ID: 458980
Cookbook: browseurl.jbs
Time: 00:12:46
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

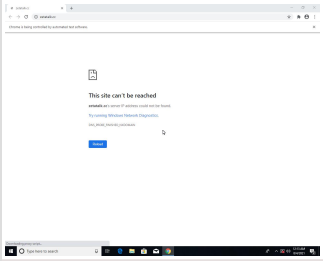
Windows Analysis Report http://zetatalk.cc

Overview

General Information

Sample URL:	http://zetatalk.cc
Analysis ID:	458980
Infos:	

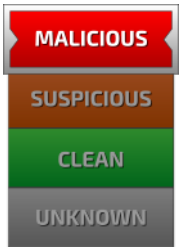
Most interesting Screenshot:



Errors

URL not reachable

Detection

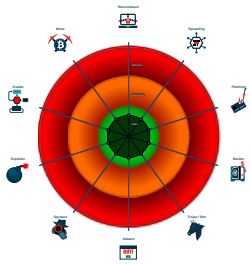


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4960 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://zetatalk.cc' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6028 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1580,1855939609835443883,8153836079990278876,131072 --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

AV Detection:

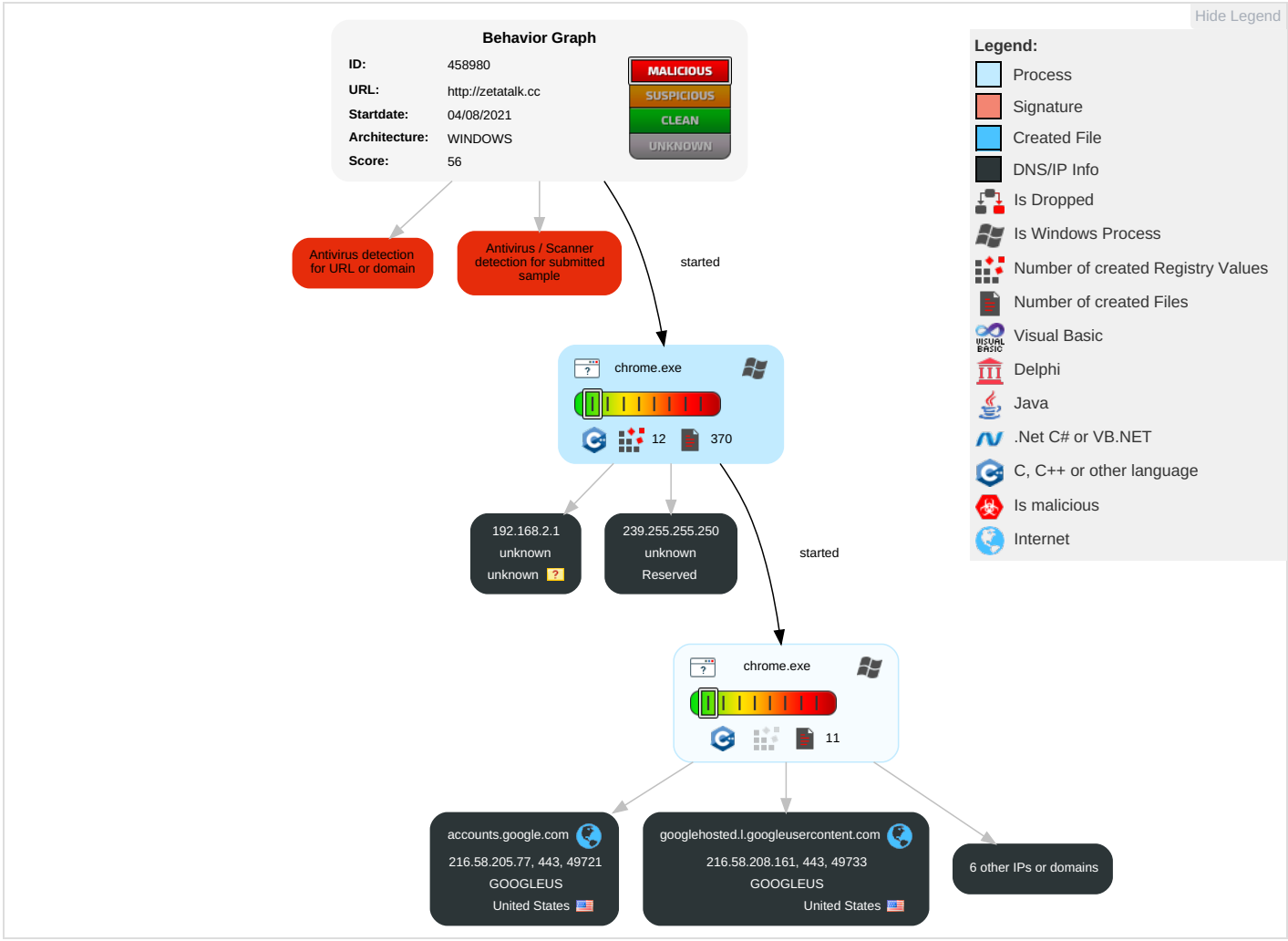
Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Mitre Att&ck Matrix

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

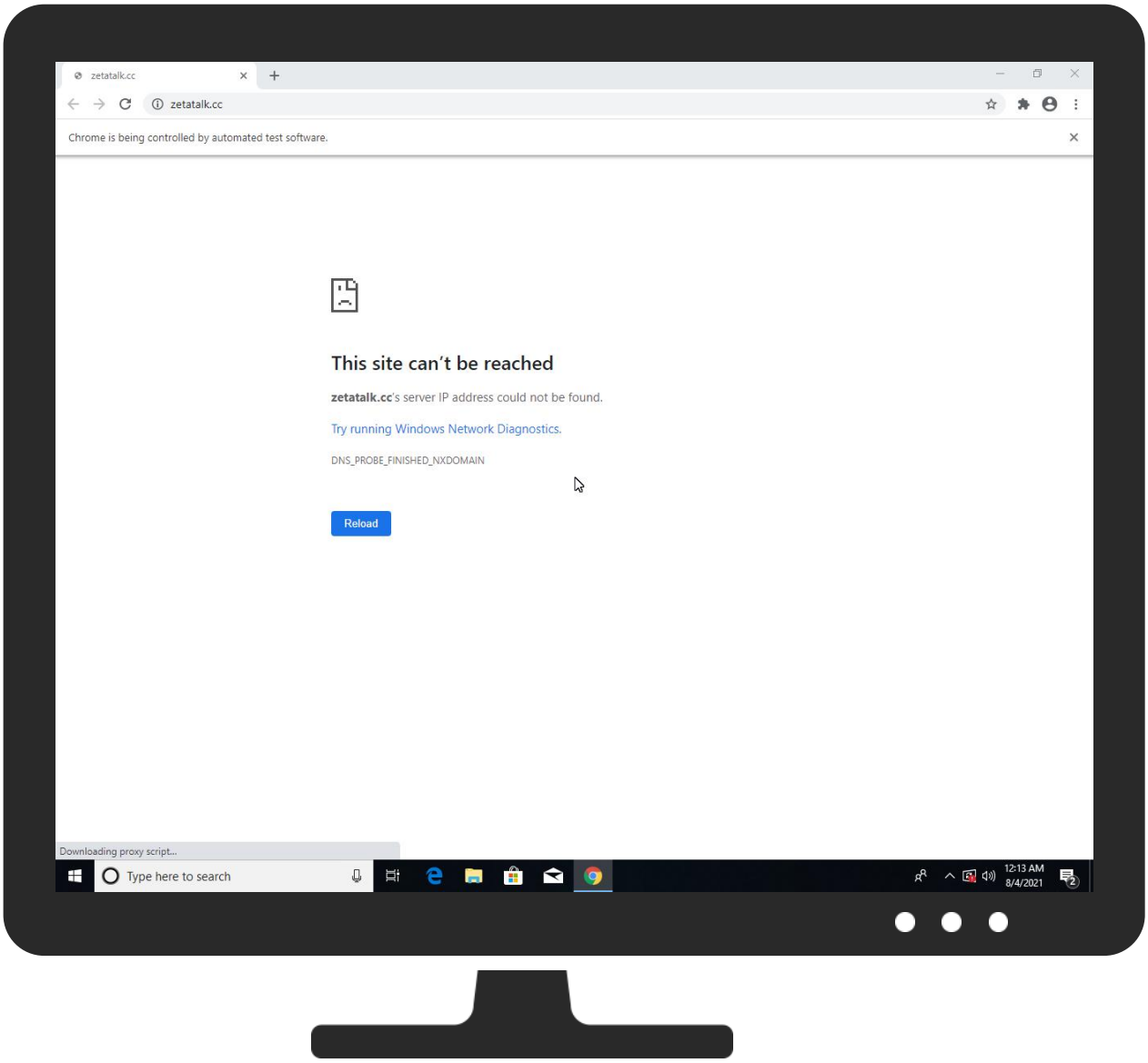
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://zetatalk.cc	3%	Virustotal		Browse
http://zetatalk.cc	100%	Avira URL Cloud	malware	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
zetatalk.cc	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://zetatalk.cc/	3%	Virustotal		Browse
http://zetatalk.cc/	100%	Avira URL Cloud	malware	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://zetatalk.cc/t	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
google.com	142.250.184.78	true	false		high
accounts.google.com	216.58.205.77	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.161	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
zetatalk.cc	unknown	unknown	false	• 3%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458980
Start date:	04.08.2021
Start time:	00:12:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://zetatalk.cc
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:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.win@25/165@6/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All
Errors:	• URL not reachable

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321 01
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 GM DS.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\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:+ftIE1G1mkftIE1G1mkftIE1n
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\0cc5d152-8bc3-4a42-afef-b70105fd4d03.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	5461
Entropy (8bit):	5.1702674344663695
Encrypted:	false
SSDEEP:	96:nmCmvy97cr8R+cKIfok0JCKL8VbOTQVuwn:nmCh9wq+c44K6
MD5:	36C309682B99625A1F06D9874B8AD2FB
SHA1:	EA19E6C31686131F52E197A41FB951B14A5225AA
SHA-256:	FE35D2627B0E80C6A30D6C1AD72B211F3DAEE68021139BBCF2A239644B70DF83
SHA-512:	72C0F1E3489E9325866BC65E4C2E1BEB1556AE6137ADCBF220790CF339CF59B56B2D3FBC39E16F50FB0B34C4A3D45172F01EC578BD7486432BD4D09C6622FC2 B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272534813804829","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5303d649-667d-4df1-9104-d5332224dfc6.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5303d649-667d-4df1-9104-d5332224dfc6.tmp	
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6dadcc2f-3d8e-4d14-8173-a8b951b07d52.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):	5.535838711805813
Encrypted:	false
SSDEEP:	384:tKiteLl1AXR1kXqKf/pUZNCgVLH2HfD3rU3HGonTXSJN4LZ:ELl4R1kXqKf/pUZNCgVLH2HfzrUXGonh
MD5:	73DF5FEE20A3734CA8D033D9BD0AAACC
SHA1:	2AFFC44B401EA618FE71AD8040E3C71178DAE553
SHA-256:	288A1F3CDC0A365C66D76D35F6EA16359C944B172711AAD79F310549F1D76A39
SHA-512:	E3253DFEF3BEDEF322F577550C286559A0ABC27C557AB225EB84292A31B45CD4B1D9273212D9E8918A438253520E5AA3E7AE60EAC149B093EEC58AD3E5453EE1
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":"13272534813520936","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\7507696b-17f1-4203-94ab-298355404188.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.224679856852974
Encrypted:	false
SSDEEP:	6:mHIL+q2PWXp+N23iKKdK9RXXTZIFUtpS25ZmwPS3tVkwOWXp+N23iKKdK9RXX5LJ:Mva5Kk7XT2FUtpj/Ps5f5Kk7XVJ
MD5:	84C447F1259CE9D0FA889E73EFFA5D61
SHA1:	C2F7E6456B8A7FA2112F62AF8A1496B4526382FC
SHA-256:	8E8F5C20D5539D667157A4E1A2484DDBD391B0E6AD13DEDDC627B03C4C416E72
SHA-512:	866B1E09A4A33D7272B3750CFEFC35B00E41E3EDAEC1FBE1CE64073838F0CD5C6B843B2BAE3803B6A5BE9D7EDA553B00A36C04710CF11AA5436A5B1B3DF2E93F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2021/08/04-00:13:38.769 18d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-00:13:38.770 18d8 Recovering log #3.2021/08/04-00:13:38.771 18d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.224679856852974
Encrypted:	false
SSDEEP:	6:mHIL+q2PWXp+N23iKKdK9RXXTZIFUtpS25ZmwPS3tVkwOWXp+N23iKKdK9RXX5LJ:Mva5Kk7XT2FUtpj/Ps5f5Kk7XVJ
MD5:	84C447F1259CE9D0FA889E73EFFA5D61
SHA1:	C2F7E6456B8A7FA2112F62AF8A1496B4526382FC
SHA-256:	8E8F5C20D5539D667157A4E1A2484DDBD391B0E6AD13DEDDC627B03C4C416E72
SHA-512:	866B1E09A4A33D7272B3750CFEFC35B00E41E3EDAEC1FBE1CE64073838F0CD5C6B843B2BAE3803B6A5BE9D7EDA553B00A36C04710CF11AA5436A5B1B3DF2E93F
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.769 18d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-00:13:38.770 18d8 Recovering log #3.2021/08/04-00:13:38.771 18d8 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):	5.228898598933179
Encrypted:	false
SSDEEP:	6:mHj+q2PWXp+N23iKKdKyDZIFUtpSmZmwPSiVkwOWXp+N23iKKdKyJLJ:rva5Kk02FUtpr/Ph5f5KkWJ
MD5:	EF524236343788E964CBAD0EC368F506
SHA1:	A559E415F3A4D7EE75D9C6DC22418CEC09957680
SHA-256:	04DCCCD514E9FA7D39A6E2DC87DED02ED8931114BFC0D6E23A889D51F6E9B7AB
SHA-512:	AAB308427446B7415B1BDE9AD68035759AA8CF5E9FD375831A7170B2A058DF103CE18846E6ED4632DA9A95853C03CF2E58AD70B450C2F9838A21C0EA8647628
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.755 18d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-00:13:38.756 18d8 Recovering log #3.2021/08/04-00:13:38.756 18d8 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.oldDB (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.228898598933179
Encrypted:	false
SSDEEP:	6:mHj+q2PWXp+N23iKKdKyDZIFUtpSmZmwPSiVkwOWXp+N23iKKdKyJLJ:rva5Kk02FUtpr/Ph5f5KkWJ
MD5:	EF524236343788E964CBAD0EC368F506
SHA1:	A559E415F3A4D7EE75D9C6DC22418CEC09957680
SHA-256:	04DCCCD514E9FA7D39A6E2DC87DED02ED8931114BFC0D6E23A889D51F6E9B7AB
SHA-512:	AAB308427446B7415B1BDE9AD68035759AA8CF5E9FD375831A7170B2A058DF103CE18846E6ED4632DA9A95853C03CF2E58AD70B450C2F9838A21C0EA8647628
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.755 18d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-00:13:38.756 18d8 Recovering log #3.2021/08/04-00:13:38.756 18d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	901

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Entropy (8bit):	3.024074112658905
Encrypted:	false
SSDEEP:	12:3olydJhmjp7w6PlpxlpN8klyTlzLLEXmoIQAlCm0zLLEXXBlptlpl:34SipkQlrlAEDWAaalLlL
MD5:	66F92300531CE2617CA0375B845A798D
SHA1:	BC196859B415DFFCC8B36724AB9CD8A4955110AB
SHA-256:	8AA2ED805FE2C7C05D128DD6E38373CA0781A030301A804825383A2E46C7FB04
SHA-512:	A424FD2B409536144194183C7F339CFF53AE70DA83C492EBE2CC30CD85B9B0CFB19DE5AC4240CEDF24AC4870D8DF1D4A612E3EF6607CAB0A1E85A3C3E9D79A3
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...1064e860_8d32_4421_a94e_8ccbf4fcc727.....5.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....http://zetatalk.cc/....t...p.....h.....h.....`.....s.....s.....h.t.t.p.:././.z.e.t.a.t.a.l.k...c.c./.....8.....0.....8.....http://zetatalk.cc/.....L'/.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	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):	317
Entropy (8bit):	5.187701436161351
Encrypted:	false
SSDEEP:	6:mn4q2PWXp+N23iKKdK8aPrqIFUtpDZmwPgkwOWXp+N23iKKdK8amLJ:c4va5KkL3FUtpD/Pg5f5KkQJ
MD5:	B2E0A3E0876E72CFF1B2190B06488B48
SHA1:	496A2D415775EE0D601F94E998EF909182964C01
SHA-256:	50472041EEBAC8D463A3D8469B2B74A4D40F7011AB74B314735E800F7AE5B96D
SHA-512:	401AB50E36D36019D50E21CD1EA9208ED24D01714180D01452402482B52E469D9521F92B919C0139C06934B9F1731A678077141ADB43F07FB21E16C840C11A9E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Preview:	2021/08/04-00:13:33.816 190 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-00 :13:33.817 190 Recovering log #3.2021/08/04-00:13:33.818 190 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.187701436161351
Encrypted:	false
SSDEEP:	6:mn4q2PWXp+N23iKKdK8aPrqIFUtpDZmwPgkwOWXp+N23iKKdK8amLJ:c4va5KkL3FUtpD/Pg5f5KkQJ
MD5:	B2E0A3E0876E72CFF1B2190B06488B48
SHA1:	496A2D415775EE0D601F94E998EF909182964C01
SHA-256:	50472041EEBAC8D463A3D8469B2B74A4D40F7011AB74B314735E800F7AE5B96D
SHA-512:	401AB50E36D36019D50E21CD1EA9208ED24D01714180D01452402482B52E469D9521F92B919C0139C06934B9F1731A678077141ADB43F07FB21E16C840C11A9E
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.816 190 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-00 :13:33.817 190 Recovering log #3.2021/08/04-00:13:33.818 190 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.219780673321068
Encrypted:	false
SSDEEP:	6:mmrMq2PWXp+N23iKKdK8NIFUtpb0RZmwPArkwOWXp+N23iKKdK8+eLJ:HMva5KkpFUtpIR/PAr5f5KkqJ
MD5:	F125A6D9125FAB1F3E5A7E79B7706577
SHA1:	B8051263419EA9FE8DCC6BA4FDA8E3F5794051E9
SHA-256:	763FDCEE951613699D740B12C53ADAA90723288993591EF2DA2CC49C3CB81A3B
SHA-512:	7142A1156560DD71925EDE4A96E9EAFF80AB2156243B200495409A379ECB481085A65806491C7D6142857950EC6A469157952AA899DB6677EA5CF6D96A323E39
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:35.998 f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-00 :13:35.999 f24 Recovering log #3.2021/08/04-00:13:36.000 f24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003. log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old. (copy)	
Entropy (8bit):	5.219780673321068
Encrypted:	false
SSDEEP:	6:mmrMq2PWXp+N23iKKdK8NIFUtpb0RZmwPArkwOWXp+N23iKKdK8+eLJ:HMva5KkpFUtpIR/PAr5f5KkqJ
MD5:	F125A6D9125FAB1F3E5A7E79B7706577
SHA1:	B8051263419EA9FE8DCC6BA4FDA8E3F5794051E9
SHA-256:	763FDCEE951613699D740B12C53ADAA90723288993591EF2DA2CC49C3CB81A3B
SHA-512:	7142A1156560DD71925EDE4A96E9EAFF80AB2156243B200495409A379ECB481085A65806491C7D6142857950EC6A469157952AA899DB6677EA5CF6D96A323E39
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:35.998 f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-00:13:35.999 f24 Recovering log #3.2021/08/04-00:13:36.000 f24 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=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.250012230900801
Encrypted:	false
SSDEEP:	6:mH6M+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpSIZmwPSYVkwOWXp+N23iKKdK25+M:hva5KkTXfchI3FUtpp/Pj5f5KkTXfchn
MD5:	ACADAE88E382AD247F28654A3C49257B
SHA1:	34EBFD4960CE6BA7DCF0AA64EF3538BF2D9537D9
SHA-256:	DA68E744EA1CDF28BD1624306BA68FFD0A0ADA511B7FC78B5D48294D4E8995F3
SHA-512:	1FFA2DD2D87DC8A8C847A21C1EE60FEC31CC2D2D3F89B36D0FB9445AAF832A0676A4A2B8075B9D83A4CB8E4C9F337A004F22996DA0F7C830AD2730F61CEC1 AC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.748 18d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/08/04-00:13:38.750 18d8 Recovering log #3.2021/08/04-00:13:38.750 18d8 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):	5.250012230900801
Encrypted:	false
SSDEEP:	6:mH6M+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpSIZmwPSYVkwOWXp+N23iKKdK25+M:hva5KkTXfchI3FUtpp/Pj5f5KkTXfchn
MD5:	ACADAE88E382AD247F28654A3C49257B
SHA1:	34EBFD4960CE6BA7DCF0AA64EF3538BF2D9537D9
SHA-256:	DA68E744EA1CDF28BD1624306BA68FFD0A0ADA511B7FC78B5D48294D4E8995F3
SHA-512:	1FFA2DD2D87DC8A8C847A21C1EE60FEC31CC2D2D3F89B36D0FB9445AAF832A0676A4A2B8075B9D83A4CB8E4C9F337A004F22996DA0F7C830AD2730F61CEC1 AC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.748 18d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/08/04-00:13:38.750 18d8 Recovering log #3.2021/08/04-00:13:38.750 18d8 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):	5.2041933408509795
Encrypted:	false
SSDEEP:	6:mH8M+q2PWXp+N23iKKdK25+XuoIFUtpSsNZmwPSWURVkwOWXp+N23iKKdK25+Xu6:FRva5KkTXYFUtpd/PI/5f5KkTXHJ
MD5:	2F6A80BBCBA9850CD77CB2608F40F8D2
SHA1:	B420D5BA1B9A1A4FAC3FD09EB7FCC9569780238A
SHA-256:	72E35657B0323144C8E83FEB56ADAA7629C3C6761586B8AED159AE176E98050D
SHA-512:	C03B0134A1A5B916A172FBA30ABE03D20895F763485344A8B181DB2BB8C45638F7E0303FF65A00B91AB20FAF97E15C9B243F5209AEA5198AF9C811090E2FA40D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Preview:	2021/08/04-00:13:38.742 18d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-00:13:38.743 18d8 Recovering log #3.2021/08/04-00:13:38.744 18d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.2041933408509795
Encrypted:	false
SSDEEP:	6:mH8M+q2PWXp+N23iKKdK25+XuoIFUtpSsNZmwPSWURVkwOWXp+N23iKKdK25+Xu6:FRva5KkTXYFUtpd/PI/5f5KkTXHJ
MD5:	2F6A80BBCBA9850CD77CB2608F40F8D2
SHA1:	B420D5BA1B9A1A4FAC3FD09EB7FCC9569780238A
SHA-256:	72E35657B0323144C8E83FEB56ADAA7629C3C6761586B8AED159AE176E98050D
SHA-512:	C03B0134A1A5B916A172FBA30ABE03D20895F763485344A8B181DB2BB8C45638F7E0303FF65A00B91AB20FAF97E15C9B243F5209AEA5198AF9C811090E2FA40D
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.742 18d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-00:13:38.743 18d8 Recovering log #3.2021/08/04-00:13:38.744 18d8 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):	5.242067061729857
Encrypted:	false
SSDEEP:	6:mH8M+q2PWXp+N23iKKdKWT5g1IdqIFUtpSuMZmwPSFd3VkwOWXp+N23iKKdKWT5i:zva5Kkg5gSRFUtpDM/PSF5f5Kkg5gS3e
MD5:	3CB5FB4395D105ED07572F9D5F2E92C5
SHA1:	EE71E8836CBA0DCF123243BACFA9183C39BB0585
SHA-256:	4E2C8552FC9CE975721CBB08060043DE5C8F0F4248CEE06FB4D68A81192AA581
SHA-512:	439890A5B4C18F4F555846235EDECB27D10685E33C6B02EFD65EA266EA7D5360924384176CCC459E608118466597E0863F6DBD2169101AA99124D724E67CE3CA
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.687 18d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-00:13:38.689 18d8 Recovering log #3.2021/08/04-00:13:38.690 18d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.242067061729857
Encrypted:	false
SSDEEP:	6:mH8M+q2PWXp+N23iKKdKWT5g1IdqIFUtpSuMZmwPSFd3VkwOWXp+N23iKKdKWT5i:zva5Kkg5gSRFUtpDM/PSF5f5Kkg5gS3e
MD5:	3CB5FB4395D105ED07572F9D5F2E92C5
SHA1:	EE71E8836CBA0DCF123243BACFA9183C39BB0585
SHA-256:	4E2C8552FC9CE975721CBB08060043DE5C8F0F4248CEE06FB4D68A81192AA581
SHA-512:	439890A5B4C18F4F555846235EDECB27D10685E33C6B02EFD65EA266EA7D5360924384176CCC459E608118466597E0863F6DBD2169101AA99124D724E67CE3CA
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.687 18d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/04-00:13:38.689 18d8 Recovering log #3.2021/08/04-00:13:38.690 18d8 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\Last Session= (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	901
Entropy (8bit):	3.024074112658905

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session= (copy)	
Encrypted:	false
SSDEEP:	12:3olydJhmjp7w6PlpxlpN8klyTlzLLEXmoIQAlCm0zLLEXXBlptlpl:34SipkQlrlAEDWAaalLlL
MD5:	66F92300531CE2617CA0375B845A798D
SHA1:	BC196859B415DFFCC8B36724AB9CD8A4955110AB
SHA-256:	8AA2ED805FE2C7C05D128DD6E38373CA0781A030301A804825383A2E46C7FB04
SHA-512:	A424FD2B409536144194183C7F339CFF53AE70DA83C492EBE2CC30CD85B9B0CFB19DE5AC4240CEDF24AC4870D8DF1D4A612E3EF6607CAB0A1E85A3C3E9D79A3
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...1064e860_8d32_4421_a94e_8ccbf4fcc727.....5.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....http://zetatalk.cc/.....t...p.....h.....h.....`.....s.....s.....h.t.t.p.:././.z.e.t.a.t.a.l.k...c.c./.....8.....0.....8..... ....http://zetatalk.cc/.....L'/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabsfi (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\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.19938758594158
Encrypted:	false
SSDEEP:	6:mnAdQL+q2PWXp+N23iKKdK8a2jMGIFUtpszAG1ZmwPsVASQLVkwOWXp+N23iKKdD:c8va5Kk8EFUtpsn1/PsVAF5f5Kk8bJ
MD5:	7976438FBE6A92E0C280CCB442102ABF
SHA1:	71423DC9F0E86E4C5C54EB4A32D82F993B205860
SHA-256:	F0995141288773F0ACA93CC41749FC3A7FA35B80DEE43B79A4EC2824F1D1CB22
SHA-512:	9113E54205FA113E7C6DB025A680641F54B4935552624F7F7E955869DB303F4DFA106EA7F996E10C2FF26A3516C59700158F0624B797F2B41DECA6246DD88041
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.570 6c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:13:33.578 6c8 Recovering log #3.2021/08/04-00:13:33.582 6c8 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.oldR (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.19938758594158
Encrypted:	false
SSDEEP:	6:mnAdQL+q2PWXp+N23iKKdK8a2jMGIFUtpszAG1ZmwPsVASQLVkwOWXp+N23iKKdD:c8va5Kk8EFUtpsn1/PsVAF5f5Kk8bJ
MD5:	7976438FBE6A92E0C280CCB442102ABF
SHA1:	71423DC9F0E86E4C5C54EB4A32D82F993B205860
SHA-256:	F0995141288773F0ACA93CC41749FC3A7FA35B80DEE43B79A4EC2824F1D1CB22
SHA-512:	9113E54205FA113E7C6DB025A680641F54B4935552624F7F7E955869DB303F4DFA106EA7F996E10C2FF26A3516C59700158F0624B797F2B41DECA6246DD88041
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.oldR (copy)	
Preview:	2021/08/04-00:13:33.570 6c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:13:33.578 6c8 Recovering log #3.2021/08/04-00:13:33.582 6c8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.209655451350382
Encrypted:	false
SSDEEP:	6:mdZSQL+q2PWXp+N23iKKdKgXz4rRIFUtpQGKWZmwPPU8SQLVkwOWXp+N23iKKdKt:OSQ+va5KkgXiuFUtpQGKW/PPsQV5f5K2
MD5:	3E1C6BCD354FABE69291619B7D45A895
SHA1:	7E158988CC453AD82EB47AE7A96E5BD97ED80A83
SHA-256:	FB2767C9F041C6698174F33C5DCA2421B1887CD800C8E648EB51E821341DE5AE
SHA-512:	D6D70D2CCE277EF7FCE6EEF0E1005A8DDB7331316AC8E63B77E8929F88B4FBBAA500D797A00F1918B07CEBF3A836340A81AFBDFEF3269B3CA9D52ADF2A250 3A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.838 155c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-00:13:33.839 155c Recovering log #3.2021/08/04-00:13:33.840 155c 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.old1h (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.209655451350382
Encrypted:	false
SSDEEP:	6:mdZSQL+q2PWXp+N23iKKdKgXz4rRIFUtpQGKWZmwPPU8SQLVkwOWXp+N23iKKdKt:OSQ+va5KkgXiuFUtpQGKW/PPsQV5f5K2
MD5:	3E1C6BCD354FABE69291619B7D45A895
SHA1:	7E158988CC453AD82EB47AE7A96E5BD97ED80A83
SHA-256:	FB2767C9F041C6698174F33C5DCA2421B1887CD800C8E648EB51E821341DE5AE
SHA-512:	D6D70D2CCE277EF7FCE6EEF0E1005A8DDB7331316AC8E63B77E8929F88B4FBBAA500D797A00F1918B07CEBF3A836340A81AFBDFEF3269B3CA9D52ADF2A250 3A
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.838 155c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-00:13:33.839 155c Recovering log #3.2021/08/04-00:13:33.840 155c 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\PreferencesTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesTM (copy)	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5461
Entropy (8bit):	5.1702674344663695
Encrypted:	false
SSDEEP:	96:nmCmvy97cr8R+cKIfok0JCKL8VbOTQVuwn:nmCh9wq+c44K6
MD5:	36C309682B99625A1F06D9874B8AD2FB
SHA1:	EA19E6C31686131F52E197A41FB951B14A5225AA
SHA-256:	FE35D2627B0E80C6A30D6C1AD72B211F3DAEE68021139BBCF2A239644B70DF83
SHA-512:	72C0F1E3489E9325866BC65E4C2E1BEB1556AE6137ADCBF220790CF339CF59B56B2D3FBC39E16F50FB0B34C4A3D45172F01EC578BD7486432BD4D09C6622FC2 B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272534813804829","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22594
Entropy (8bit):	5.535838711805813
Encrypted:	false
SSDEEP:	384:tKiteLl1AXR1kXqKf/pUZNCgVLH2HfD3rU3HGonTXSJN4LZ:ELl4R1kXqKf/pUZNCgVLH2HfzrUXGonh
MD5:	73DF5FEE20A3734CA8D033D9BD0AAACC
SHA1:	2AFFC44B401EA618FE71AD8040E3C71178DAE553
SHA-256:	288A1F3CDC0A365C66D76D35F6EA16359C944B172711AAD79F310549F1D76A39
SHA-512:	E3253DFEF3BEDEF322F577550C286559A0ABC27C557AB225EB84292A31B45CD4B1D9273212D9E8918A438253520E5AA3E7AE60EAC149B093EEC58AD3E5453EE 1
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":"13272534813520936","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	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\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.171325538449574
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
SSDEEP:	6:mlISQL+q2PWXp+N23iKKdKrQMxIFUtpu7TSGKWZmwPu7TSQLVkwOWXp+N23iKKd0:/SQ+va5KkCFUtpbGKW/PbQV5f5KktJ
MD5:	9D6D96379BE6F5CD54A21E07799BC83D
SHA1:	FA4BB3D1B7A643383017B5A398A6AE5126E3916C
SHA-256:	6B275C1A148628F756F222A254190FC708D5CE21DFE9A7F1E3F0D050F6F5A8BA
SHA-512:	6720F66F6C5DA284DC27E1D5064EC8D0D2E5DD6156F6E3B2E16EDA02E8F7FD3F793942E240CD83CE30FF536B4FB26BEAD1AA7F7FFF3696DC50AC1D7862360A70
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.738 155c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-00:13:33.740 155c Recovering log #3.2021/08/04-00:13:33.740 155c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.171325538449574
Encrypted:	false
SSDEEP:	6:mlISQL+q2PWXp+N23iKKdKrQMxIFUtpu7TSGKWZmwPu7TSQLVkwOWXp+N23iKKd0:/SQ+va5KkCFUtpbGKW/PbQV5f5KktJ
MD5:	9D6D96379BE6F5CD54A21E07799BC83D
SHA1:	FA4BB3D1B7A643383017B5A398A6AE5126E3916C
SHA-256:	6B275C1A148628F756F222A254190FC708D5CE21DFE9A7F1E3F0D050F6F5A8BA
SHA-512:	6720F66F6C5DA284DC27E1D5064EC8D0D2E5DD6156F6E3B2E16EDA02E8F7FD3F793942E240CD83CE30FF536B4FB26BEAD1AA7F7FFF3696DC50AC1D7862360A70
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.738 155c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-00:13:33.740 155c Recovering log #3.2021/08/04-00:13:33.740 155c 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):	5.204069399820948
Encrypted:	false
SSDEEP:	6:mniAQ+q2PWXp+N23iKKdK7Uh2ghZIFUtpslAgZmwPsLqNAQVkwOWXp+N23iKKdKs:c8+va5KklhHh2FUtpsf/PsSV5f5Kklh9
MD5:	FF3390A28103864FE615EB5BBEC0BBD9
SHA1:	98319687DB0C37E152A64F433E959CAFCE948A46
SHA-256:	013630A1AE78684C56F1123A1A5CBBC39E4CB9BD2BAE0C14391CD87942E4DC26
SHA-512:	0B324BCBAFAE331AC92D0EE1E3EA01E3456B2995B3CDDB635EFB02BE687C47419EF6AF99B2227DF022D1AAA66A34CB75BFA414AA872638054BA8A869939CCBDC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.539 17bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/04-00:13:33.556 17bc Recovering log #3.2021/08/04-00:13:33.559 17bc 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.oldP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.204069399820948
Encrypted:	false
SSDEEP:	6:mniAQ+q2PWXp+N23iKKdK7Uh2ghZIFUtpslAgZmwPsLqNAQVkwOWXp+N23iKKdKs:c8+va5KklhHh2FUtpsf/PsSV5f5Kklh9
MD5:	FF3390A28103864FE615EB5BBEC0BBD9
SHA1:	98319687DB0C37E152A64F433E959CAFCE948A46
SHA-256:	013630A1AE78684C56F1123A1A5CBBC39E4CB9BD2BAE0C14391CD87942E4DC26
SHA-512:	0B324BCBAFAE331AC92D0EE1E3EA01E3456B2995B3CDDB635EFB02BE687C47419EF6AF99B2227DF022D1AAA66A34CB75BFA414AA872638054BA8A869939CCBDC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.oldP (copy)	
Preview:	2021/08/04-00:13:33.539 17bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/04-00:13:33.556 17bc Recovering log #3.2021/08/04-00:13:33.559 17bc 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\035ca2b3-5b2c-4e5f-8050-f7a2837ff10b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.264834477016172
Encrypted:	false
SSDEEP:	6:mlhSQL+q2PWXp+N23iKKdKusNpV/2jMGIFUtpu1GKWZmwPubeQLVkwOWXp+N23i3:ySQ+va5KkFFUtpUGKW/PTQV5f5KkOJ
MD5:	5CF69F36B6A64EE446FBB794778DD605
SHA1:	9D5D5530450D832534A82EFA5B1BD0CC6F8777F7
SHA-256:	6E5B35BB0163AD0B19D51452DF6B32813BB30D2522D4E44132C40DD63F63E327
SHA-512:	4E8A46AB7FB5CCC47F71AE3835BA89EBD5105836EEB66E02E9F9A5A182B1073BD34DC2BD8EED61EF52CF05D7865F88270FF950AC7754732E13E602B562E9476 5
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.782 155c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:13:33.783 155c Recovering log #3.2021/08/04-00:13:33.784 155c 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):	5.264834477016172
Encrypted:	false
SSDEEP:	6:mlhSQL+q2PWXp+N23iKKdKusNpV/2jMGIFUtpu1GKWZmwPubeQLVkwOWXp+N23i3:ySQ+va5KkFFUtpUGKW/PTQV5f5KkOJ
MD5:	5CF69F36B6A64EE446FBB794778DD605
SHA1:	9D5D5530450D832534A82EFA5B1BD0CC6F8777F7
SHA-256:	6E5B35BB0163AD0B19D51452DF6B32813BB30D2522D4E44132C40DD63F63E327
SHA-512:	4E8A46AB7FB5CCC47F71AE3835BA89EBD5105836EEB66E02E9F9A5A182B1073BD34DC2BD8EED61EF52CF05D7865F88270FF950AC7754732E13E602B562E9476 5
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.782 155c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:13:33.783 155c Recovering log #3.2021/08/04-00:13:33.784 155c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
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):	5.256194760916679
Encrypted:	false
SSDEEP:	6:mdDcq2PWXp+N23iKKdKusNpqz4rRIFUtpNZmwPUkwOWXp+N23iKKdKusNpqz4q8d:Nva5KkmiuFUtpN/PU5f5Kkm2J
MD5:	83CC2856170BD32D85989B7BDF8DAE4F
SHA1:	C590C211FC5EA008691E803797F5C8997BD4FB67
SHA-256:	39A1B625405C67F991F42141FB93781B30BEB228EFA6A9C7FADC9D1542251DF1
SHA-512:	FB3116499F2B22271887F264A97861CDF8127B9B0B2C4BAB0BE85658A3F9447ECDC53865365C110D648F06FD39001DDD689DC79B86D500C3A950E6A143A4CE6
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.838 f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/08/04-00:13:33.839 f24 Recovering log #3.2021/08/04-00:13:33.841 f24 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):	5.256194760916679
Encrypted:	false
SSDEEP:	6:mdDcq2PWXp+N23iKKdKusNpqz4rRIFUtpNZmwPUkwOWXp+N23iKKdKusNpqz4q8d:Nva5KkmiuFUtpN/PU5f5Kkm2J
MD5:	83CC2856170BD32D85989B7BDF8DAE4F
SHA1:	C590C211FC5EA008691E803797F5C8997BD4FB67
SHA-256:	39A1B625405C67F991F42141FB93781B30BEB228EFA6A9C7FADC9D1542251DF1
SHA-512:	FB3116499F2B22271887F264A97861CDF8127B9B0B2C4BAB0BE85658A3F9447ECDC53865365C110D648F06FD39001DDD689DC79B86D500C3A950E6A143A4CE6
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.838 f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/08/04-00:13:33.839 f24 Recovering log #3.2021/08/04-00:13:33.841 f24 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\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.192599134297465
Encrypted:	false
SSDEEP:	12:OQ+va5KkkGHArBFUtppQpGKW/PpQpQV5f5KkkGHAryJ:O5a5KkkGgPgbeGKqeSf5KkkGga
MD5:	EFDCAF81CA3FF77FC4DD0525BCDFA9F8
SHA1:	A8E0306AE4A86DC7F1B997FD78330698A36A5177
SHA-256:	91357BD64C1CDE0F2338E1703BB77DAC3E7AEBB1672D0DAA9D827DA4542C21E1
SHA-512:	239B77D40EF82A7601FAC2C8E5474655FE2948F130CFD1840FEDD780EE66F2DD24BB2C32A2243463E3B69DE48FBB8220EE68B535419EB673AD06FBF4475765D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:39.350 155c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:13:39.352 155c Recovering log #3.2021/08/04-00:13:39.352 155c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.192599134297465
Encrypted:	false
SSDEEP:	12:OQ+va5KkkGHArBFUtppQpGKW/PpQpQV5f5KkkGHAryJ:O5a5KkkGgPgbeGKqeSf5KkkGga
MD5:	EFDCAF81CA3FF77FC4DD0525BCDFA9F8
SHA1:	A8E0306AE4A86DC7F1B997FD78330698A36A5177
SHA-256:	91357BD64C1CDE0F2338E1703BB77DAC3E7AEBB1672D0DAA9D827DA4542C21E1
SHA-512:	239B77D40EF82A7601FAC2C8E5474655FE2948F130CFD1840FEDD780EE66F2DD24BB2C32A2243463E3B69DE48FBB8220EE68B535419EB673AD06FBF4475765D
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:39.350 155c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-00:13:39.352 155c Recovering log #3.2021/08/04-00:13:39.352 155c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.260627899451485
Encrypted:	false
SSDEEP:	12:E+va5KkkGHArqiuFUtpsX/PFfV5f5KkkGHArq2J:la5KkkGgCg0f5KkkGg7
MD5:	79CF1B49656F1E14BAB4ACA52A87DCF4
SHA1:	ECB88EA5AB45B6C143791A10FE2652E20ACA7008
SHA-256:	816689E23A1047A25D4D14F43DE59B32596605820CB015AF87ABFF0A671F7785
SHA-512:	53C3786864A584944917FDF8CE3A1AEDE17079FABF6DCA2F114536E0B8DD89A148DF410AAED27B34720A06A4BE37CD3F72E549C8FD22462C03BD9CA418E71F5
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:39.361 17bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/04-00:13:39.365 17bc Recovering log #3.2021/08/04-00:13:39.366 17bc 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):	5.260627899451485
Encrypted:	false
SSDEEP:	12:E+va5KkkGHArqiuFUtpsX/PFfV5f5KkkGHArq2J:la5KkkGgCg0f5KkkGg7
MD5:	79CF1B49656F1E14BAB4ACA52A87DCF4
SHA1:	ECB88EA5AB45B6C143791A10FE2652E20ACA7008
SHA-256:	816689E23A1047A25D4D14F43DE59B32596605820CB015AF87ABFF0A671F7785
SHA-512:	53C3786864A584944917FDF8CE3A1AEDE17079FABF6DCA2F114536E0B8DD89A148DF410AAED27B34720A06A4BE37CD3F72E549C8FD22462C03BD9CA418E71F5
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:39.361 17bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/04-00:13:39.365 17bc Recovering log #3.2021/08/04-00:13:39.366 17bc 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\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.233654744149527
Encrypted:	false
SSDEEP:	6:mnmdDM+q2PWXp+N23iKKdKpIFUtpsUdgZmwPsKDMVkwOWXp+N23iKKdKa/WLJ:cqDM+va5KkmFUtpsUdg/PsKDMV5f5Kk7
MD5:	5BFE699058998A49C7516CB2FE1E2A0D
SHA1:	E1027FAC9CD812858C871C12D2BF409C8A0443BD
SHA-256:	4E83110EA961880FEAE6E06E9D05BF55769EC6F09C4EC719B3349EEC509C72B7
SHA-512:	708AA782C97872922DDB1CB87800DEE0A8CC33F2E24D1071802AB6296248A6E449C093746E06DAAD978640742F2317606F930A3D7FA5D40F56ABF76D364F4E34
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.532 156c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-00:13:33.538 156c Recovering log #3.2021/08/04-00:13:33.543 156c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.233654744149527
Encrypted:	false
SSDEEP:	6:mnmdDM+q2PWXp+N23iKKdKpIFUtpsUdgZmwPsKDMVkwOWXp+N23iKKdKa/WLJ:cqDM+va5KkmFUtpsUdg/PsKDMV5f5Kk7
MD5:	5BFE699058998A49C7516CB2FE1E2A0D
SHA1:	E1027FAC9CD812858C871C12D2BF409C8A0443BD
SHA-256:	4E83110EA961880FEAE6E06E9D05BF55769EC6F09C4EC719B3349EEC509C72B7
SHA-512:	708AA782C97872922DDB1CB87800DEE0A8CC33F2E24D1071802AB6296248A6E449C093746E06DAAD978640742F2317606F930A3D7FA5D40F56ABF76D364F4E34
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:33.532 156c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-00:13:33.538 156c Recovering log #3.2021/08/04-00:13:33.543 156c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.312109990206194
Encrypted:	false
SSDEEP:	12:VO+va5KkkOrsFUtplY/PloV5f5KkkOrzJ:Ja5Kk+g3f5Kkn
MD5:	109FE03232AA59F01B7848EB2BE6520F
SHA1:	9005200951ED0EC6C665B87333BD74817C6D0AD9
SHA-256:	C5E2F56AD26319C43FEABE77941C2BADFF3B70E09BFFB1CD25E6D8772917ABF9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
SHA-512:	EDF98377389DB48A8E4FB9EF79981B3313BB632984DD636957639ECD4C8ABA57299124D7EC3769E3F58C350F852CBCD450FFCEB0D0CA5C7DF8AA342AA800C4 8
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:40.484 17bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmb meomcjbeemfm/MANIFEST-000001.2021/08/04-00:13:40.486 17bc Recovering log #3.2021/08/04-00:13:40.486 17bc Reusing old log C:\Users\user\AppData\Local\G oogle\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):	402
Entropy (8bit):	5.312109990206194
Encrypted:	false
SSDEEP:	12:VO+va5KkkOrsFUtplY/PloV5f5KkkOrzJ:Ja5Kk+g3f5Kkn
MD5:	109FE03232AA59F01B7848EB2BE6520F
SHA1:	9005200951ED0EC6C665B87333BD74817C6D0AD9
SHA-256:	C5E2F56AD26319C43FEABE77941C2BADFF3B70E09BFFB1CD25E6D8772917ABF9
SHA-512:	EDF98377389DB48A8E4FB9EF79981B3313BB632984DD636957639ECD4C8ABA57299124D7EC3769E3F58C350F852CBCD450FFCEB0D0CA5C7DF8AA342AA800C4 8
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:40.484 17bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmb meomcjbeemfm/MANIFEST-000001.2021/08/04-00:13:40.486 17bc Recovering log #3.2021/08/04-00:13:40.486 17bc Reusing old log C:\Users\user\AppData\Local\G oogle\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.5088454775035025
Encrypted:	false
SSDEEP:	3:tUK6p3Bd11Zmwv3Ip0JSV8sIpWRWSWGv:mH3B5ZmwPSISVvS/Stv
MD5:	4FBF64C4C3E9BCFBBD5C864B4D94246B
SHA1:	D3498599AD8A8141AFAD847162770F35FE02595A
SHA-256:	2A9780DC7C784718EDEDD0F3691148A4FCB0931CC434D18310F3F69AC5764806
SHA-512:	29B24F8A3D367929B5BCE8E7B29EB68B959E813BB440BF202A6670FC367297D1D14AC985426943F1BE190D1162C2B064DA26A84F6664A99FF7F57C0816D102AC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.517 18d8 Recovering log #3.2021/08/04-00:13:38.597 18d8 Delete type=0 #3.2021/08/04-00:13:38.598 18d8 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.5088454775035025
Encrypted:	false
SSDEEP:	3:tUK6p3Bd11Zmwv3Ip0JSV8sIpWRWSWGv:mH3B5ZmwPSISVvS/Stv
MD5:	4FBF64C4C3E9BCFBBD5C864B4D94246B
SHA1:	D3498599AD8A8141AFAD847162770F35FE02595A
SHA-256:	2A9780DC7C784718EDEDD0F3691148A4FCB0931CC434D18310F3F69AC5764806
SHA-512:	29B24F8A3D367929B5BCE8E7B29EB68B959E813BB440BF202A6670FC367297D1D14AC985426943F1BE190D1162C2B064DA26A84F6664A99FF7F57C0816D102AC
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.517 18d8 Recovering log #3.2021/08/04-00:13:38.597 18d8 Delete type=0 #3.2021/08/04-00:13:38.598 18d8 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):	5.239481690463218
Encrypted:	false
SSDEEP:	6:mHOzIq2PWXp+N23iKKdKfrzAdIFUtpSGZmwPS6kwOWXp+N23iKKdKfrzILJ:1zIva5Kk9FUtp9/PP5f5Kk2J
MD5:	3A216BCFCEE37002866D19DC9138DFB4
SHA1:	77715E75B443BDFB8FE68D5E2AAF0EFC5545640E
SHA-256:	7F19B6588E2425343D25D4F876FE2E368741C0DA99F364EF43BB313255C6566B
SHA-512:	CAFA9B10536E2F0977B38A69111D70F5FD2F6D22F104675255C44D7B917797953BA8C966FC89FF94A20763F2A99F71EE07052D05868D798D59A1B818C96889B9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Preview:	2021/08/04-00:13:38.795 f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/04-00:13:38.797 f24 Recovering log #3.2021/08/04-00:13:38.797 f24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.oldl (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.239481690463218
Encrypted:	false
SSDEEP:	6:mHOzlq2PWXp+N23iKKdKfrzAdIFUtpSGZmwPS6kwOWXp+N23iKKdKfrzILJ:1zlva5Kk9FUtp9/PP5f5Kk2J
MD5:	3A216BCFCEE37002866D19DC9138DFB4
SHA1:	77715E75B443BDFB8FE68D5E2AAF0EFC5545640E
SHA-256:	7F19B6588E2425343D25D4F876FE2E368741C0DA99F364EF43BB313255C6566B
SHA-512:	CAFA9B10536E2F0977B38A69111D70F5FD2F6D22F104675255C44D7B917797953BA8C966FC89FF94A20763F2A99F71EE07052D05868D798D59A1B818C96889B9
Malicious:	false
Reputation:	low
Preview:	2021/08/04-00:13:38.795 f24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/04-00:13:38.797 f24 Recovering log #3.2021/08/04-00:13:38.797 f24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Temp\0586c934-e1f5-4c67-ad8b-bf3183a22c03.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

C:\Users\user\AppData\Local\Temp\0586c934-e1f5-4c67-ad8b-bf3183a22c03.tmp	
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...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\072fe52c-7ce3-4c6e-8bc8-3298cbb5ac20.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."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.j5Sl..8.....H"i.-I..`.Q.{...F0D. .0...!'..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\541e9faf-1eb9-46d9-9d59-ea5981b447ae.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\5815492c-fdf7-4777-8892-c38047f9d2fb.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

C:\Users\user\AppData\Local\Temp\5815492c-fdf7-4777-8892-c38047f9d2fb.tmp	
Preview:	.

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):	4.646142101207134
Encrypted:	false
SSDEEP:	96:4O2vvHJn1oTe3PwmCSDMU/Hv2s7E+zP3uuNqN3MErxHMsA2:wvRaeC8b/Hua2cw7
MD5:	F05D0F711A800F5EEF655DB221AB847A
SHA1:	19157C792DF50E74214A0EF639AB1F7C40D2FAB5
SHA-256:	BB4F05C0E76E12710B58B1B33FA0C599157021A375446C52F13FB5C193F81910
SHA-512:	96556AF592CB1614A089D9CF0DD375F0A72FC2B7AA877186B4A3F0212834FD9B2E937599804DA14A2A07BA83C7D9ED739600F7C8319461A7FEAF2B661F6C8D86
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 77a45a66bc36dc298699e1979c6fccc7692be208950b5cb0c64f244001210f1b 7efecb2b779552cef8fbc1d20564323a1 2fca2e33203bc6eccf882300d2c5af4.SERVER_HANDSHAKE_TRAFFIC_SECRET 77a45a66bc36dc298699e1979c6fccc7692be208950b5cb0c64f244001210f1b 0 0ba169cd95ef72602ce6234b3b6879a8060ca16fbe3fbc7318171a66a87903e.CLIENT_HANDSHAKE_TRAFFIC_SECRET 5fb933463833b2fd45c7c2a709ee506ca5 2d64fdd18fc4f4a505a11ade5f902a d076083459d6f3e78d0f46231b0d50e6e19df72c82ed4e290d98cead9e2cc7fa.SERVER_HANDSHAKE_TRAFFIC_SECRET 5f b933463833b2fd45c7c2a709ee506ca52d64fdd18fc4f4a505a11ade5f902a 11804887f12fb32ca88e88ca5cc7ce8cb842b92982d6d98cdb133e7af0e0a7a3.CLIENT_HANDSHAKE_TRAFFIC_SECRET a1e8e32e27408ab25de573738fb3ebbe94791cb01c38a6df63827691b49c66da f5b6f471298486005026be22b0f70f23d5cb96dfe34d0 e8f4c15d12bc943588b.SERVER_HANDSHAKE_TRAFFIC_SECRET a1e8e32e27408ab25de573738fb3ebbe94791cb01c38a6df63827691b49c66da 674c89a9925c5 95a821b19e28ef93fe2e361b4908235acdbc48981f20020874d.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\0586c934-e1f5-4c67-ad8b-bf3183a22c03.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\scoped_dir4960_606368120\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0lprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": ".. .. ..".. },.. "12827687646031907 5": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "...".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "... .. ..-..... ....?".. },.. "12827687646031907 5": {.. "message": "..... .. ..".. },.. "14284488690781267 31": {.. "message": "..... .. ..".. },.. "15221406833188603 51": {.. "message": "..... .. .., ...".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": ".... .. ..".. },.. "18503975003120203 88": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:lPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".... ...".. },.. "12139579827238759 20": {.. "message": "..... ....?".. },.. "12827687646031907 5": {.. "message": "..... ....".. },.. "14284488690781267 31": {.. "message": "..... ....".. },.. "15221406833188603 51": {.. "message": "..... ... .".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": ".....".. },.. "18503975003120203 88": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\ca\messages.json	
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE 1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "1522140683318860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\de\messages.json	
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "H.ngenbleiben".. },.. "12139579827238759 20": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "12827687646031907 5": {.. "message": "Ger.teerkennung".. },.. "14284488690781267 31": {.. "message": "Videowiedergabequalit.t".. },.. "15221406833188603 51": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "15509040647108289 58": {.. "message": "St.rungsfrei".. },.. "16366867476874943 76": {.. "message": "Perfekt".. },.. "18027627465894571 77": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "......".. },.. "12139579827238759 20": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "......... ....".. },.. "14284488690781267 31": {.. "message": "......... .....".. },.. "15221406833188603 51": {.. "message": "........ ....".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874943 76": {.. "message": "......".. },.. "18027627465894571 77": {.. "message": "..... ....".. },.. "18503975003120203 88": {.. "message": "........ .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Freezes".. },.. "12139579827238759 20": {.. "message": "Which of the following best describes your network?".. },.. "12827687646031907 5": {.. "message": "Device Discovery".. },.. "14284488690781267 31": {.. "message": "Video Smoothness".. },.. "15221406833188603 51": {.. "message": "Connection failed. Please try again.".. },.. "15509040647108289 58": {.. "message": "Smooth".. },.. "16366867476874943 76": {.. "message": "Perfect".. },.. "18027627465894571 77": {.. "message": "Volume".. },.. "18503975003120203 88": {.. "message": "Are you able to see your Chromecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\es\messages.json	
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71EEEE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas describe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB11202723566
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "1522140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A526195205021

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\fi\messages.json	
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "152214068331886 0351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "180276274658945717 7": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C00 0
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "128276876460319075": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-s mooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smoot h".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51 B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Se fige".. },.. "1213957982723875920": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "1428448869078126731": {.. "message": "Fluidit. de la vid.o".. },.. "1522140683318860351": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "1550904064710828958": {.. "message": "Fluide".. },.. "163 6686747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\gu\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876 460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "128276 876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15507
Entropy (8bit):	5.290847699527565
Encrypted:	false
SSDEEP:	192:Pdapr6h85tRwVQgkvJryLkla5Kfndg/V6c8TEKdl:Arwot2Q7BryVce/V6uml
MD5:	3ED90E66789927D80B42346BB431431E
SHA1:	2B061E3271DF4255B1FFC47BDB207CDEC0D9724F
SHA-256:	0B41E3C42414F72C9A12C05F8772597F9685115366A774C66018467AD4B71A74
SHA-512:	92BE43F1FFC8EFBF5BBC50573AC4C65F6104416A5B6CD04404C3A9854CA3DCF2A43A4044C168590CDF83887D234495843572331ADCD5B020D2E48A3956F3C16
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Zamrzavanje".. },.. "1213957982723875920": {.. "message": "Koje od sljede.eg najbolje opisuje va.u mre.u?".. },.. "128276876460319075": {.. "message": "Otkrivanje ure.aja".. },.. "1428448869078126731": {.. "message": "Ujedna.enost videoreprodukcije".. },.. "1 522140683318860351": {.. "message": "Povezivanje nije uspjelo. Poku.ajte ponovo.".. },.. "1550904064710828958": {.. "message": "Glatko".. },.. "16366867 47687494376": {.. "message": "Savr.ena".. },.. "1802762746589457177": {.. "message": "Glasno.a".. },.. "1850397500312020388": {.. "message": "Vidite li svoj Chromecast u $START_LINK$aplikaciji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "co ntent": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15682
Entropy (8bit):	5.354505633120392
Encrypted:	false
SSDEEP:	192:CCEAproS9fZv+JwkDMrC2NSxoSgbV6c8TEKdl:5r5VZv+RDMrazoV6uml
MD5:	8E9FF7E49473C5734A2F6F0812E12EB3
SHA1:	A4F10DDD1580582533D5EB59EDF6D8048F887C81
SHA-256:	6CDD2FB39ADECE00E88B989E464B05ED1414092D0492F6D0AE58D549BFD1A46A
SHA-512:	E9A4AF31B1A276F395599BB620A3164CABF3459F3C102DD3F57DFEA734510BD985DE65CB409E1975559ACCC615075439A08E1DEBE22C90A0ABCAA3CAFEE79A C7
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Lefagy".. },.. "1213957982723875920": {.. "message": "Az al.bbiak k.z.l melyik jellemzi legjobban h.l.zat.t?".. },.. "128276876460319075": {.. "message": "Eszk.zfelfedez.s".. },.. "1428448869078126731": {.. "message": "Vide. folyamatoss.ga".. },.. "1522140683318860351" : {.. "message": "Sikertelen kapcsol.d.s. K.rj.k, pr.b.lja .jra.".. },.. "1550904064710828958": {.. "message": "Folyamatos".. },.. "1636686747687494376": {.. "message": "T.k.letes".. },.. "1802762746589457177": {.. "message": "Hanger.".. },.. "1850397500312020388": {.. "message": "L.tja a Chromecastot a $STA RT_LINK$Google Home alkalmaz.sbanEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15070
Entropy (8bit):	5.190057470347349
Encrypted:	false
SSDEEP:	192:GsprMtChjkWfrEWL0KRCnEOWV6c8TEKdl:9rtAEr3LTRuWV6uml
MD5:	7ADF9F2048944821F93879336EB61A78
SHA1:	C3DA74FB544684D5B250767BB0CB66FFB7C58963
SHA-256:	3630947E1075E3663AD3E4824D0BE42CB47C0D615D8053E83B9595047C8BA9BE
SHA-512:	1F28BB80E1839C5581106BEA3AE2501C7618249D7E3115819F5A9A87771D59F5DE346C1B9C87F7FFC390604D5B9888CE738E25F2F04A094002A0FB3B22CBEC95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Membeku".. },.. "1213957982723875920": {.. "message": "Dari berikut ini, manakah yang paling mendeskripsikan jaringan Anda?".. },.. "128276876460319075": {.. "message": "Penemuan Perangkat".. },.. "1428448869078126731": {.. "message": "Kelancaran Video".. },.. "1522140683318860351": {.. "message": "Sambungan gagal. Coba lagi.".. },.. "1550904064710828958": {.. "message": "Lancar".. },.. "1636686747687494376" : {.. "message": "Sempurna".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Bisakah Anda melihat Chromecast di $START_LINK$aplikasi Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": " $1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15256
Entropy (8bit):	5.210663765771143
Encrypted:	false
SSDEEP:	192:lYprk52dAaykVza8rE0QWBKD9+vq0hKEV6c8TEKdl:qrlA8r6DalV6uml
MD5:	BB3041A2B485B900F623E57459AE698A
SHA1:	502F5EA89F9FB0287E864B240EA39889D72053A4
SHA-256:	025737EF8FA06706B3F26D0F52B4844244A6D33DAE1D82FEF2931A14C003D57E
SHA-512:	BA51784073BEF82F3A116B33DA406FDB10EC823B9EE74375C46036DAD8BDCB4141F60845DE141ABE42CEEF9251572F6AB287CA5FC7669C60E4F68071D5AB8C D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Si blocca".. },.. "1213957982723875920": {.. "message": "Quale delle seguenti definizioni descrive meglio la tua rete?".. },.. "128276876460319075": {.. "message": "Rilevamento dispositivi".. },.. "1428448869078126731": {.. "message": "Uniformit. video".. },.. "1522140 683318860351": {.. "message": "Connessione non riuscita. Riprova.".. },.. "1550904064710828958": {.. "message": "Fluido".. },.. "1636686747687494376": {.. "message": "Perfetta".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Riesci a vedere il tuo dispositivo Chromecast nell'$START_LINK$app Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16519
Entropy (8bit):	5.675556017051063
Encrypted:	false
SSDEEP:	192:nkprPhQdxkRWrZe1wYpMR5wnAV6c8TEKdl:YrLRWri65wAV6uml
MD5:	6F2CC1A6B258DF45F519BA24149FABDC
SHA1:	8A58C7880C6D22765DCBB6BCE22A192C1B109AE1
SHA-256:	42ECFEE727CFC4F2845FEFDACE5EDC2E0A40AFAD69973A3B950CE653A7633342
SHA-512:	F7454F0E14301C59CC54361ACC0A1C6D072EF9BDF5DEA60646FB90B1CE47612785938C784A4CF1DE3E62648A14420374933B5F5DA43907BC00D3799FF163A3D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "...".. },.. "1213957982723875920": {.. "message": "..".. },.. "128276876460319075": {.. "message": "......".. },.. "1428448869078126731": {.. "message": ".......".. },.. "1522140683318860351": {.. "message": "..".. },.. "15509040 64710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..".. },.. "18503975 00312020388": {.. "message": "$START_LINK$Google Home ...END_LINK. Chromecast .....$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_ LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\kn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\kn\messages.json	
Size (bytes):	20406
Entropy (8bit):	5.312117131662377
Encrypted:	false
SSDEEP:	384:a6C5rBSzvrZreGnla9ZBHRUDYr9yRwEcAa4rSeD5BSz0hJz8qbbM3gbr//Hkr44c:a6C5rBSzvFreGnla9ZBHRUDYr9yRwEcC
MD5:	2E3239FC277287810BC88D93A6691B09
SHA1:	FC5D585DA00ADC90BF79109C7377BD55E6653569
SHA-256:	5FC705AD19761204D8604EA069936A23731B055D51E7836CAAF16AC7719FBEEA
SHA-512:	DF8BC9E577D3ECB0E6C303E1D2C9E9A4A8317CAE810A9DFC88D91B373A4B665722C5A9AB5A589BB947FDA4C7CD9A6DF39DDD13EA47FE9EFF7E0AC43E49FF3479
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..... .....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... $

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	15480
Entropy (8bit):	5.617756574352461
Encrypted:	false
SSDEEP:	192:kWprGvSQtkxWffrnl5JuFBWVZV6c8TEKdl:TrkuxKfrlT4YVZV6uml
MD5:	E303CD63AD00EB3154431DED78E871C4
SHA1:	3B1E5B8E2CF5EBDF5D33656EF80A46563F751783
SHA-256:	FDE602BFDB1AFD282682DA5338C4F91D8A2F6CB5411DB8F62F4583D629CE67A6
SHA-512:	18BA1D5A25FBC1829AD957A531B0CC490AFCBD20AC22181021363AA3CFB916270B8732E824463C9B0897220E8AE86EB1BE561D6540E6C625F08F228F61DDFFA
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "...".. },.. "1213957982723875920": {.. "message": ".. . .. .?".. },.. "128276876460319075": {.. "message": ".. ..".. },.. "1428448869078126731": {.. "message": "... ..".. },.. "1522140683318860351": {.. "message": ".... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "...".. },.. "1802762746589457177": {.. "message": "..".. },.. "1850397500312020388": {.. "message": "$START_LINK$Google Home .END_LINK. Chromecast. .....? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15802
Entropy (8bit):	5.354550839818046
Encrypted:	false
SSDEEP:	192:lGxSprfkiRR+2zJckS1khrnPI85+80p3DWReV6c8TEKdl:lG4rlq0OkSmhrwbpIeV6uml
MD5:	93BBBE82F024FBCB7FB18E203F253429
SHA1:	83F4D80F64FA2ADCE6C515C5F663BD38A76C51DB
SHA-256:	E7A8570922CCC4F2CA3721C4E61F426158C4E7BC90274FBC8BE4040FF8B6CA9B
SHA-512:	B7E7878106B466CE95069141DF1DE387E847348B62E9C4D548006452F3E164B3AD842E9673A56DC011A5ECC3346B5863E2034EE477A9D1F3E0ABD76B2D0F640A
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Stringa".. },.. "1213957982723875920": {.. "message": "Kuris i. toliau pateikt. teigini. geriausiai apib.dina j.s. tinkl. ?".. },.. "128276876460319075": {.. "message": ".renginio suradimas".. },.. "1428448869078126731": {.. "message": "Vaizdo .ra.o sklandumas".. },.. "1522140683318860351": {.. "message": ".vyko ry.io klaida. Bandykite dar kart..".. },.. "1550904064710828958": {.. "message": "Leid.iama skland.iai".. },.. "1636686747687494376": {.. "message": "Puiki".. },.. "1802762746589457177": {.. "message": "Garsumas".. },.. "1850397500312020388": {.. "message": "Ar .Chromecast. rodomas $START_LINK$programoje .Google Home.END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\lv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15891
Entropy (8bit):	5.36794040601742
Encrypted:	false
SSDEEP:	192:y18prUkm15wkLDG2raqhnZDuvyI762V6c8TEKdl:RrAL7rte62V6uml
MD5:	388590CE5E144AE5467FD6585073BD11

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\lv\messages.json	
SHA1:	61228673A400A98D5834389C06127589F19D3A30
SHA-256:	05CA14196CA5D90B228C0F03684E03EBE403A3E7B513AE0A059244AE12B51164
SHA-512:	BF83AC90BC56CEB1CA12DCB47BCE542FB8CFE0BC14E34DE4FE1A84F7CDB4B54E36C125CEA7EE06EA6244F7795A0957A8A20DB30CA4C60FC6E96EF2A73544 8521
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".lesald.ts. att.ls".. },.. "1213957982723875920": {.. "message": "Kur. no t.l.k min.tajiem apgalvojumiem vislab.k raksturo j.su t.klu?".. },.. "128276876460319075": {.. "message": "ler.ces atra.ana".. },.. "1428448869078126731": {.. "message": "Video vienm.r.ba".. },.. "1522140683318860351": {.. "message": "Neizdev.s izveidot savienojumu. L.dzu, m..iniet v.lreiz.".. },.. "1550904064710828958": {.. "message": "Vienm.r.gs a tt.ls".. },.. "1636686747687494376": {.. "message": "Nevainojama".. },.. "1802762746589457177": {.. "message": "Ska.ums".. },.. "1850397500312020388": {.. "message": "Vai j.su Chromecast ier.ce ir redzama $START_LINK$lietotn. Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2"..

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\ml\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20986
Entropy (8bit):	5.347122984404251
Encrypted:	false
SSDEEP:	384:6pQrdbhWHZ3wOn1HbxytQdroExFVRnTPV6uml:X5hUtz6uml
MD5:	2AF93901DE80CA49DA869188BCDA9495
SHA1:	E60DF4F2FB12BD3F1CA869DAD9F6BDE0C17CEB11
SHA-256:	329E80AEE1212F634E180DEF7E16D6E38D9C9FDA9AC9DB1D99B8AE1626EF304E
SHA-512:	DD1711B017DC65E1272972A1BEBD7A1B1769E1F22B37B20582573392CD432725D19DCE134145B3C031428BC0B5948B02A9AA93C8A651BEAA189B686B7BC2AD4
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....."".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ....."".. },.. "1428448869078126731": {.. "message": "..... ....."".. },.. "1522140683318860351": {.. "message": "..... ...."".. },.. "1550904064710828958": {.. "message": "....."".. },.. "1636686747687494376": {.. "message": "....."".. },.. " 1802762746589457177": {.. "message"

C:\Users\user\AppData\Local\Temp\scoped_dir4960_606368120\CRX_INSTALL_locales\mr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19628
Entropy (8bit):	5.311054092888986
Encrypted:	false
SSDEEP:	192:PbrpprGy+RmIosTmidpzlF1Akk03LQYOkQrjNjP8hZYiEQ5z+excV6c8TEKdl:PbfrGUIos7dpzxbP7KrjNjaBEYuV6uml
MD5:	659F5B4ACA112D3ECBB6EC1613DDE824
SHA1:	5DEE35FCD260554999F8DDEC489FBA9F81FA8EEE
SHA-256:	C8B765E7A07578BC078A952E151E3B866506959E15E79E9E5E1DBB98F9C4008F
SHA-512:	F74B36C1B6160E444F4969D13788A9C60637BDC11DC5065B2518B668E8D638384E00557ACDC88B3EA225D9231B6BED4B227BFB2E12C92773073B256F62ADDE6
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....."".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ..."".. },.. "1428448869078126731": {.. "message": "..... ....."".. },.. "1522140683318860351": {.. "message": "..... ...."".. },.. "1550904064710828958": {.. "message": ".... ...."".. },.. "1636686747687494376": {.. "message": "...."".. },.. "18027627 46589457177": {.. "message": "....."".. },.. "1850397500312020388": {.. "message": "..... $START_LINK$ Goo

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 4, 2021 00:13:38.450855017 CEST	192.168.2.3	8.8.8.8	0x9f7	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:13:38.451539993 CEST	192.168.2.3	8.8.8.8	0x6288	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:13:38.455034018 CEST	192.168.2.3	8.8.8.8	0x3c15	Standard query (0)	zetatalk.cc	A (IP address)	IN (0x0001)
Aug 4, 2021 00:13:38.547020912 CEST	192.168.2.3	8.8.8.8	0x5e5	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:13:38.547499895 CEST	192.168.2.3	8.8.8.8	0xe32a	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 00:13:39.324893951 CEST	192.168.2.3	8.8.8.8	0xa818	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 00:13:38.489768982 CEST	8.8.8.8	192.168.2.3	0x3c15	Name error (3)	zetatalk.cc	none	none	A (IP address)	IN (0x0001)
Aug 4, 2021 00:13:38.491590023 CEST	8.8.8.8	192.168.2.3	0x6288	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:13:38.491590023 CEST	8.8.8.8	192.168.2.3	0x6288	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 4, 2021 00:13:38.494322062 CEST	8.8.8.8	192.168.2.3	0x9f7	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 4, 2021 00:13:38.580538034 CEST	8.8.8.8	192.168.2.3	0x5e5	No error (0)	google.com		142.250.184.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:13:38.581161022 CEST	8.8.8.8	192.168.2.3	0xe32a	No error (0)	google.com		142.250.184.78	A (IP address)	IN (0x0001)
Aug 4, 2021 00:13:39.367294073 CEST	8.8.8.8	192.168.2.3	0xa818	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 00:13:39.367294073 CEST	8.8.8.8	192.168.2.3	0xa818	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.161	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4960 Parent PID: 4824

General

Start time:	00:13:32
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://zetatalk.cc'
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: 6028 Parent PID: 4960

General

Start time:	00:13:34
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=1580,1855939609835443883,8153836079990278876,131072 --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