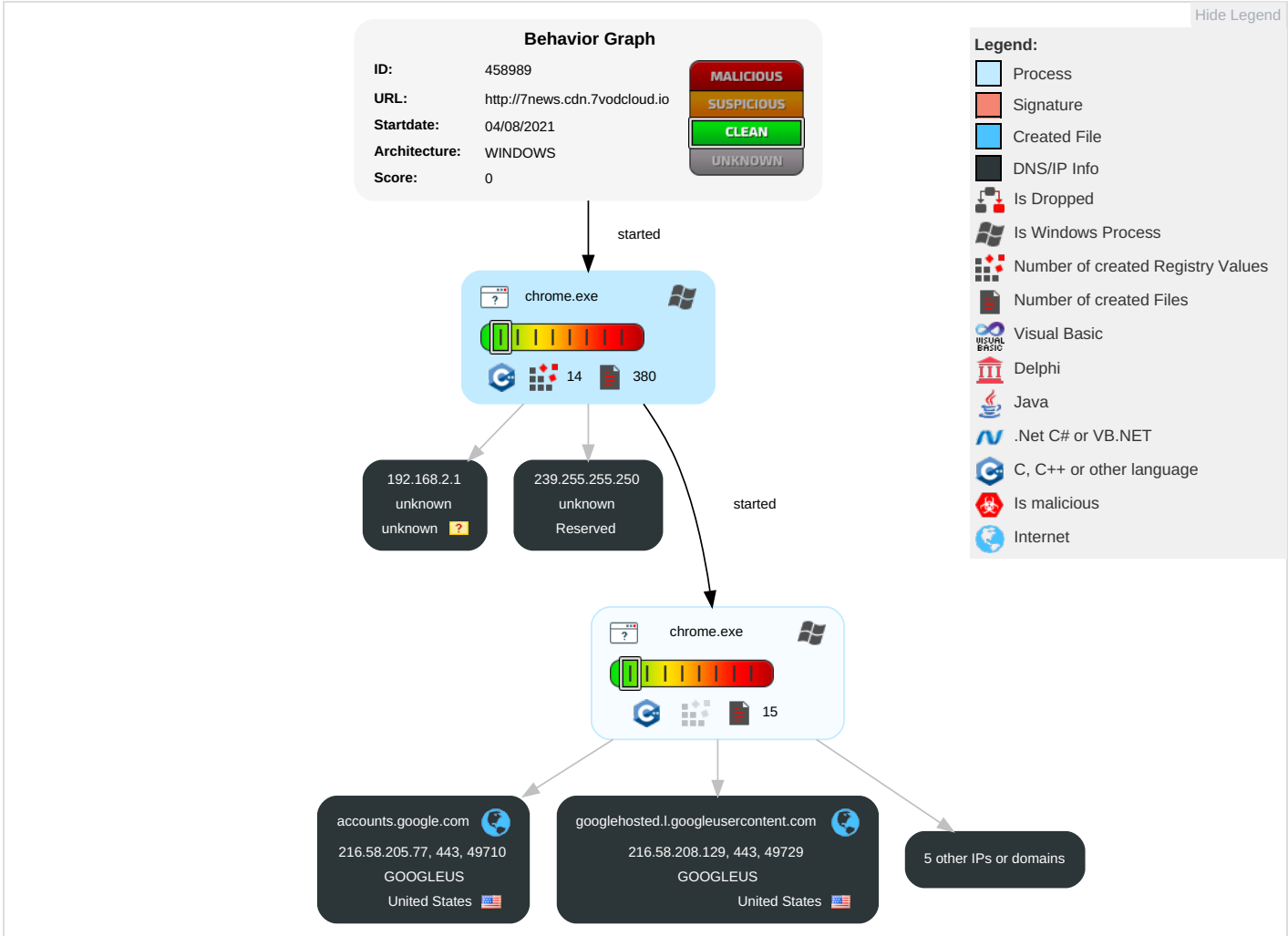
Click to jump to signature section

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

Mitre Att&ck Matrix

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

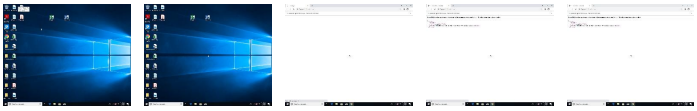
Behavior Graph

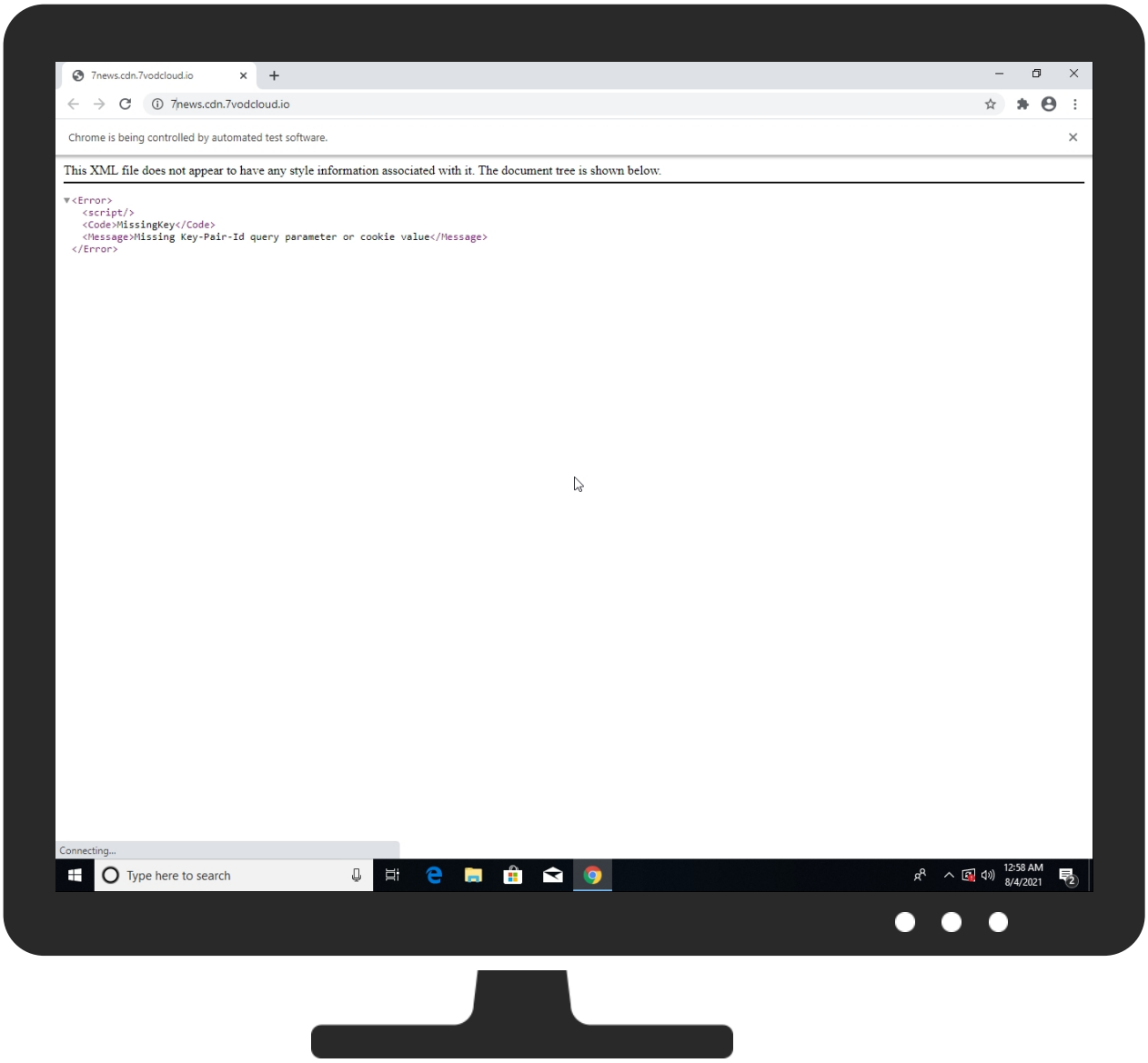


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://7news.cdn.7vodcloud.io	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://7news.cdn.7vodcloud.io//	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	
http://7news.cdn.7vodcloud.io/favicon.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
7news.cdn.7vodcloud.io	13.32.14.64	true	false		unknown
clients.l.google.com	216.58.208.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://7news.cdn.7vodcloud.io/	false		unknown
http://7news.cdn.7vodcloud.io/	false		unknown
http://7news.cdn.7vodcloud.io/favicon.ico	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
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
13.32.14.64	7news.cdn.7vodcloud.io	United States		7018	ATT-INTERNET4US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458989
Start date:	04.08.2021
Start time:	00:57:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 3s

Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://7news.cdn.7vodcloud.io
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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@28/194@4/7
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\0a9f6591-b981-4da6-a0c6-48631d9c0761.tmp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\42b8f297-afbb-409b-8bbc-263a05a89a7f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.567067380713962
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvN7wUXRUenHQ:YI6UUhVseKUewqPeUer2UefNwUBUenw

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\42b8f297-afbb-409b-8bbc-263a05a89a7f.tmp	
MD5:	41295EED287BA10D02242FFAB1EBCAF2
SHA1:	9065B0CF392E147B6DDE2523CD972DCF5872EFDA
SHA-256:	B30412146AB3E9EA2B2EAFC5E23CB5CDB459723EA0A5FAF150D1BBCAD3A883E1
SHA-512:	449E39B48895C64BC4AFC759A316F5D1AE931882B5970647EDD4666B0CA0524D484AA28BD842ADAACE57386A68726EF0AF87E07CBCFCAA0A4E270E9EDA012E D8
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659599897.660061,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628063897.660066},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\59a5c1b3-23ed-4dc9-8262-d26f67cef2fc.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):	5742
Entropy (8bit):	5.184932519953728
Encrypted:	false
SSDEEP:	96:nCCdqF9xyOcKIcrok0JCKL80kZ1zbOTQVuwn:nCC498OcqG4KbkZN
MD5:	A2466D0AF4CDC496A86F911CD8760114
SHA1:	400B851C6E0DB39D045D482B57F1E3C8560033BB
SHA-256:	D50DCF45A71D02E096294897E47858107CC1110B06B964A0205CAFCCFD675D0A
SHA-512:	F032674A47FC93E55A37C19A3D7E1D5E43DE9141AAA9095C012285811BA8D522BFA3EC19BB1BFB54C74E4C704737F33B166F8010EE7F9031F90314DEF7908749
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272537494744686","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8b39fb42-ac40-4336-88d2-79de0a1a39db.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):	5742
Entropy (8bit):	5.184932519953728
Encrypted:	false
SSDEEP:	96:nCCdqF9xyOcKIcrok0JCKL80kZ1zbOTQVuwn:nCC498OcqG4KbkZN
MD5:	A2466D0AF4CDC496A86F911CD8760114
SHA1:	400B851C6E0DB39D045D482B57F1E3C8560033BB
SHA-256:	D50DCF45A71D02E096294897E47858107CC1110B06B964A0205CAFCCFD675D0A
SHA-512:	F032674A47FC93E55A37C19A3D7E1D5E43DE9141AAA9095C012285811BA8D522BFA3EC19BB1BFB54C74E4C704737F33B166F8010EE7F9031F90314DEF7908749
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272537494744686","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8dade386-e055-4121-82a8-52d082ab1753.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):	5.536114175190453
Encrypted:	false
SSDEEP:	384:UMBtqLlZwXv1kXqKf/pUZNCgVLH2HfDBrUNHGmnT0w3T4Cm:CLlUv1kXqKf/pUZNCgVLH2Hf1rUxGmnI
MD5:	1DCC43935F61FF655AD417E2084541B0
SHA1:	1937720CFFCB636D8751A0C47E6ACEC898043B5F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8dade386-e055-4121-82a8-52d082ab1753.tmp	
SHA-256:	7AAB8572DD54F6CFEB860BF28A404C7FDA08AE053D2B85F2B30308C0DF0AA255
SHA-512:	8472D5041CDDEB8ADE98D0C88C5D220C8AA619B71A88015F51D1C885948A1C36DCD31AF4E6CE9876A2480E20291EF898302A317974DD249C637DA28958C0565
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":"13272537494445856","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\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.155775655050918
Encrypted:	false
SSDEEP:	6:mDhUSyq2PWXp+N23iKKdK9RXXTZIFUtp2hUi1ZmwP2hU0RkwOWXp+N23iKKdK9Rn:IUSyva5Kk7XT2FUtpYU0/PYU0R5f5KkT
MD5:	1A23CD3ADE31508F7F3A9B596927D3B7
SHA1:	6CC25B88B504B61F29FD2DEEDE3FDB462779F16C
SHA-256:	8A9DFCF8EE43F79F45B799D59B7028DF80188BF83C793DBBC6ECF4FC0FE2CBDB
SHA-512:	5A74398354DD5589333918E35C0D341B3E11621E99DC3346A8F38A8A6A4D3E1756CE8517343ADF3DDE5CC576B2A5C7D4B8D2A930325ADEF36E2E59C41073F4E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.192 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-00:58:20.194 1010 Recovering log #3.2021/08/04-00:58:20.194 1010 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.oldB (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.155775655050918
Encrypted:	false
SSDEEP:	6:mDhUSyq2PWXp+N23iKKdK9RXXTZIFUtp2hUi1ZmwP2hU0RkwOWXp+N23iKKdK9Rn:IUSyva5Kk7XT2FUtpYU0/PYU0R5f5KkT
MD5:	1A23CD3ADE31508F7F3A9B596927D3B7
SHA1:	6CC25B88B504B61F29FD2DEEDE3FDB462779F16C
SHA-256:	8A9DFCF8EE43F79F45B799D59B7028DF80188BF83C793DBBC6ECF4FC0FE2CBDB
SHA-512:	5A74398354DD5589333918E35C0D341B3E11621E99DC3346A8F38A8A6A4D3E1756CE8517343ADF3DDE5CC576B2A5C7D4B8D2A930325ADEF36E2E59C41073F4E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.192 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-00:58:20.194 1010 Recovering log #3.2021/08/04-00:58:20.194 1010 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):	5.125382508908943
Encrypted:	false
SSDEEP:	6:mDhUhbyq2PWXp+N23iKKdKyDZIFUtp2hUa+r1ZmwP2hUa+9RkwOWXp+N23iKKdKy:IUhbyva5Kk02FUtpYUaa/PYUayR5f5K1
MD5:	E7EBA84A8015E8B457372388F8084E13
SHA1:	91A26B257F6E45F26A6FF394D2E8C13AFA2B681A
SHA-256:	C756434D8E8B743D8233DA3B6D22628B3911C841783BBD7A3D96492414F6874F
SHA-512:	B45BB8BF9538963377E1279CE4610609560A04A518F39552B5AC67C17AE42ABC4E694FA551768E01E80BA3FA883057431BE688DBDC32306BB6BDED1D1E206F8E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.162 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-00:58:20.184 1010 Recovering log #3.2021/08/04-00:58:20.184 1010 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):	5.125382508908943
Encrypted:	false
SSDEEP:	6:mDhUhbyq2PWXp+N23iKKdKyDZIFUtp2hUa+r1ZmwP2hUa+9RkwOWXp+N23iKKdKy:IUhbyva5Kk02FUtpYUaa/PYUayR5f5K1
MD5:	E7EBA84A8015E8B457372388F8084E13
SHA1:	91A26B257F6E45F26A6FF394D2E8C13AFA2B681A
SHA-256:	C756434D8E8B743D8233DA3B6D22628B3911C841783BBD7A3D96492414F6874F
SHA-512:	B45BB8BF9538963377E1279CE4610609560A04A518F39552B5AC67C17AE42ABC4E694FA551768E01E80BA3FA883057431BE688DBDC32306BB6BDED1D1E206F8
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.162 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-00:58:20.184 1010 Recovering log #3.2021/08/04-00:58:20.184 1010 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC761F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9660737542759482
Encrypted:	false
SSDEEP:	24:hcLgAZOZD/RpqLbJLbXaFpEO5bNmISHn06Uwh8:h8NOZRpq5LLOpEO5J/Kn7Uy8
MD5:	85070E2C84F71756C7E685D9364C9241
SHA1:	919EB5F3FAD88C3D0D142E239B7C74AC3E4D6AC3
SHA-256:	204C9E9F195C85CA6D42A92575D60A2AA93BF3A665B373FB0C023AEBA7EF429B
SHA-512:	EEBDA943F2139728465526F453C9E2875564DFC5D4E99310D88DF441BC19E43C305B2243C42CB11CD8A6F32D1654E5AB40D967B583DFF4D02A74F565013FC28
Malicious:	false
Reputation:	low
Preview:	....u..... ....

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):	949
Entropy (8bit):	3.1978879262712128
Encrypted:	false
SSDEEP:	12:3olydJhvAxddhPlpxlpN8klyTpelYAejIcpKIClmW9lptlpl:34S5IDlrlAqJ/X4lLlL
MD5:	0CFABA79F0FCCC5EC8485E3F65794F64

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
SHA1:	F29B86DD24B7D4D5A4A0E72A6CBAFDFA17708A05
SHA-256:	CAB00A318BBA0048B3BA71BC51830D0493C354331F18E4F60A9BE9A6D990F094
SHA-512:	117EAFDF8B9F18A900C5E05FAA1281D0DC8BC8F0741CC4D97682144B57FB65DA71CE5E71D8BA2AED440CDDD5874E91AA9B5D88B5FCA3308FBAE0754F7149DE74
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...bed85c44_8f3b_4394_9b46_684ee49345c6.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....1.,.....http://7news.cdn.7vodcloud.io/.....h.....`.....2.J*....3.J*.....D.....h.t.t.p.:.//.7.n.e.w.s...c.d.n...7.v.o.d.c.l.o.u.d...i.o./.....8.....0.....8.....http://7news.cdn.7vodcloud.io/.....".rM'/.....

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.280620835540338
Encrypted:	false
SSDEEP:	6:my7qM+q2PWXp+N23iKKdK8aPrqIFUtpvPZmwPvxMVkwOWXp+N23iKKdK8amLJ:jqM+va5KkL3FUtp3/PpMV5f5KkQJ
MD5:	0B1CF1945907686D66DDF9589754535F
SHA1:	5B304D4D9374FD0CDEBDBBAF5198692ECA669420
SHA-256:	FBBB6705049C43B78A31D1E74C51560BDBEBB5266946BF397BA28105BE454D39
SHA-512:	ED563ECBDEADF3C2715641B176959CC0A24DA3091A9B21EAA1B81A5A2D657A5360054B0BBF817DA29EF327B9A1CFDBD4F2DC3F1BFBA3288211232E76A02FB37D
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.793 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-00:58:14.797 176c Recovering log #3.2021/08/04-00:58:14.798 176c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.280620835540338
Encrypted:	false
SSDEEP:	6:my7qM+q2PWXp+N23iKKdK8aPrqIFUtpvPZmwPvxMVkwOWXp+N23iKKdK8amLJ:jqM+va5KkL3FUtp3/PpMV5f5KkQJ
MD5:	0B1CF1945907686D66DDF9589754535F
SHA1:	5B304D4D9374FD0CDEBDBBAF5198692ECA669420
SHA-256:	FBBB6705049C43B78A31D1E74C51560BDBEBB5266946BF397BA28105BE454D39
SHA-512:	ED563ECBDEADF3C2715641B176959CC0A24DA3091A9B21EAA1B81A5A2D657A5360054B0BBF817DA29EF327B9A1CFDBD4F2DC3F1BFBA3288211232E76A02FB 7D
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.793 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-0 0:58:14.797 176c Recovering log #3.2021/08/04-00:58:14.798 176c 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
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.....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):	5.243574972664197
Encrypted:	false
SSDEEP:	6:mRPnpM+q2PWXp+N23iKKdK8NIFUtpiBUjZmwPi/qMVkwOWXp+N23iKKdK8+eLJ:ShM+va5KkpFUtpiBm/Pi/qMV5f5KkqJ
MD5:	5E9449E5DFE4534DA46923C8074012B9
SHA1:	E5E86D3BC0DA8321F667E8E825DDD1A942EAF62C
SHA-256:	258E3B73216180BBD8055ADE2A9FCD62F377C95832798A9D9DD9C7A62A36498D
SHA-512:	78DF1A31709434EAEC2EA6841511B0BA343F2133E8090124EBF85F9AE41EE3E178885A46D93CE02897327F7DD206BC90F1A3FC92B9DB9E3D3E5C23768608BB6
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:17.046 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-0 0:58:17.048 176c Recovering log #3.2021/08/04-00:58:17.049 176c 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.oldJ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.243574972664197
Encrypted:	false
SSDEEP:	6:mRPnpM+q2PWXp+N23iKKdK8NIFUtpiBUjZmwPi/qMVkwOWXp+N23iKKdK8+eLJ:ShM+va5KkpFUtpiBm/Pi/qMV5f5KkqJ
MD5:	5E9449E5DFE4534DA46923C8074012B9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.oldJ (copy)	
SHA1:	E5E86D3BC0DA8321F667E8E825DDD1A942EAF62C
SHA-256:	258E3B73216180BBD8055ADE2A9FCD62F377C95832798A9D9DD9C7A62A36498D
SHA-512:	78DF1A31709434EAEC2EA6841511B0BA343F2133E8090124EBF85F9AE41EE3E178885A46D93CE02897327F7DD206BC90F1A3FC92B9DB9E3D3E5C23768608BB6
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:17.046 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-00:58:17.048 176c Recovering log #3.2021/08/04-00:58:17.049 176c 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
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=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	5.197449589603466
Encrypted:	false
SSDEEP:	6:mDhUxjyq2PWXp+N23iKKdK25+Xqx8chI+IFUtp2hUF1ZmwP2hUSbRkwOWXp+N23U:IUxjyva5KkTXfchI3FUtpYUn/PYUyR5M
MD5:	5E5DBB38B384DE481AB54F195B21EDF0
SHA1:	B2A99D35E994FA04EF058939465FC8BEDDDDAE50
SHA-256:	77D9BEE660C10562AB9177443C0571740B3335BE7FA39F3113ADED595328204C
SHA-512:	4D2E2CB47AFE9632347AE2DD9DF227896835EE70C7A204963E992627D9257DC68135B29C3FD931A366CB8AFBECE73113003C30AE9871F98D4E066F9941BF472
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.153 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-00:58:20.155 1010 Recovering log #3.2021/08/04-00:58:20.156 1010 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.197449589603466
Encrypted:	false
SSDEEP:	6:mDhUxjyq2PWXp+N23iKKdK25+Xqx8chI+IFUtp2hUF1ZmwP2hUSbRkwOWXp+N23U:IUxjyva5KkTXfchI3FUtpYUn/PYUyR5M
MD5:	5E5DBB38B384DE481AB54F195B21EDF0
SHA1:	B2A99D35E994FA04EF058939465FC8BEDDDDAE50
SHA-256:	77D9BEE660C10562AB9177443C0571740B3335BE7FA39F3113ADED595328204C
SHA-512:	4D2E2CB47AFE9632347AE2DD9DF227896835EE70C7A204963E992627D9257DC68135B29C3FD931A366CB8AFBECE73113003C30AE9871F98D4E066F9941BF472
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.153 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-00:58:20.155 1010 Recovering log #3.2021/08/04-00:58:20.156 1010 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):	5.156844113666705
Encrypted:	false
SSDEEP:	6:mDhU29jyq2PWXp+N23iKKdK25+XuoIFUtp2hU0uVu1ZmwP2hU0uV4RkwOWXp+N2R:IU29jyva5KkTXYFUtpYUw/PYUAR5f5Ky
MD5:	80514E752CF133866157AD8FCFC2051E
SHA1:	6ADA93FD9F9FCB09B15CA4BEEAE0A2861944BF0C
SHA-256:	9B51DCA849C7FD4ACF28F60E152F6C4599A9B96DB15147E1426EF85B7A0A2482
SHA-512:	1AFBAFB27580BFB89E1F9ADCE2083ECF39A359E69C43AF13556941BB56C031C4ACCF2BE20362C55FAA4D2F5F23565CE5F1D14357D8D0254F4DB9685E6116A14
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.145 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-00:58:20.147 1010 Recovering log #3.2021/08/04-00:58:20.147 1010 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.156844113666705
Encrypted:	false
SSDEEP:	6:mDhU29jyq2PWXp+N23iKKdK25+XuoIFUtp2hU0uVu1ZmwP2hU0uV4RkwOWXp+N2R:IU29jyva5KkTXYFUtpYUw/PYUAR5f5Ky
MD5:	80514E752CF133866157AD8FCFC2051E
SHA1:	6ADA93FD9F9FCB09B15CA4BEEAE0A2861944BF0C
SHA-256:	9B51DCA849C7FD4ACF28F60E152F6C4599A9B96DB15147E1426EF85B7A0A2482
SHA-512:	1AFBAFB27580BFB89E1F9ADCE2083ECF39A359E69C43AF13556941BB56C031C4ACCF2BE20362C55FAA4D2F5F23565CE5F1D14357D8D0254F4DB9685E6116A14
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.145 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-00:58:20.147 1010 Recovering log #3.2021/08/04-00:58:20.147 1010 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):	5.178400969431029
Encrypted:	false
SSDEEP:	6:mDhvqjyq2PWXp+N23iKKdKWT5g1IdqIFUtp2he1ZmwP2hIRkwOWXp+N23iKKdKW4:Ivqjyva5Kkg5gSRFUtpYI/PYIR5f5Kkn
MD5:	09C1CF2FA0ECFE78BDC9BB46DBB422CA
SHA1:	5A3A8B6FA4EF08ABE9374EF4D9D58CBA1F006A8E
SHA-256:	1E16934D2C37DA3C00D816AB96E146B68F6EE83DDE2FE6F43AF4821F84FD7573
SHA-512:	35C7304517791EE3D21B1FA95C4F630A63AECCA6C47BF7B0CEEABB7CDCB5991B6470B5ABF82CC9B825D6B7C661CF65A6BC2129A64799D2232F442FFAA33925E4E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.065 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-00:58:20.067 1010 Recovering log #3.2021/08/04-00:58:20.067 1010 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old.d (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.178400969431029
Encrypted:	false
SSDEEP:	6:mDhvqjyq2PWXp+N23iKKdKWT5g1IdqIFUtp2he1ZmwP2hIRkwOWXp+N23iKKdKW4:Ivqjyva5Kkg5gSRFUtpYI/PYIR5f5Kkn
MD5:	09C1CF2FA0ECFE78BDC9BB46DBB422CA
SHA1:	5A3A8B6FA4EF08ABE9374EF4D9D58CBA1F006A8E
SHA-256:	1E16934D2C37DA3C00D816AB96E146B68F6EE83DDE2FE6F43AF4821F84FD7573
SHA-512:	35C7304517791EE3D21B1FA95C4F630A63AECCA6C47BF7B0CEEABB7CDCB5991B6470B5ABF82CC9B825D6B7C661CF65A6BC2129A64799D2232F442FFAA33925E4E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.065 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-00:58:20.067 1010 Recovering log #3.2021/08/04-00:58:20.067 1010 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09076029360900889
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvSt7WPoOo/lCxthiZNCGCxC+/erYEzc:TL+A/ONuQDCGI/Ww
MD5:	52AA9D108722D006945AAF75E63F93A5
SHA1:	B0F0EF594B8B1A98324DE5BBB3D3D24DD630F832
SHA-256:	2454AA244800916B0533209A1B109578E9F53B61787C88CE1203822F1009C5F7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
SHA-512:	FF07EDCD4B9C13A13AA0F1F8D9DBC371B64B03910F8FD5F81E8E92BDE300D000779DE2436E5A0A5148B3544DEAF0B7DB69D0A2DA41A5D6D58A31C1AE3B2EA FE7
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):	33356
Entropy (8bit):	0.04707693496830768
Encrypted:	false
SSDEEP:	6:a/G9j/s0/hK/a/IXE/8/2li/pg9bNFlWCj/lil3n:q0bsUYqIXkcCypqLBj/Q3n
MD5:	2332D1E5B69408B18556CB668FF3E2BB
SHA1:	4CEC8FE6327E6FE7BAEEB641BE978FC2C17F04A8
SHA-256:	C9EC9C36B141CBA86D84DFF19946A5D9B588AE35B7BF0E2F7BEF9A720E981992
SHA-512:	35A5ADAAEC69DAF1F07128225E54EE615B66B1B4B68487A1E396B0B2AB264409CADCC85B297338C4A322B3BAFCFC5101AE47AB32DFD6E020CE55844BCAE8D 0EA
Malicious:	false
Reputation:	low
Preview:	.....H8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Sessione (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	949
Entropy (8bit):	3.1978879262712128
Encrypted:	false
SSDEEP:	12:3olydJhvAxddhPlpxlpN8kIyTpelYAejIcpKIClmW9lptlpl:34S5IDlrlAqJ/X4lLlL
MD5:	0CFABA79F0FCCC5EC8485E3F65794F64
SHA1:	F29B86DD24B7D4D5A4A0E72A6CBAFDFA17708A05
SHA-256:	CAB00A318BBA0048B3BA71BC51830D0493C354331F18E4F60A9BE9A6D990F094
SHA-512:	117EAFDF8B9F18A900C5E05FAA1281D0DC8BC8F0741CC4D97682144B57FB65DA71CE5E71D8BA2AED440CDDD5874E91AA9B5D88B5FCA3308FBAE0754F7149D E74
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...bed85c44_8f3b_4394_9b46_684ee49345c6..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....1.,.....http://7news.cdn.7vodcloud.io/.....h. .....`.....2.J*....3.J*.....D.....h.t.t.p.:././.7.n.e.w.s...c.d.n...7.v.o.d.c.l.o.u.d...i.o./.....8.....0.....8. ....http://7news.cdn.7vodcloud.io/....."..rM'/..... .....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.477054506443696
Encrypted:	false
SSDEEP:	48:zBGEPa7iMZ8db0l17bQSefgGGNrS0U9RdiN9rr:ja7iMadb0l17bQ5fgGarS0N
MD5:	C02ABD49342AA87A0256465E989581B8
SHA1:	6521E1A7BD0928946545A4E87A6094B0666D4154
SHA-256:	E2DC0318CDE2EB3AA5C4B57D1E9435637993FA255BF46069F54882756B22DA1B
SHA-512:	C37E2FD8EEEA1F564B099948B560D8F01364CE640DD8A3FFAB7EFF4D031C53C6B273589FA32ECB308958D740E29C8F0254850F6D8C9B10D91AAAD130E93234F
Malicious:	false
Reputation:	low
Preview:	.y.B...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..725833000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-04 00:58:21.97][INFO][mr.Init] MR instance ID: 5ee78983-1582-4b1f-abaf-4688b409db85\n","[2021-08-04 00:58:21.97][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-04 00:58:21.97][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-04 00:58:21.97][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-04 00:58:21.97][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-04 00:58:21.97][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-04 00:58:21.97][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.213345574982051
Encrypted:	false
SSDEEP:	6:myyt+q2PWXp+N23iKKdK8a2jMGIFUtpv6UdNZmwPv6bFNVkwOWXp+N23iKKdK8as:Dva5Kk8EFUtpSIN/PShz5f5Kk8bJ
MD5:	2541ADED876CF0E88940923D9992BFBD
SHA1:	AC4A6A0A500322E91591062DF15625173ECBC82E
SHA-256:	0F66CB9B5A1FE0DB80581E8A9452F099D12D986341D56D28B4B7F9FE7295191A
SHA-512:	14B8CDD8267CB457ACA9529B193031C9469F28CAB8C9BB8C34715CCC0ACF147013E4B85F8AEAACD6B4789318646BA9DF76A378A77A1BA667E139976C39D325B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.489 17f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:58:14.491 17f8 Recovering log #3.2021/08/04-00:58:14.492 17f8 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.oldg (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.213345574982051
Encrypted:	false
SSDEEP:	6:myyt+q2PWXp+N23iKKdK8a2jMGIFUtpv6UdNZmwPv6bFNVkwOWXp+N23iKKdK8as:Dva5Kk8EFUtpSIN/PShz5f5Kk8bJ
MD5:	2541ADED876CF0E88940923D9992BFBD
SHA1:	AC4A6A0A500322E91591062DF15625173ECBC82E
SHA-256:	0F66CB9B5A1FE0DB80581E8A9452F099D12D986341D56D28B4B7F9FE7295191A
SHA-512:	14B8CDD8267CB457ACA9529B193031C9469F28CAB8C9BB8C34715CCC0ACF147013E4B85F8AEAACD6B4789318646BA9DF76A378A77A1BA667E139976C39D325B
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.489 17f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:58:14.491 17f8 Recovering log #3.2021/08/04-00:58:14.492 17f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State1e (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 State1e (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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.252340293797617
Encrypted:	false
SSDEEP:	6:myWQGqM+q2PWXp+N23iKKdKgXz4rRIFUtpvWGZmwPvW0LlMVkwOWXp+N23iKKdKt:eQpM+va5KkgXiuFUtpuG/Pu0LlMV5f5j
MD5:	9CC8E9B784F39943D948041C04F9E4AF
SHA1:	ED3D2F9A74ED5ED244FA00ECB5353BCF8833DAD7
SHA-256:	1424B53A11806651707471F8A6686BE981EAE400E0414EAE34A08AD3723A0479
SHA-512:	07C596ED4AF0836DA0A6F281F1065A5E3C234AB0226C5DD570D6AF9BA0454F6E4FDF5853D1627C0B0AB96FD011185A7CBDD19D3DB46924D6B564DA02EE0869 8
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.815 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/ 08/04-00:58:14.818 176c Recovering log #3.2021/08/04-00:58:14.819 176c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.252340293797617
Encrypted:	false
SSDEEP:	6:myWQGqM+q2PWXp+N23iKKdKgXz4rRIFUtpvWGZmwPvW0LlMVkwOWXp+N23iKKdKt:eQpM+va5KkgXiuFUtpuG/Pu0LlMV5f5j
MD5:	9CC8E9B784F39943D948041C04F9E4AF
SHA1:	ED3D2F9A74ED5ED244FA00ECB5353BCF8833DAD7
SHA-256:	1424B53A11806651707471F8A6686BE981EAE400E0414EAE34A08AD3723A0479
SHA-512:	07C596ED4AF0836DA0A6F281F1065A5E3C234AB0226C5DD570D6AF9BA0454F6E4FDF5853D1627C0B0AB96FD011185A7CBDD19D3DB46924D6B564DA02EE0869 8
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.815 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/ 08/04-00:58:14.818 176c Recovering log #3.2021/08/04-00:58:14.819 176c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences.r (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):	5742
Entropy (8bit):	5.184932519953728
Encrypted:	false
SSDEEP:	96:nCCdqF9xyOcKIcrok0JCKL80kZ1zbOTQVuwn:nCC498OcqG4KbkZN
MD5:	A2466D0AF4CDC496A86F911CD8760114
SHA1:	400B851C6E0DB39D045D482B57F1E3C8560033BB
SHA-256:	D50DCF45A71D02E096294897E47858107CC1110B06B964A0205CAFCCFD675D0A
SHA-512:	F032674A47FC93E55A37C19A3D7E1D5E43DE9141AAA9095C012285811BA8D522BFA3EC19BB1BFB54C74E4C704737F33B166F8010EE7F9031F90314DEF7908749

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences.r (copy)	
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272537494744686","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\PreferencesP (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):	5742
Entropy (8bit):	5.184932519953728
Encrypted:	false
SSDEEP:	96:nCCdqF9xyOcKIcrok0JCKL80kZ1zbOTQVuwn:nCC498OcqG4KbkZN
MD5:	A2466D0AF4CDC496A86F911CD8760114
SHA1:	400B851C6E0DB39D045D482B57F1E3C8560033BB
SHA-256:	D50DCF45A71D02E096294897E47858107CC1110B06B964A0205CAFCCFD675D0A
SHA-512:	F032674A47FC93E55A37C19A3D7E1D5E43DE9141AAA9095C012285811BA8D522BFA3EC19BB1BFB54C74E4C704737F33B166F8010EE7F9031F90314DEF7908749
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272537494744686","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	1.1786848321706758
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU9oTRs/oTRse9l:wIElwQF8mpcSibYro1
MD5:	35820F9F1261460313C5C904BC0AE7EB
SHA1:	34C0C29B12360EFCD697DF03BEA262464BCB1462
SHA-256:	2ED60650DB467F52D5C4AB57F2011A912F8B656ACB79A08802981A12FC571E94
SHA-512:	E1E7975B99CEC4B8F8CCAE0DEE5D5F144D17F3E009F561A4D905FB6C02FA04D41879A15AEA53575D3529F42F2059AF2756233568EC60545B10939505FD9E8041
Malicious:	false
Reputation:	low

Preview:

SQLite format 3......@ ....C.........g...^........j..
....
....
....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8262688549592127
Encrypted:	false
SSDEEP:	48:Rk1WqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU26:uohIElwQF8mpcSv
MD5:	16C4C7FF704BB649E815490AC34E7B6F
SHA1:	DD722DDC49CD8B31952C4D65F35A15AF324ADEE3
SHA-256:	67CFF2BE161BF5AF32786C775C4850214EB2F5FA6D9F9FDE41A26D25B017E8F5
SHA-512:	A80A264B1BD16E859AFB366579324CFFACE7676EBBB224539A0A0275DC8FFA02F0C51BB3CB3BE37EA47FF0AB135564E70B9D346D3D2240B84806A0A4171F42EB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Preview:	.....6^..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.536127470728629
Encrypted:	false
SSDEEP:	384:UMBt/LlZwXv1kXqKf/pUZNCgVLH2HfDBrUNHG1nTow8T48a:3LlUv1kXqKf/pUZNCgVLH2Hf1rUxG1n7
MD5:	894CF6D5D7D3979A4FCBB98440B880BD
SHA1:	6CED053FD56609AD5EDFFC38D8D93A558F29ED7C
SHA-256:	23E213962E1894E636A840DE1209577A1FFBAC41770ECDF8079D5E305C80D862
SHA-512:	9CA6BE2522DD3507DB0462A4416A7751A3E1018089BFBA09E30A0D30AA3B296147CA653E17B409DDDECD47A1C7FA39027E3CAFD9DDE4BA062AABABA90A69F8D6
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":"13272537494445856","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.211419340117859
Encrypted:	false
SSDEEP:	6:myEOq2PWXp+N23iKKdKrQMxIFUtpvQHZZmwPvQHzkwOWXp+N23iKKdKrQMFLJ:Nva5KkCFUtpYHZ/PYHz5f5KktJ
MD5:	DC1CB3A8AF71B0B85CF0543B118BF6D3
SHA1:	E894AFD89D59B0461E1F108623DC2FBA66F35504
SHA-256:	EEA780DD0D15816B55660C6F6562E473C02DA8FE4446D1D7F6FDB3B1E3F662D7
SHA-512:	D74DD068D5A6CE6DD5708CA09BB436A7C8453D88E5D4309F1ECAF852E06A6DCA66C89707C5D7D93F24C2D0081755FE0BEA355B29761FA7407C31B3E3266EF87
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.735 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-00:58:14.737 864 Recovering log #3.2021/08/04-00:58:14.737 864 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.211419340117859
Encrypted:	false
SSDEEP:	6:myEOq2PWXp+N23iKKdKrQMxIFUtpvQHZZmwPvQHzkwOWXp+N23iKKdKrQMFLJ:Nva5KkCFUtpYHZ/PYHz5f5KktJ
MD5:	DC1CB3A8AF71B0B85CF0543B118BF6D3
SHA1:	E894AFD89D59B0461E1F108623DC2FBA66F35504
SHA-256:	EEA780DD0D15816B55660C6F6562E473C02DA8FE4446D1D7F6FDB3B1E3F662D7
SHA-512:	D74DD068D5A6CE6DD5708CA09BB436A7C8453D88E5D4309F1ECAF852E06A6DCA66C89707C5D7D93F24C2D0081755FE0BEA355B29761FA7407C31B3E3266EF87
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.735 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-00:58:14.737 864 Recovering log #3.2021/08/04-00:58:14.737 864 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):	5.188928969408851
Encrypted:	false
SSDEEP:	6:my2SFMq2PWXp+N23iKKdK7Uh2ghZIFUtpvJRXZmwPvBkwOWXp+N23iKKdK7Uh2gd:OS+va5KklhHh2FUtph9/PZ5f5KklhHLJ
MD5:	CC7797DA94058B523C36D92BDE174D9E
SHA1:	E3F620C4C1EA72B8984626DC54BA62CB00FC79F0
SHA-256:	AA20E0565C0A9BB628048AD2C74462E506F1A795245CF51138EF2B9F4545531C
SHA-512:	90CCC3F90A45FD72E36C736D0E5A6E5E951470782D694CBD7EF4AD141B6326E0F21AA1409C42059E01C85EB2FE2A14BD932DBCFFF5EB66F7F2CA81A2C36E9ECE
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.457 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/04-00:58:14.460 1764 Recovering log #3.2021/08/04-00:58:14.464 1764 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):	5.188928969408851
Encrypted:	false
SSDEEP:	6:my2SFMq2PWXp+N23iKKdK7Uh2ghZIFUtpvJRXZmwPvBkwOWXp+N23iKKdK7Uh2gd:OS+va5KklhHh2FUtph9/PZ5f5KklhHLJ
MD5:	CC7797DA94058B523C36D92BDE174D9E
SHA1:	E3F620C4C1EA72B8984626DC54BA62CB00FC79F0
SHA-256:	AA20E0565C0A9BB628048AD2C74462E506F1A795245CF51138EF2B9F4545531C
SHA-512:	90CCC3F90A45FD72E36C736D0E5A6E5E951470782D694CBD7EF4AD141B6326E0F21AA1409C42059E01C85EB2FE2A14BD932DBCFFF5EB66F7F2CA81A2C36E9ECE
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.457 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/04-00:58:14.460 1764 Recovering log #3.2021/08/04-00:58:14.464 1764 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\8978d707-6a67-4f32-add8-d7380b00d42b.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\8978d707-6a67-4f32-add8-d7380b00d42b.tmp	
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):	5.289045280834078
Encrypted:	false
SSDEEP:	6:my1qM+q2PWXp+N23iKKdKusNpV/2jMGIFUtpvvZmwPv3pMVkwOWXp+N23iKKdKux:cM+va5KkFFUtpH/PfpMV5f5KkOJ
MD5:	1FB03EAC1F42C4D9133F1F788DE8E2BF
SHA1:	524FDCB3FCDF68EC241EA6F01687B83A503285B5
SHA-256:	636327CFB754F4C41A0B7238F3B66504A5F1DA4253B1AA58AA082E9DED13671C
SHA-512:	A2F33D56BA0F31DA5FD3DA5175C12E660BF8FB1370D3702204531C744285B34702874E9DFB3E6A6EA7A89B037DD3594DFBAE89B1FE69D7346559C677A976C89
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.751 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:58:14.753 176c Recovering log #3.2021/08/04-00:58:14.754 176c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.289045280834078
Encrypted:	false
SSDEEP:	6:my1qM+q2PWXp+N23iKKdKusNpV/2jMGIFUtpvvZmwPv3pMVkwOWXp+N23iKKdKux:cM+va5KkFFUtpH/PfpMV5f5KkOJ
MD5:	1FB03EAC1F42C4D9133F1F788DE8E2BF
SHA1:	524FDCB3FCDF68EC241EA6F01687B83A503285B5
SHA-256:	636327CFB754F4C41A0B7238F3B66504A5F1DA4253B1AA58AA082E9DED13671C
SHA-512:	A2F33D56BA0F31DA5FD3DA5175C12E660BF8FB1370D3702204531C744285B34702874E9DFB3E6A6EA7A89B037DD3594DFBAE89B1FE69D7346559C677A976C89
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.751 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:58:14.753 176c Recovering log #3.2021/08/04-00:58:14.754 176c 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 StateTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.255371476101857
Encrypted:	false
SSDEEP:	12:eQU+va5KkmiuFUtpunFmW/Pu0V5f5Kkm2J:9Va5KkSg6mEf5Kkr
MD5:	E6BD1EA560D9FEC17D2388ECD077030C
SHA1:	1149091E9DEA8A31E3C99B51276839235AA364C6
SHA-256:	B59C23D7F7121FA5FE4D78C210E808044CE66E1726CC23BACBA293D827AB925E
SHA-512:	790FBA36894BEF88C31C7C7D1ACF56899BE0D387B5B419B8A6655B1E815F7D737B0267D96C960627A3FAEC19C25C6FE35AD73831DEEA5A5E7F666F4392C870D 4
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.815 1ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/08/04-00:58:14.817 1ec Recovering log #3.2021/08/04-00:58:14.818 1ec 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):	5.255371476101857
Encrypted:	false
SSDEEP:	12:eQU+va5KkmiuFUtpunFmW/Pu0V5f5Kkm2J:9Va5KkSg6mEf5Kkr
MD5:	E6BD1EA560D9FEC17D2388ECD077030C
SHA1:	1149091E9DEA8A31E3C99B51276839235AA364C6
SHA-256:	B59C23D7F7121FA5FE4D78C210E808044CE66E1726CC23BACBA293D827AB925E
SHA-512:	790FBA36894BEF88C31C7C7D1ACF56899BE0D387B5B419B8A6655B1E815F7D737B0267D96C960627A3FAEC19C25C6FE35AD73831DEEA5A5E7F666F4392C870D 4
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.815 1ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/08/04-00:58:14.817 1ec Recovering log #3.2021/08/04-00:58:14.818 1ec 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.278517281171351
Encrypted:	false
SSDEEP:	6:mVlSlM+q2PWXp+N23iKKdKusNpZQMxIFUtpU+jZmwPUTqMVkwOWXp+N23iKKdKuG:LlM+va5KkMFUtpvj/PvMV5f5KkTJ
MD5:	26FD21D476ED8C76690B3E09F1C9310E
SHA1:	0CA78ED6A4F1A4D2EE5F9BF23F79867273F141FE
SHA-256:	E3C48C1AF6FBD2720A4FEC44BD72D53E27E7642D923875DED521839FCC2C8D0F
SHA-512:	0C66F163D696251A8F5CC96F9E4E7C8F1A1D0ABE98F795D645CE0980B79CF137AC776E3DD279EC32B560AAE85B71DFF003FBA18706608893CD7B2ECF318301
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:31.061 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/04-00:58:31.062 176c Recovering log #3.2021/08/04-00:58:31.063 176c Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.278517281171351
Encrypted:	false
SSDEEP:	6:mVlSlM+q2PWXp+N23iKKdKusNpZQMxIFUtpU+jZmwPUTqMVkwOWXp+N23iKKdKuG:LlM+va5KkMFUtpvj/PvMV5f5KkTJ
MD5:	26FD21D476ED8C76690B3E09F1C9310E
SHA1:	0CA78ED6A4F1A4D2EE5F9BF23F79867273F141FE
SHA-256:	E3C48C1AF6FBD2720A4FEC44BD72D53E27E7642D923875DED521839FCC2C8D0F
SHA-512:	0C66F163D696251A8F5CC96F9E4E7C8F1A1D0ABE98F795D645CE0980B79CF137AC776E3DD279EC32B560AAE85B71DFF003FBA18706608893CD7B2ECF318301
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:31.061 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/04-00:58:31.062 176c Recovering log #3.2021/08/04-00:58:31.063 176c 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\36960312-8e31-4ae0-be98-31ccfa181d43.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1

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):	5.201201983945317
Encrypted:	false
SSDEEP:	12:IIova5KkkGHArBFUtpYj5/PYS5f5KkkGHAryJ:ITa5KkkGgPg2mcf5KkkGga
MD5:	6C02EE341DEF65047BE4C3B5DD9CAA20
SHA1:	FB958B9E1B75444D18D9A3FDBA341C34F3383153
SHA-256:	75D9205A9E0D3F29CCBBF90BB19EA8A41A9B6539399F61037164426CFCD323B6
SHA-512:	61CE8A21B1756C4D66AF2752BEFD79E3A2A9DDE0896277BD69C25B98940C474ABD0A8D6CF46251FB39E79CD5F867190379D6AA62F37269CCCAEEC4439D4687 1
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.698 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:58:20.701 864 Recovering log #3.2021/08/04-00:58:20.702 864 Reusing old log C:\Users\user\AppD ata\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):	5.201201983945317
Encrypted:	false
SSDEEP:	12:IIova5KkkGHArBFUtpYj5/PYS5f5KkkGHAryJ:ITa5KkkGgPg2mcf5KkkGga
MD5:	6C02EE341DEF65047BE4C3B5DD9CAA20
SHA1:	FB958B9E1B75444D18D9A3FDBA341C34F3383153
SHA-256:	75D9205A9E0D3F29CCBBF90BB19EA8A41A9B6539399F61037164426CFCD323B6
SHA-512:	61CE8A21B1756C4D66AF2752BEFD79E3A2A9DDE0896277BD69C25B98940C474ABD0A8D6CF46251FB39E79CD5F867190379D6AA62F37269CCCAEEC4439D4687 1
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.698 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:58:20.701 864 Recovering log #3.2021/08/04-00:58:20.702 864 Reusing old log C:\Users\user\AppD ata\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy)	
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):	432
Entropy (8bit):	5.200510743134386
Encrypted:	false
SSDEEP:	12:ILh9+va5KkkGHArqiuFUtpYjH3J/PYu9V5f5KkkGHArq2J:ILhKa5KkkGgCg2r3KuVf5KkkGg7
MD5:	6461B9D457D24C0F9B7D320217C7ECE8
SHA1:	8F0A20A9AB9CC14135DBFFD55FC63C28B8C6913B
SHA-256:	955B58319CF7B2D1514A761D0CFA86D789DFA1F98627D98AFA32364D804A0813
SHA-512:	14E419F475C87458A3A8BB183113A87B9C171F10D9BAC813D977B8A8AA953D6761F0150BDF8CB4A428761B520DC7250C8FE741D94E9B6D85CAA48DE3C947F79
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.699 140c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/04-00:58:20.701 140c Recovering log #3.2021/08/04-00:58:20.702 140c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.200510743134386
Encrypted:	false
SSDEEP:	12:ILh9+va5KkkGHArqiuFUtpYjH3J/PYu9V5f5KkkGHArq2J:ILhKa5KkkGgCg2r3KuVf5KkkGg7
MD5:	6461B9D457D24C0F9B7D320217C7ECE8
SHA1:	8F0A20A9AB9CC14135DBFFD55FC63C28B8C6913B
SHA-256:	955B58319CF7B2D1514A761D0CFA86D789DFA1F98627D98AFA32364D804A0813
SHA-512:	14E419F475C87458A3A8BB183113A87B9C171F10D9BAC813D977B8A8AA953D6761F0150BDF8CB4A428761B520DC7250C8FE741D94E9B6D85CAA48DE3C947F79
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.699 140c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/04-00:58:20.701 140c Recovering log #3.2021/08/04-00:58:20.702 140c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.199408955252712
Encrypted:	false
SSDEEP:	12:oO+va5KkkGHArAFUtp4FmW/P40V5f5KkkGHArfJ:oHa5KkkGgkgOFmLef5KkkGgV
MD5:	6C6D5A4B2C28C06B9A5D0F65F10B34E1
SHA1:	C5B3F684B5CA53108107C25DCC50B05BDDEF802A
SHA-256:	8A07C5C7534B8EDB04DD9EB3C16A1E1989CDC5749E7F10EA58EDDD28BE3B5A7F
SHA-512:	18158D109B2E8A804110342A70CD70B31DD4C0058FF4A91330DB5294037F92F9D49091383F7269B065016EA2E55A97A73FB2D4DD607B32D19370F04AB5AF5A32
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:35.916 1ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/04-00:58:35.917 1ec Recovering log #3.2021/08/04-00:58:35.918 1ec 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):	5.199408955252712
Encrypted:	false
SSDEEP:	12:oO+va5KkkGHArAFUtp4FmW/P40V5f5KkkGHArfJ:oHa5KkkGgkgOFmLef5KkkGgV
MD5:	6C6D5A4B2C28C06B9A5D0F65F10B34E1
SHA1:	C5B3F684B5CA53108107C25DCC50B05BDDEF802A
SHA-256:	8A07C5C7534B8EDB04DD9EB3C16A1E1989CDC5749E7F10EA58EDDD28BE3B5A7F
SHA-512:	18158D109B2E8A804110342A70CD70B31DD4C0058FF4A91330DB5294037F92F9D49091383F7269B065016EA2E55A97A73FB2D4DD607B32D19370F04AB5AF5A32
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:35.916 1ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/04-00:58:35.917 1ec Recovering log #3.2021/08/04-00:58:35.918 1ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.248734389238185
Encrypted:	false
SSDEEP:	6:my2WFB1M+q2PWXp+N23iKKdKpIFUtpv2SFYZmwPv27MVkwOWXp+N23iKKdKa/WLJ:OWJM+va5KkmFUtpeSG/Pe7MV5f5KkaUJ
MD5:	77943013B60FB2E1E1CCA85795C0080E
SHA1:	21DC746A327B3A90EDD39CE65A0A4CB488938197
SHA-256:	7F6498841308AA661AE854CD023E95993C48B88460FB778F396A9A498CB2FC59

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
SHA-512:	DECB59CE6113166EDC92F8E42147732E5ACF8F745923557C185651246872CE44DBFAC29B924A1ED9A789F43FCB9BCADDC8077EF2BCD1EE018E1B5838A4470CE
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.453 dfc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-00:58:14.457 dfc Recovering log #3.2021/08/04-00:58:14.458 dfc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.248734389238185
Encrypted:	false
SSDEEP:	6:my2WFB1M+q2PWXp+N23iKKdKpIFUtpv2SFYZmwPv27MVkwOWXp+N23iKKdKa/WLJ:OWJM+va5KkmFUtpeSG/Pe7MV5f5KkaUJ
MD5:	77943013B60FB2E1E1CCA85795C0080E
SHA1:	21DC746A327B3A90EDD39CE65A0A4CB488938197
SHA-256:	7F6498841308AA661AE854CD023E95993C48B88460FB778F396A9A498CB2FC59
SHA-512:	DECB59CE6113166EDC92F8E42147732E5ACF8F745923557C185651246872CE44DBFAC29B924A1ED9A789F43FCB9BCADDC8077EF2BCD1EE018E1B5838A4470CE
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:14.453 dfc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-00:58:14.457 dfc Recovering log #3.2021/08/04-00:58:14.458 dfc 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):	5.3572088820418795
Encrypted:	false
SSDEEP:	6:mDzIq2PWXp+N23iKKdKks8Y5JKKhdIFUtp2KRXZmwP2tdFkwOWXp+N23iKKdKksp:6Iva5KkkOrsFUtp9X/PudF5f5KkkOrzJ
MD5:	B6ADAD91400B1277430E16CBFE8D8737
SHA1:	3D3B593BB321B8D661493A189FBA82C2BEA2D416
SHA-256:	A4D01F5A1E3A29CA5CC088CF19A7663AA45D0E1F114F1FE7C219C3F32EE4A88C
SHA-512:	063D9A70AFB91B2E27CDB0A667D33EE9AA89671CAF885737E7EEC5DC110013A13C50DE96490DC044C9B776F1FCA248C97959BE5966CAC92E0BB1F6750821B09
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:21.953 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/04-00:58:21.954 864 Recovering log #3.2021/08/04-00:58:21.955 864 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
Size (bytes):	399
Entropy (8bit):	5.3572088820418795
Encrypted:	false
SSDEEP:	6:mDzIq2PWXp+N23iKKdKks8Y5JKKhdIFUtp2KRXZmwP2tdFkwOWXp+N23iKKdKksp:6Iva5KkkOrsFUtp9X/PudF5f5KkkOrzJ
MD5:	B6ADAD91400B1277430E16CBFE8D8737
SHA1:	3D3B593BB321B8D661493A189FBA82C2BEA2D416
SHA-256:	A4D01F5A1E3A29CA5CC088CF19A7663AA45D0E1F114F1FE7C219C3F32EE4A88C
SHA-512:	063D9A70AFB91B2E27CDB0A667D33EE9AA89671CAF885737E7EEC5DC110013A13C50DE96490DC044C9B776F1FCA248C97959BE5966CAC92E0BB1F6750821B09
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:21.953 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/04-00:58:21.954 864 Recovering log #3.2021/08/04-00:58:21.955 864 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.567067380713962
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvN7wUXRUenHQ:YI6UUhVseKUewqPeUer2UefNwUBUenw
MD5:	41295EED287BA10D02242FFAB1EBCAF2
SHA1:	9065B0CF392E147B6DDE2523CD972DCF5872EFDA
SHA-256:	B30412146AB3E9EA2B2EAFC5E23CB5CDB459723EA0A5FAF150D1BBCAD3A883E1
SHA-512:	449E39B48895C64BC4AFC759A316F5D1AE931882B5970647EDD4666B0CA0524D484AA28BD842ADAACE57386A68726EF0AF87E07CBCFCAA0A4E270E9EDA012E D8
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_inc lude_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mo de":"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":1659599897.660061,"host":"8/RrMmQlCD2Gsp 14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628063897.660066},{"expiry":1633014077.462534,"hos t":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:xlqMn:xpn
MD5:	97C3660EEBAD73E6C81D6F56ADEAFAB6
SHA1:	608072CE6181D03FDE12C9A16B90B127D701D4DB
SHA-256:	64F44B846EA788C867BDC7E43530D9CC5B4EB7D2A7236BC37844451D40149C61
SHA-512:	56E81212129248AE14546D0A61E99CE28BD3B6330977D890EDB13CD75D6817CEF9C9EC9D4ED511B8C66F615E3660504174E6BBC997497C53A810FC64117F397A
Malicious:	false
Reputation:	low
Preview:	.....S..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b18f4bc7-033e-412e-9b91-7b3f42745f2c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	22596
Entropy (8bit):	5.536127470728629
Encrypted:	false
SSDEEP:	384:UMBt/LlZwXv1kXqKf/pUZNCgVLH2HfDBrUNHG1nTow8T48a:3LlUv1kXqKf/pUZNCgVLH2Hf1rUxG1n7
MD5:	894CF6D5D7D3979A4FCBB98440B880BD
SHA1:	6CED053FD56609AD5EDFFC38D8D93A558F29ED7C
SHA-256:	23E213962E1894E636A840DE1209577A1FFBAC41770ECDF8079D5E305C80D862
SHA-512:	9CA6BE2522DD3507DB0462A4416A7751A3E1018089BFBA09E30A0D30AA3B296147CA653E17B409DDDECD47A1C7FA39027E3CAFD9DDE4BA062AABABA90A69F 8D6
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272537494445856","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c7d4e1ae-19fa-46b6-8ea3-058a7a83ffaf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c7d4e1ae-19fa-46b6-8ea3-058a7a83ffaf.tmp	
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cf34f05e-0256-4032-a72d-77fc09d6eb1e.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\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.461120918367275
Encrypted:	false
SSDEEP:	3:tUK6uiuVUvj1Zmwv3lujRaUvhH1V8sIujQuVUVbH1WGv:mXz1ZmwP3fbVv3VUVhtv
MD5:	C21DD56727E3E558D541D8A9FD2A3D55
SHA1:	A267AD19125BB6F8E8D01AF0A160088F9ECB25B1
SHA-256:	80178C1FF3F4CDB59002B0D1D73B421B29E9C6DFC33358FC5357C6ECEA14187D
SHA-512:	5C40A242BCF65CC5509EA958F9641E095FE3322EF74D10EB30E041034ECA01840029B63721AC6FA72D04BEA1652920178807EB1C1913F3015CD0830C08E6822E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:19.857 1010 Recovering log #3.2021/08/04-00:58:19.964 1010 Delete type=0 #3.2021/08/04-00:58:19.965 1010 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old6 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.461120918367275
Encrypted:	false
SSDEEP:	3:tUK6uiuVUvj1Zmwv3lujRaUvhH1V8sIujQuVUVbH1WGv:mXz1ZmwP3fbVv3VUVhtv
MD5:	C21DD56727E3E558D541D8A9FD2A3D55
SHA1:	A267AD19125BB6F8E8D01AF0A160088F9ECB25B1
SHA-256:	80178C1FF3F4CDB59002B0D1D73B421B29E9C6DFC33358FC5357C6ECEA14187D
SHA-512:	5C40A242BCF65CC5509EA958F9641E095FE3322EF74D10EB30E041034ECA01840029B63721AC6FA72D04BEA1652920178807EB1C1913F3015CD0830C08E6822E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:19.857 1010 Recovering log #3.2021/08/04-00:58:19.964 1010 Delete type=0 #3.2021/08/04-00:58:19.965 1010 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.1838366726780185
Encrypted:	false
SSDEEP:	6:mDhWzMq2PWXp+N23iKKdKfrzAdIFUtp2hWAZZmwP2hWhkwOWXp+N23iKKdKfrzId:Idva5Kk9FUtpYF/PYe5f5Kk2J
MD5:	3679BE67BCEDF17CCD08A501905813DF
SHA1:	AC17FC356C55AC48B2F1C0ECD384AE5CCF4B4624

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
SHA-256:	4A2ECD944D995F53D210B1A324BA9D15209584C87434AB42A33169334EAB5D0F
SHA-512:	88E625F18F785DC7B3702E4342DFBF876C00F26E0B00A9551D73806D276FEAF64BB759629242952FF9AB6F9CA22CD2B927B0D908C97A8D19D84E4BB893881766
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.322 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021 /08/04-00:58:20.323 864 Recovering log #3.2021/08/04-00:58:20.324 864 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shar ed_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old8 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.1838366726780185
Encrypted:	false
SSDEEP:	6:mDhWzMq2PWXp+N23iKKdKfrzAdIFUtp2hWAZZmwP2hWhkwOWXp+N23iKKdKfrzId:Idva5Kk9FUtpYF/PYe5f5Kk2J
MD5:	3679BE67BCEDF17CCD08A501905813DF
SHA1:	AC17FC356C55AC48B2F1C0ECD384AE5CCF4B4624
SHA-256:	4A2ECD944D995F53D210B1A324BA9D15209584C87434AB42A33169334EAB5D0F
SHA-512:	88E625F18F785DC7B3702E4342DFBF876C00F26E0B00A9551D73806D276FEAF64BB759629242952FF9AB6F9CA22CD2B927B0D908C97A8D19D84E4BB893881766
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:58:20.322 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021 /08/04-00:58:20.323 864 Recovering log #3.2021/08/04-00:58:20.324 864 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shar ed_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Reputation:	low
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Size (bytes):	174336
Entropy (8bit):	6.079335192781154
Encrypted:	false
SSDEEP:	3072:LE2GaYTJQE+mugy9+QV1T7IRwdfLSNPsFcbXafIB0u1GOJmA3iuR9:o7xaV+QfT7GSmh6aqfIlUOoSiuR9
MD5:	96778082E366AA384CBD0B2B40111B8B
SHA1:	49BB6167C1A2C23E123E18BFECE06ED23D56401A
SHA-256:	31B70827AFA4E6A8C6BC593C06D9311EB20A123404E27323751A5565D7499DDB
SHA-512:	134279CEF23C2AB63E96E8581AF89035FF9E1EA105AD433494BB89E0F3BC1F17D75EC7385B9500178C8571EFF5A10ECE3B2FD73738AEF64383E27C854B641E46
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":1.628063897468283e+12,"network":1.628031498e+12,"ticks":4728866921.0,"uncertainty":4363911.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174336
Entropy (8bit):	6.079335192781154
Encrypted:	false
SSDEEP:	3072:LE2GaYTJQE+mugy9+QV1T7IRwdfLSNPsFcbXafIB0u1GOJmA3iuR9:o7xaV+QfT7GSmh6aqfIlUOoSiuR9
MD5:	96778082E366AA384CBD0B2B40111B8B
SHA1:	49BB6167C1A2C23E123E18BFECE06ED23D56401A
SHA-256:	31B70827AFA4E6A8C6BC593C06D9311EB20A123404E27323751A5565D7499DDB
SHA-512:	134279CEF23C2AB63E96E8581AF89035FF9E1EA105AD433494BB89E0F3BC1F17D75EC7385B9500178C8571EFF5A10ECE3B2FD73738AEF64383E27C854B641E46
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":1.628063897468283e+12,"network":1.628031498e+12,"ticks":4728866921.0,"uncertainty":4363911.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\a030d541-3faf-43ae-bd4f-1af3ee3b43d2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174336

C:\Users\user\AppData\Local\Google\Chrome\User Data\a030d541-3faf-43ae-bd4f-1af3ee3b43d2.tmp	
Entropy (8bit):	6.079335192781154
Encrypted:	false
SSDEEP:	3072:LE2GaYTJQE+mugy9+QV1T7IRwdfLSNPsFcbXafIB0u1GOJmA3iuR9:o7xaV+QfT7GSmh6aqfIlUOoSiuR9
MD5:	96778082E366AA384CBD0B2B40111B8B
SHA1:	49BB6167C1A2C23E123E18BFECE06ED23D56401A
SHA-256:	31B70827AFA4E6A8C6BC593C06D9311EB20A123404E27323751A5565D7499DDB
SHA-512:	134279CEF23C2AB63E96E8581AF89035FF9E1EA105AD433494BB89E0F3BC1F17D75EC7385B9500178C8571EFF5A10ECE3B2FD73738AEF64383E27C854B641E46
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":1.628063897468283e+12,"network":1.628031498e+12,"ticks":4728866921.0,"uncertainty":4363911.0}},"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\f1f22501-1cc4-40a6-88e0-73978af8d151.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174336
Entropy (8bit):	6.079335192781154
Encrypted:	false
SSDEEP:	3072:LE2GaYTJQE+mugy9+QV1T7IRwdfLSNPsFcbXafIB0u1GOJmA3iuR9:o7xaV+QfT7GSmh6aqfIlUOoSiuR9
MD5:	96778082E366AA384CBD0B2B40111B8B
SHA1:	49BB6167C1A2C23E123E18BFECE06ED23D56401A
SHA-256:	31B70827AFA4E6A8C6BC593C06D9311EB20A123404E27323751A5565D7499DDB
SHA-512:	134279CEF23C2AB63E96E8581AF89035FF9E1EA105AD433494BB89E0F3BC1F17D75EC7385B9500178C8571EFF5A10ECE3B2FD73738AEF64383E27C854B641E46
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":1.628063897468283e+12,"network":1.628031498e+12,"ticks":4728866921.0,"uncertainty":4363911.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Temp\245a5371-ef18-47f8-baa4-785d7153e300.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(...>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\42f2957f-e68e-4057-8001-752e84049ca8.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

C:\Users\user\AppData\Local\Temp\42f2957f-e68e-4057-8001-752e84049ca8.tmp	
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\573f88f9-c0f1-4ab5-8ef9-51a734493364.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\8dfba44c-4bd5-496e-be74-14bde612e938.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	5446
Entropy (8bit):	4.643243918055364
Encrypted:	false
SSDEEP:	96:wU2pxPHidFuYITFZbRxAECp52QA9WCXE4mT8z8lA8z8eB8oH40fC6neOr:3K7RxHX/AI7AFoNeW
MD5:	4E8A8C059C98305A991650AD97108244
SHA1:	AE0ACDF07509E732F5425A5173880E9BD8B5B18D
SHA-256:	64ED373C4CD268CD7A05FE4C366C3691205ABCE1449ADD60A3DB9224B981EA49
SHA-512:	D4FA3E5C952490A7272A8B5F06BD3CD0C93C89FBB12AA26D99652892EC17D9471F7EE99D50A522364A6989F8965218728CF6F2268B81EA860E6E4D1B4C69CBC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 6aa9a9f8618635ec080b91d2f4c4263c5b7342dfd1d90db3daa9c3321192ebc4 6684da6cf87ff2689e1ec7130a8c2de8e a43f07166a85b00852b03dc4259cb1b.SERVER_HANDSHAKE_TRAFFIC_SECRET 6aa9a9f8618635ec080b91d2f4c4263c5b7342dfd1d90db3daa9c3321192ebc4 e 1d1b947646174c8371c56f96a0601e2c5d7a1b447fef1073719cc03b38614ae.CLIENT_HANDSHAKE_TRAFFIC_SECRET ae2d0adac39b405f659900d12f61a7e32a 1e9a3f3d105753a414aa7064b740cb e05914161494ee79e4aac0e8d0ac50f0eea87dbeec7afca5ea0a4caf5a2bb783.SERVER_HANDSHAKE_TRAFFIC_SECRET ae 2d0adac39b405f659900d12f61a7e32a1e9a3f3d105753a414aa7064b740cb 7e5ca3533034eb51a93882a1ceb96174f2f70d5035f64ccd5c528c1d24483213.CL IENT_HANDSHAKE_TRAFFIC_SECRET a4145d1b24fe462ebe40f337c97c19e0f46c853b9804226063b8a48f51062c76 62c5de03d76fda5431dd5b797f06236c7f9 c3911e9626d92232c805a6eebed41.SERVER_HANDSHAKE_TRAFFIC_SECRET a4145d1b24fe462ebe40f337c97c19e0f46c853b9804226063b8a48f51062c76 735 4a38de7e43bee80e670819ccf3ace2dbeef73dab79b168829501f7af184cd.CLIENT_TRAFFIC_SECRET_0 ae2d

C:\Users\user\AppData\Local\Temp\scoped_dir5728_2079057866\245a5371-ef18-47f8-baa4-785d7153e300.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..& ..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,.. .W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6.. @?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5SI..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

Static File Info

No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/04/21-00:58:16.890603	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49712	13.32.14.64	192.168.2.3
08/04/21-00:58:17.502073	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49712	13.32.14.64	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 4, 2021 00:58:16.642827034 CEST	192.168.2.3	8.8.8.8	0x360f	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:58:16.646042109 CEST	192.168.2.3	8.8.8.8	0xf36c	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 4, 2021 00:58:16.651031971 CEST	192.168.2.3	8.8.8.8	0x95ed	Standard query (0)	7news.cdn.7vodcloud.io	A (IP address)	IN (0x0001)
Aug 4, 2021 00:58:19.710402012 CEST	192.168.2.3	8.8.8.8	0x2736	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 00:58:16.678009987 CEST	8.8.8.8	192.168.2.3	0x360f	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 4, 2021 00:58:16.681098938 CEST	8.8.8.8	192.168.2.3	0xf36c	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:58:16.681098938 CEST	8.8.8.8	192.168.2.3	0xf36c	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:58:16.797147989 CEST	8.8.8.8	192.168.2.3	0x95ed	No error (0)	7news.cdn.7vodcloud.io		13.32.14.64	A (IP address)	IN (0x0001)
Aug 4, 2021 00:58:16.797147989 CEST	8.8.8.8	192.168.2.3	0x95ed	No error (0)	7news.cdn.7vodcloud.io		13.32.14.104	A (IP address)	IN (0x0001)
Aug 4, 2021 00:58:16.797147989 CEST	8.8.8.8	192.168.2.3	0x95ed	No error (0)	7news.cdn.7vodcloud.io		13.32.14.123	A (IP address)	IN (0x0001)
Aug 4, 2021 00:58:16.797147989 CEST	8.8.8.8	192.168.2.3	0x95ed	No error (0)	7news.cdn.7vodcloud.io		13.32.14.122	A (IP address)	IN (0x0001)
Aug 4, 2021 00:58:19.753793001 CEST	8.8.8.8	192.168.2.3	0x2736	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:58:19.753793001 CEST	8.8.8.8	192.168.2.3	0x2736	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 7news.cdn.7vodcloud.io

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49712	13.32.14.64	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 4, 2021 00:58:16.861457109 CEST	1221	OUT	GET / HTTP/1.1 Host: 7news.cdn.7vodcloud.io Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 4, 2021 00:58:16.890603065 CEST	1221	IN	HTTP/1.1 403 Forbidden Server: CloudFront Date: Tue, 03 Aug 2021 22:58:16 GMT Content-Type: text/xml Content-Length: 146 Connection: keep-alive X-Cache: Error from cloudfront Via: 1.1 218366faeb88f6d265d2589e37ea2dac.cloudfront.net (CloudFront) X-Amz-Cf-Pop: VIE50-C2 X-Amz-Cf-Id: 52dShWLT3lilvlaKSG0_kUedMAG5ixsW3w8KdCcg1nV8p3B7gzCOWA== Data Raw: 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 45 72 72 6f 72 3e 3c 43 6f 64 65 3e 4d 69 73 73 69 6e 67 4b 65 79 3c 2f 43 6f 64 65 3e 3c 4d 65 73 73 61 67 65 3e 4d 69 73 73 69 6e 67 20 4b 65 79 2d 50 61 69 72 2d 49 64 20 71 75 65 72 79 20 70 61 72 61 6d 65 74 65 72 20 6f 72 20 63 6f 6f 6b 69 65 20 76 61 6c 75 65 3c 2f 4d 65 73 73 61 67 65 3e 3c 2f 45 72 72 6f 72 3e Data Ascii: <?xml version="1.0" encoding="UTF-8"?><Error><Code>MissingKey</Code><Message>Missing Key-Pair-Id query parameter or cookie value</Message></Error>

Timestamp	kBytes transferred	Direction	Data
Aug 4, 2021 00:58:17.472728968 CEST	1233	OUT	GET /favicon.ico HTTP/1.1 Host: 7news.cdn.7vodcloud.io Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://7news.cdn.7vodcloud.io/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 4, 2021 00:58:17.502073050 CEST	1240	IN	HTTP/1.1 403 Forbidden Server: CloudFront Date: Tue, 03 Aug 2021 22:58:17 GMT Content-Type: text/xml Content-Length: 146 Connection: keep-alive X-Cache: Error from cloudfront Via: 1.1 218366faeb88f6d265d2589e37ea2dac.cloudfront.net (CloudFront) X-Amz-Cf-Pop: VIE50-C2 X-Amz-Cf-Id: ya277_evGxfRApta2oep44gH0naEoLZO-NXYC91mEAn7Hj4rf_ydZQ== Data Raw: 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 45 72 72 6f 72 3e 3c 43 6f 64 65 3e 4d 69 73 73 69 6e 67 4b 65 79 3c 2f 43 6f 64 65 3e 3c 4d 65 73 73 61 67 65 3e 4d 69 73 73 69 6e 67 20 4b 65 79 2d 50 61 69 72 2d 49 64 20 71 75 65 72 79 20 70 61 72 61 6d 65 74 65 72 20 6f 72 20 63 6f 6f 6b 69 65 20 76 61 6c 75 65 3c 2f 4d 65 73 73 61 67 65 3e 3c 2f 45 72 72 6f 72 3e Data Ascii: <?xml version="1.0" encoding="UTF-8"?><Error><Code>MissingKey</Code><Message>Missing Key-Pair-Id query parameter or cookie value</Message></Error>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5728 Parent PID: 2844

General

Start time:	00:58:13
Start date:	04/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://7news.cdn.7vodcloud.io'
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: 852 Parent PID: 5728

General

Start time:	00:58:15
Start date:	04/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,17392542265336455136,3443799518247237767,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1776 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly