ID: 458977
Cookbook: browseurl.jbs
Time: 23:49:20
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

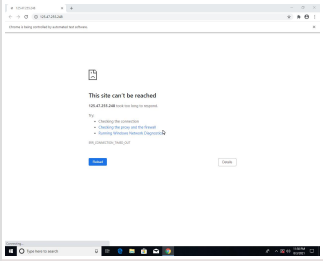
Windows Analysis Report http://125.47.255.248

Overview

General Information

Sample URL:	http://125.47.255.248
Analysis ID:	458977
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

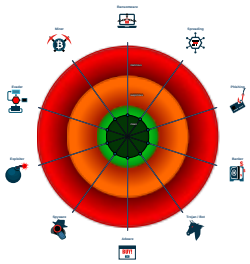
Detection

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

Signatures

No high impact signatures.

Classification



Analysis Advice

Joe Sandbox was unable to browse the URL (domain or webserver down or HTTPS issue), try to browse the URL again later

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Process Tree

- **System is w10x64**
- chrome.exe (PID: 1048 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://125.47.255.248' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2588 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,275807099243823227,4504885289812018906,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1832 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

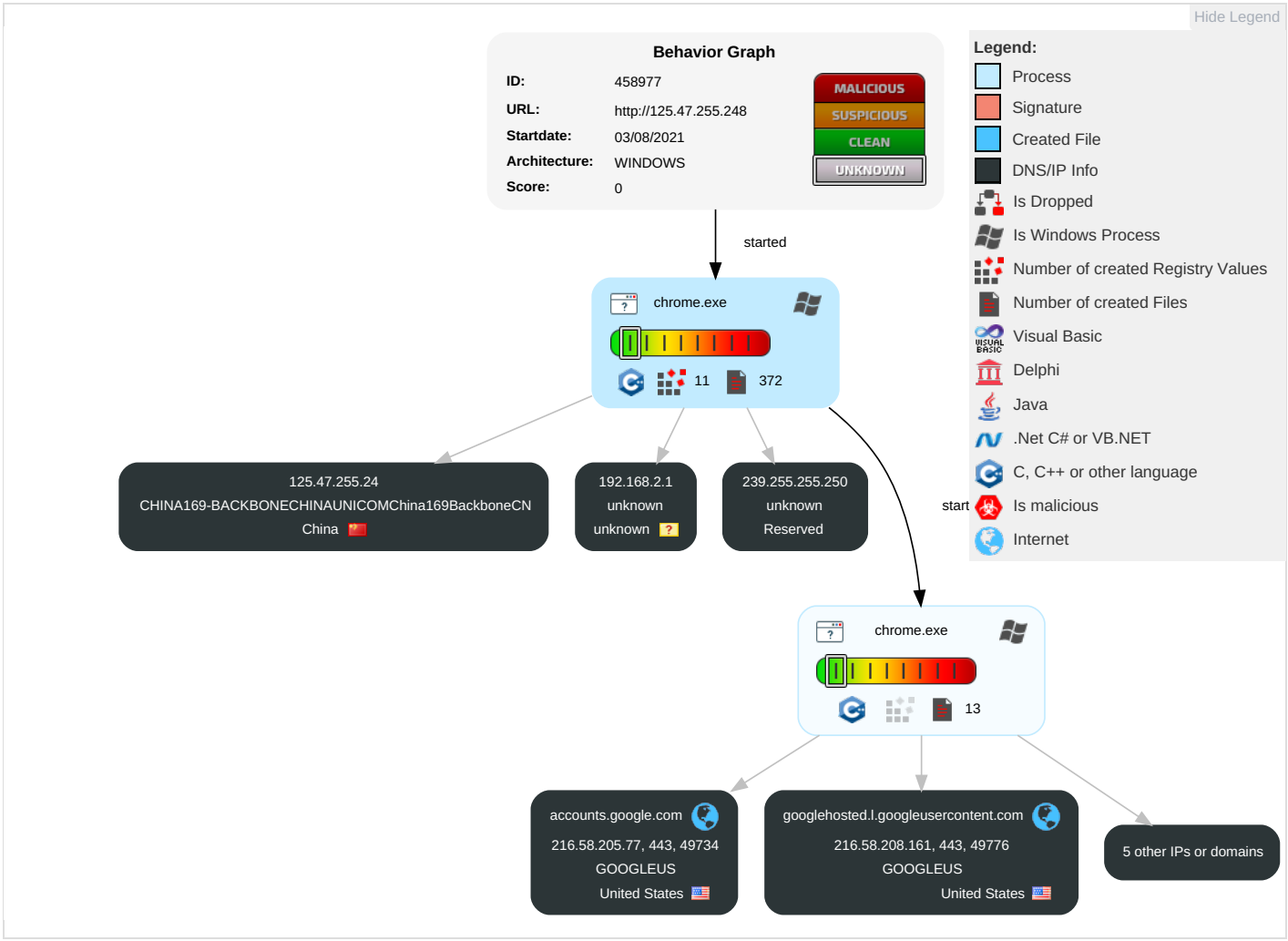
Click to jump to signature section

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

Mitre Att&ck Matrix

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

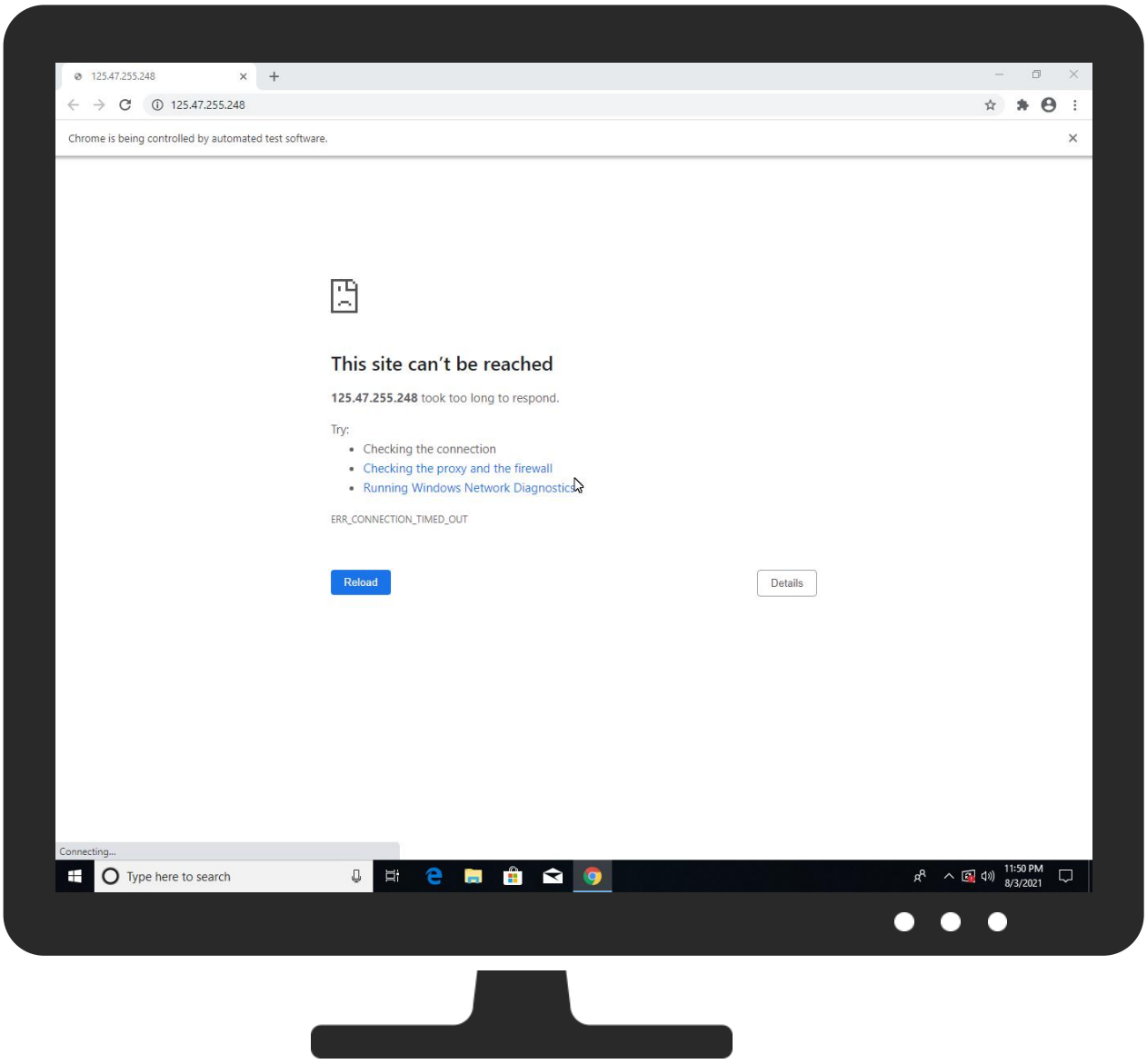
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://125.47.255.248	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://125.47.255.248/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.205.77	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.161	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
125.47.255.248	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
125.47.255.24	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458977
Start date:	03.08.2021
Start time:	23:49:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Sample URL:	http://125.47.255.248
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:	7
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:	UNKNOWN
Classification:	unknown0.win@26/174@3/8
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

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\91c9014b-4d6f-4786-98f4-95e17cb4ef37.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174336
Entropy (8bit):	6.079351421192836
Encrypted:	false
SSDEEP:	3072:LUVGaYTJQE+mugy9+QV1T7IRwdfLSNPHFcbXafIB0u1GOJmA3iuRA:QAxaV+QfT7GSmhlaqfIlUOoSiuRA
MD5:	8CC158CA3A0C7848196DB60A5A9F5719
SHA1:	96834E7B5EC4D769E807A47ED48822969735621F
SHA-256:	550E4E53E4AE2889382D35525B3FD9B0E12896F666AF0CFE45B7F1BCD1844842
SHA-512:	4FD8BD1ED6F5502D27A40D942954AD535FEC43BA202E08986340894B4273B3CC3273D698C187B79AF11632DEA60A2FDEC270E1488337A01D3A35D8DA2735D99
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628059810237143e+12,"network":1.628027412e+12,"ticks":5115804561.0,"uncertainty":4575038.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	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\51266b58-8967-4bf9-a400-3d250baa9f60.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\51266b58-8967-4bf9-a400-3d250baa9f60.tmp	
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6ed57a7b-9d4a-47ce-a761-f21e5423ce87.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):	5.23650541587848
Encrypted:	false
SSDEEP:	6:mcQLq2PWXp+N23iKKdK9RXXTZIFUtp5EZmwP5dkwOWXp+N23iKKdK9RXX5LJ:mLva5Kk7XT2FUtp6/P/5f5Kk7XVJ
MD5:	26447D84E2FFED1C424830C9EE7E5E1F
SHA1:	3696537BBF7C92B3F88EC341676EDB488EC62460
SHA-256:	6A914D66E84451DF7C8F4801CEE206BDAC160E58FAAE2B30DA0D119CF96DCA38
SHA-512:	B6E12A9B3E10F8B2E9716E4601B2CEEC5D5996E4FEE99E73392CD5A88F2359850B1258009FB9FBEE70291F3759414DBDF9A5F35BC933196CF24EE9E1CF2B187
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.615 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-23:50:40.652 14b0 Recovering log #3.2021/08/03-23:50:40.657 14b0 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):	5.23650541587848
Encrypted:	false
SSDEEP:	6:mcQLq2PWXp+N23iKKdK9RXXTZIFUtp5EZmwP5dkwOWXp+N23iKKdK9RXX5LJ:mLva5Kk7XT2FUtp6/P/5f5Kk7XVJ
MD5:	26447D84E2FFED1C424830C9EE7E5E1F
SHA1:	3696537BBF7C92B3F88EC341676EDB488EC62460
SHA-256:	6A914D66E84451DF7C8F4801CEE206BDAC160E58FAAE2B30DA0D119CF96DCA38
SHA-512:	B6E12A9B3E10F8B2E9716E4601B2CEEC5D5996E4FEE99E73392CD5A88F2359850B1258009FB9FBEE70291F3759414DBDF9A5F35BC933196CF24EE9E1CF2B187
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.615 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-23:50:40.652 14b0 Recovering log #3.2021/08/03-23:50:40.657 14b0 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):	5.201579106549625
Encrypted:	false
SSDEEP:	6:mvHAq2PWXp+N23iKKdKyDZIFUtp3jZmwPrbkwOWXp+N23iKKdKyJLJ:OHAva5Kk02FUtpz/Pn5f5KkWJ
MD5:	2C558C89CC195C805D3EC84737685C0F
SHA1:	21E05F32CDC6347117A34B0BE50FA6CB6EEF74B3
SHA-256:	31560A191AE8B882B70C1D510AC665353C5BF496523F78A6DA727D3925003B15
SHA-512:	C66B793A9EB53E366EBC2BA80862B02B12D349182D8CFA50DE0CBA0C95067AC09489AE4CD6D9C2F2AE8159FCCA50737F2A896BB686AF612514A16AA584E082D1
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.571 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-23:50:40.581 14b0 Recovering log #3.2021/08/03-23:50:40.583 14b0 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.oldon (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.201579106549625
Encrypted:	false
SSDEEP:	6:mvHAq2PWXp+N23iKKdKyDZIFUtp3jZmwPrbkwOWXp+N23iKKdKyJLJ:OHAva5Kk02FUtpz/Pn5f5KkWJ
MD5:	2C558C89CC195C805D3EC84737685C0F
SHA1:	21E05F32CDC6347117A34B0BE50FA6CB6EEF74B3
SHA-256:	31560A191AE8B882B70C1D510AC665353C5BF496523F78A6DA727D3925003B15
SHA-512:	C66B793A9EB53E366EBC2BA80862B02B12D349182D8CFA50DE0CBA0C95067AC09489AE4CD6D9C2F2AE8159FCCA50737F2A896BB686AF612514A16AA584E082D1
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.571 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-23:50:40.581 14b0 Recovering log #3.2021/08/03-23:50:40.583 14b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9679161034659685
Encrypted:	false
SSDEEP:	24:gcLgAZOZD/hhqLbJLbXaFpEO5bNmISHn06Uwm8:g8NOZbq5LLOpEO5J/Kn7UR8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
MD5:	A17736EFEC34A4D0165655EE7EAF48EF
SHA1:	71EC888E59BD90EDDD9BFA0531938536827AA5DC
SHA-256:	1403262D78CAD7081F0E907A1A9FCBCAC5F8B56577213F417772508D892B9E12
SHA-512:	3569362DA3699AA527F69771A5222B38179BFB8D68597C68460B61CB286087667BC4BFA29C7101938B325A59069EAC0C9EB0076E867F0F211D62E768931C8F65
Malicious:	false
Reputation:	low
Preview:	.....w.@..... ....

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):	917
Entropy (8bit):	2.996853625799143
Encrypted:	false
SSDEEP:	12:3olydJh82K/7EcPlpxlpN8kIyT0lptlpyziobOV3VV:34SWlrlA5lLlQ2os
MD5:	A72F8E62260269A1EF66695AC4220FFA
SHA1:	3E20191B5B5A9F632D61DB2A99C3B8F578ED3A67
SHA-256:	3A77B9E8A6C9E765AAD1270A7A535EC14EC7452B43983724BDCC716B4B96D262
SHA-512:	CF4FCEC8ECE8993462AA22800FE9A6D6271C5FB816D28AE6DAF253F502FD3DFD357C094948702B3FA222270D71D69C7E86926894D183B23FD641F3EA7664781
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...3832f6db_42eb_4d95_8c71_8a5f2c7261e5.....ay.0..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....http://125.47.255.248/... ...|...x.....p.....h.....`.....7.....7.....4.....h.t.t.p.:./.1.2.5...4.7...2.5.5...2.4.8./..... .....8.....0.....8..... .....http://125.47.255.248/.....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):	145
Entropy (8bit):	4.510979736598761
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+:qT5z/t2qoEwhXeLK
MD5:	451377CA73B52FBC253654785EFDF530
SHA1:	68236D62983F864939757B23275FCBE8AD693BBC
SHA-256:	DA2E175130A7CFDC3BD0742D65F9BF6F3FD326C5258579C669DC5667C957236F
SHA-512:	F6621A16AB75B1F4EDCC2B36E9FFDD879F75B2D43B45DF8A4D1A0F76A7964B00D821E7E159DB5C8F261AF7C7B21280BE7F5D62545EEDC0AAAAEEDC9110357DF8
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.237327032837868
Encrypted:	false
SSDEEP:	6:mQg+q2PWXp+N23iKKdK8aPrqIFUtp1oWZmwP1mNVkwOWXp+N23iKKdK8amLJ:6+va5KkL3FUtp6W/P4NV5f5KkQJ
MD5:	3558E36A7FDD6657D5DE3CFF490723FF
SHA1:	FC90DC1E2D8ECF13A652863A3E84D531791B926B
SHA-256:	1F7C55637771242C6A64F1E80421BBCC062FED73ACA088176F466B55656681F1
SHA-512:	BE8B3228E6C8D38476199D3EBC858C4AB5CEEF14E49F6D001E9D629F32463CF72A7B045546FEF022A4E686BB2B9948A64115DF729049E43EDC79C5D5E4CB656 F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.736 14cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-23:50:07.737 14cc Recovering log #3.2021/08/03-23:50:07.738 14cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.237327032837868
Encrypted:	false
SSDEEP:	6:mQg+q2PWXp+N23iKKdK8aPrqIFUtp1oWZmwP1mNVkwOWXp+N23iKKdK8amLJ:6+va5KkL3FUtp6W/P4NV5f5KkQJ
MD5:	3558E36A7FDD6657D5DE3CFF490723FF
SHA1:	FC90DC1E2D8ECF13A652863A3E84D531791B926B
SHA-256:	1F7C55637771242C6A64F1E80421BBCC062FED73ACA088176F466B55656681F1
SHA-512:	BE8B3228E6C8D38476199D3EBC858C4AB5CEEF14E49F6D001E9D629F32463CF72A7B045546FEF022A4E686BB2B9948A64115DF729049E43EDC79C5D5E4CB656 F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.736 14cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-23:50:07.737 14cc Recovering log #3.2021/08/03-23:50:07.738 14cc 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):	513
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	C92EABB217D45C77F8D52725AD3758F0
SHA1:	43B422AC002BB445E2E9B2C27D74C27CD70C9975
SHA-256:	388C5C95F0F54F32B499C03A37AABFA5E0A31030EC70D0956A239942544B0EEA
SHA-512:	DFD5D1C614F0EBFF97F354DFC23266655C336B9B7112781D7579057814B4503D4B63AB1263258BDA3358E5EE9457429C1A2451B22261A1F1E2D8657F31240D3C
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.. ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.272323375817752
Encrypted:	false
SSDEEP:	6:m8U+q2PWXp+N23iKKdK8NIFUtpyWZmwPhUVkwOWXp+N23iKKdK8+eLJ:TU+va5KkpFUtpyW/PSV5f5KkqJ
MD5:	C15089492423CB957F7D5AF69DEEC2AA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
SHA1:	07287FBAA8132EE846B9F1584420453E5C97B1B1
SHA-256:	B55C8844BC16121700555133FC57367468F886E20A6A2AFE0CA2454AD240436C
SHA-512:	AFB993EC909A58A0169ED5161C8B431A393802D80A14548AFA1B9BC08466D3B1DC15BBEEA41882A67A7918C02D78A547C88882F4315FE35B0AABA23756EA306
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:09.765 14cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-23:50:09.766 14cc Recovering log #3.2021/08/03-23:50:09.767 14cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.272323375817752
Encrypted:	false
SSDEEP:	6:m8U+q2PWXp+N23iKKdK8NIFUtpyWZmwPhUVkwOWXp+N23iKKdK8+eLJ:TU+va5KkpFUtpyW/PSV5f5KkqJ
MD5:	C15089492423CB957F7D5AF69DEEC2AA
SHA1:	07287FBAA8132EE846B9F1584420453E5C97B1B1
SHA-256:	B55C8844BC16121700555133FC57367468F886E20A6A2AFE0CA2454AD240436C
SHA-512:	AFB993EC909A58A0169ED5161C8B431A393802D80A14548AFA1B9BC08466D3B1DC15BBEEA41882A67A7918C02D78A547C88882F4315FE35B0AABA23756EA306
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:09.765 14cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-23:50:09.766 14cc Recovering log #3.2021/08/03-23:50:09.767 14cc 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\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	5.246376331652673
Encrypted:	false
SSDEEP:	6:mbq2PWXp+N23iKKdK25+Xqx8chI+IFUtpDBZmwPD77kwOWXp+N23iKKdK25+Xqx7:Cva5KkTXfchI3FUtpDB/PD775f5KkTXc
MD5:	F61D0F37B347DF6F8803A27C9D3DBB5B
SHA1:	8AF2369A81F4C3D689B2D70398D8A0D60B1C91E6
SHA-256:	F1C254A8C3EB9AA06C0CFF4B6A91F189388E29DBB8AA13DCED1C82AB5A1F72CC
SHA-512:	12A8D7213AE9786C0D4A46AB1D4DE6FE9AF3FE84D5E6969F859727F9C5BC2046F52932CC673817164B86F0A892699F17F23B4FFAC2F0CF9F2FA8ED0375BDC94
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.408 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-23:50:40.415 14b0 Recovering log #3.2021/08/03-23:50:40.419 14b0 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.oldW (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.246376331652673
Encrypted:	false
SSDEEP:	6:mbq2PWXp+N23iKKdK25+Xqx8chI+IFUtpDBZmwPD77kwOWXp+N23iKKdK25+Xqx7:Cva5KkTXfchI3FUtpDB/PD775f5KkTXc
MD5:	F61D0F37B347DF6F8803A27C9D3DBB5B
SHA1:	8AF2369A81F4C3D689B2D70398D8A0D60B1C91E6
SHA-256:	F1C254A8C3EB9AA06C0CFF4B6A91F189388E29DBB8AA13DCED1C82AB5A1F72CC
SHA-512:	12A8D7213AE9786C0D4A46AB1D4DE6FE9AF3FE84D5E6969F859727F9C5BC2046F52932CC673817164B86F0A892699F17F23B4FFAC2F0CF9F2FA8ED0375BDC94
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.408 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-23:50:40.415 14b0 Recovering log #3.2021/08/03-23:50:40.419 14b0 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):	5.208926040496049
Encrypted:	false
SSDEEP:	6:mOq2PWXp+N23iKKdK25+XuoIFUtpCeBZmwPA0kwOWXp+N23iKKdK25+XuxWLJ:fva5KkTXYFUtpC0/PL5f5KkTXHJ
MD5:	C4A6B0B88A23D9F494CDC253013E1C0B
SHA1:	C19CAFB3B5DE561E2495FAC75FDFA16F827EAB6C
SHA-256:	757D49D47C9AF9F3D0D29D896F22C42A386EEB3603FF2EE1B105FE0884E25EE0
SHA-512:	74B1DFCFCB62E0F560682F8A80C6659B16BA796F1EF9DC4337453BC30F1D4407F18B7BD542C9042274D12E6EA911E3D9A3CA0BC04B709396BAA3A6C3200C7DI 8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.317 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-23:50:40.321 14b0 Recovering log #3.2021/08/03-23:50:40.323 14b0 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.oIdes (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.208926040496049
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.oldes (copy)	
SSDEEP:	6:mOq2PWXp+N23iKKdK25+XuoIFUtpCeBZmwPA0kwOWXp+N23iKKdK25+XuxWLJ:fva5KkTXYFUtpC0/PL5f5KkTXHJ
MD5:	C4A6B0B88A23D9F494CDC253013E1C0B
SHA1:	C19CAFB3B5DE561E2495FAC75FDFA16F827EAB6C
SHA-256:	757D49D47C9AF9F3D0D29D896F22C42A386EEB3603FF2EE1B105FE0884E25EE0
SHA-512:	74B1DFCFCB62E0F560682F8A80C6659B16BA796F1EF9DC4337453BC30F1D4407F18B7BD542C9042274D12E6EA911E3D9A3CA0BC04B709396BAA3A6C3200C7DI 8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.317 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-23:50:40.321 14b0 Recovering log #3.2021/08/03-23:50:40.323 14b0 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):	5.232983662842729
Encrypted:	false
SSDEEP:	6:mSq2PWXp+N23iKKdKWT5g1IdqIFUtp7XZmwPwkwOWXp+N23iKKdKWT5g1I3ULJ:rva5Kkg5gSRFUtpr/Pw5f5Kkg5gS3SJ
MD5:	B6E19E9ABD824173622142D97A0E2C84
SHA1:	1EEA02F7419817630B2AEE24E6C6F68F7AA671D7
SHA-256:	B2061226E50C4AEBB039F0E317633FD9F2565B92E57E7C08D612331F2AA3EF7E
SHA-512:	F14F8DFB0A5BA5E2D47651B6E335A3A34350B05D26A7DE7D46973CDBB38C491FAB480869D7C532DFE41F8EEEFD4B97D17D24DA0A04DC9AB8570E024BDA5D7 AA6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.241 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-23:50:40.242 14b0 Recovering log #3.2021/08/03-23:50:40.247 14b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.232983662842729
Encrypted:	false
SSDEEP:	6:mSq2PWXp+N23iKKdKWT5g1IdqIFUtp7XZmwPwkwOWXp+N23iKKdKWT5g1I3ULJ:rva5Kkg5gSRFUtpr/Pw5f5Kkg5gS3SJ
MD5:	B6E19E9ABD824173622142D97A0E2C84
SHA1:	1EEA02F7419817630B2AEE24E6C6F68F7AA671D7
SHA-256:	B2061226E50C4AEBB039F0E317633FD9F2565B92E57E7C08D612331F2AA3EF7E
SHA-512:	F14F8DFB0A5BA5E2D47651B6E335A3A34350B05D26A7DE7D46973CDBB38C491FAB480869D7C532DFE41F8EEEFD4B97D17D24DA0A04DC9AB8570E024BDA5D7 AA6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.241 14b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-23:50:40.242 14b0 Recovering log #3.2021/08/03-23:50:40.247 14b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	917
Entropy (8bit):	2.996853625799143
Encrypted:	false
SSDEEP:	12:3olydJh82K/7EcPlpxlpN8kIyT0lptlpyziobOV3VV:34SWlrlA5lLlQ2os
MD5:	A72F8E62260269A1EF66695AC4220FFA
SHA1:	3E20191B5B5A9F632D61DB2A99C3B8F578ED3A67
SHA-256:	3A77B9E8A6C9E765AAD1270A7A535EC14EC7452B43983724BDCC716B4B96D262
SHA-512:	CF4FCEC8ECE8993462AA22800FE9A6D6271C5FB816D28AE6DAF253F502FD3DFD357C094948702B3FA222270D71D69C7E86926894D183B23FD641F3EA7664781
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session (copy)	
Preview:	SNSS.....!.....1.,.....$...3832f6db_42eb_4d95_8c71_8a5f2c7261e5.....ay.0..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....http://125.47.255.248/... ...|...x.....p.....h.....`.....7.....7.....4.....h.t.t.p.:././.1.2.5...4.7...2.5.5...2.4.8./..... .....8.....0.....8..... .....http://125.47.255.248/.....L'/.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.221938881246944
Encrypted:	false
SSDEEP:	6:mwq2PWXp+N23iKKdK8a2jMGIFUtp8ZmwP/kwOWXp+N23iKKdK8a2jMmLJ:7va5Kk8EFUtp8/P/5f5Kk8bJ
MD5:	906CCF78FF8A4E890A4EE594E61DB7BD
SHA1:	01601F4F3FEADB9BAE2A19F58A7D35C3978B2D8E
SHA-256:	126A9688A5DB9F76B47AE96CA758A8C4EFA91C69595664446F023F41D46FCCE7
SHA-512:	0C3C1E317E59D5F55C28BE2A153618575AAAE423E812E432B6A102EBDC6BC21F68169F397D7DF82179EBFDE6E96806D58D1A874023B0924257458804EF446246
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.463 4f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:50:07.465 4f4 Recovering log #3.2021/08/03-23:50:07.468 4f4 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.olde (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.221938881246944
Encrypted:	false
SSDEEP:	6:mwq2PWXp+N23iKKdK8a2jMGIFUtp8ZmwP/kwOWXp+N23iKKdK8a2jMmLJ:7va5Kk8EFUtp8/P/5f5Kk8bJ
MD5:	906CCF78FF8A4E890A4EE594E61DB7BD
SHA1:	01601F4F3FEADB9BAE2A19F58A7D35C3978B2D8E
SHA-256:	126A9688A5DB9F76B47AE96CA758A8C4EFA91C69595664446F023F41D46FCCE7
SHA-512:	0C3C1E317E59D5F55C28BE2A153618575AAAE423E812E432B6A102EBDC6BC21F68169F397D7DF82179EBFDE6E96806D58D1A874023B0924257458804EF446246
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.463 4f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:50:07.465 4f4 Recovering log #3.2021/08/03-23:50:07.468 4f4 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 StateTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateTM (copy)	
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2220737908562915
Encrypted:	false
SSDEEP:	6:mWAd3+q2PWXp+N23iKKdKgXz4rRIFUtpzWZmwPzSVkwOWXp+N23iKKdKgXz4q8LJ:jAova5KkgXiuFUtpzW/Pzq5f5KkgX2J
MD5:	0AE3499B640B99D664297AD4CAAF9950
SHA1:	C99FBE05F1161FC7FEDE6B680F99991C85ECA6AD
SHA-256:	54B2EA71B94A1417CEA3FB0D631E15A9B24DA2D0446A777EF2C4252CCA35D8BA
SHA-512:	2FEE34C8A24096CA89802AC313A5AFB6E98E2BE10279E094771A7177648A54FD82F6E582853FE97ADFB224B0E1B9A89FFFDBDEDB65A4DFCCA65B4AFEA8FB5F E7
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.750 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-23:50:07.752 12b8 Recovering log #3.2021/08/03-23:50:07.752 12b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2220737908562915
Encrypted:	false
SSDEEP:	6:mWAd3+q2PWXp+N23iKKdKgXz4rRIFUtpzWZmwPzSVkwOWXp+N23iKKdKgXz4q8LJ:jAova5KkgXiuFUtpzW/Pzq5f5KkgX2J
MD5:	0AE3499B640B99D664297AD4CAAF9950
SHA1:	C99FBE05F1161FC7FEDE6B680F99991C85ECA6AD
SHA-256:	54B2EA71B94A1417CEA3FB0D631E15A9B24DA2D0446A777EF2C4252CCA35D8BA
SHA-512:	2FEE34C8A24096CA89802AC313A5AFB6E98E2BE10279E094771A7177648A54FD82F6E582853FE97ADFB224B0E1B9A89FFFDBDEDB65A4DFCCA65B4AFEA8FB5F E7
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.750 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-23:50:07.752 12b8 Recovering log #3.2021/08/03-23:50:07.752 12b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4865
Entropy (8bit):	4.957635176551404
Encrypted:	false
SSDEEP:	48:Yc/UklSLklwHjvc2qA8qqTlYqlQKHoTw0PWH3CH3G/s8C1Nfct/9BhUJo3KhmeSz:n/CmHX9pcKI2ok0JCKL8VbOTQVuwn
MD5:	31BB33A20B7B6B33296D3C13B2523AB9
SHA1:	B5CC0B56533416E6AE796631E97AB55C3BA8D8E9
SHA-256:	458D90DA00DB9F5A2287073B7B3E89690B2A8A16919C875C678478D9959D82E8
SHA-512:	43624FE4068E9A5B4AF2266A761177DB617AAF1C98A5323FD544EA4F34F57619060D7D3D18AE3124F0B44158CB91AD97A678254DF4DDE778A22EDE997E7E1BA
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences.. (copy)	
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272533407727857","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	16746
Entropy (8bit):	5.577566093446622
Encrypted:	false
SSDEEP:	384:mFFtALl3oXL1kXqKf/pUZNCgVLH2HfDgrUR7mki4H:ZLlCL1kXqKf/pUZNCgVLH2Hf8rUvis
MD5:	475F3D4BBC3119DF82AB5B783EA98A62
SHA1:	217437F465582E891601243E3B5E5CC6654DBCC6
SHA-256:	72241BC661F27033B2E6D61D1D2F239C4D39D1AF2F5AA33D96FD391651F981CC
SHA-512:	E58E8F3C7A95EEB7434BD1D73049E0053F95DED6A7665310019B775F69129A16BFBE96457A26907E91F07E842D0F12C4D36F5D7B6A3821AC36D05EEA0F4F7314
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":"13272533407402468","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure 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):	16745
Entropy (8bit):	5.577525404226197
Encrypted:	false
SSDEEP:	384:mFFtJLl3oXL1kXqKf/pUZNCgVLH2HfDgrUH7mki4zk:SLlCL1kXqKf/pUZNCgVLH2Hf8rUdiz
MD5:	87AFFC51BE0233BBC3102CD0D97F2B3C
SHA1:	966FD6F81EF899E7DDBAAEC14A9CC8441B5114F9
SHA-256:	DEAB50A89BB1C2B5339C93495FE8B585377C25772C349825E3FCB74D588DB915
SHA-512:	FFD22017672A5765719210FB4462ECA51394A1C65455FF9B67BAAD0E1F05DA1A5EB4BB46646D6EEAB85064B681EF179153CAFBF1B1FB3203A62EBEBC652CD5F 3
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":"13272533407402468","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):	95
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	181ED05FAE6D31CDBFC2680CB632F859
SHA1:	B6391180B7167969686A3986E06D975F4CE67FAD
SHA-256:	62150C5EA1D8CFDE4916440F9662C32F3DCC1207BBC5441536D121EC683607E4
SHA-512:	40D79847C0420FA9395511DAA271B735ABD60CB55983F23DBF9552E56AAE1D915058D6D236D37D433FA7B16567957DB2C515BDB61B9032003914FF34EFA26BB5
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.220144103929602
Encrypted:	false
SSDEEP:	6:mL3+q2PWXp+N23iKKdKrQMxIFUtpgZmwPQVkwOWXp+N23iKKdKrQMFLJ:Lva5KkCFUtpg/PI5f5KktJ
MD5:	A1E94AD54FFAE53E04402E9A4A6C2745
SHA1:	8C01BAC564E8DA5B26819BE2599CB3418E893D1D
SHA-256:	76FD2E4B5C69321CBEDD184B2E31E92354D0B23D04009E8DE3C648140C45C5C1
SHA-512:	327A166ACC9F1147B6FB12B90134FBCA019A532807E415CED2F94610664CD394DA4007324D99D790C2936097EA69102D784EB538C29CB3391978BAAF99031C53
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.662 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-23:50:07.664 12b8 Recovering log #3.2021/08/03-23:50:07.664 12b8 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):	5.220144103929602
Encrypted:	false
SSDEEP:	6:mL3+q2PWXp+N23iKKdKrQMxIFUtpgZmwPQVkwOWXp+N23iKKdKrQMFLJ:Lva5KkCFUtpg/PI5f5KktJ
MD5:	A1E94AD54FFAE53E04402E9A4A6C2745
SHA1:	8C01BAC564E8DA5B26819BE2599CB3418E893D1D
SHA-256:	76FD2E4B5C69321CBEDD184B2E31E92354D0B23D04009E8DE3C648140C45C5C1
SHA-512:	327A166ACC9F1147B6FB12B90134FBCA019A532807E415CED2F94610664CD394DA4007324D99D790C2936097EA69102D784EB538C29CB3391978BAAF99031C53
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.662 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-23:50:07.664 12b8 Recovering log #3.2021/08/03-23:50:07.664 12b8 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):	345
Entropy (8bit):	5.145613037781457
Encrypted:	false
SSDEEP:	6:mP4q2PWXp+N23iKKdK7Uh2ghZIFUtpV3JZmwPWOvDkwOWXp+N23iKKdK7Uh2gnLJ:84va5KklhHh2FUtpn/P1vD5f5KklhHLJ
MD5:	0413A890A238147F0210B1140859F48A
SHA1:	99B13BF007CD853BA18D29E2BA7B617E0128C5A1
SHA-256:	17818832FF4D5ECA145A58127B3099969CC2F9B3289F9D9003BF8062E3519BCB
SHA-512:	87CBC634F825F4718864A20AEC84AE21AE44FBC665DC8EEA15D74E02F87CA9C8C4DBDC688F0B110CDF175D14DDAC14E39CDAE038B79585178EFFD2DC9629C0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.402 f50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-23:50:07.407 f50 Recovering log #3.2021/08/03-23:50:07.410 f50 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.oldww (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.145613037781457
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.oldww (copy)	
SSDEEP:	6:mP4q2PWXp+N23iKKdK7Uh2ghZIFUtpV3JZmwPWOvDkwOWXp+N23iKKdK7Uh2gnLJ:84va5KkIhHh2FUtpn/P1vD5f5KkIhHLJ
MD5:	0413A890A238147F0210B1140859F48A
SHA1:	99B13BF007CD853BA18D29E2BA7B617E0128C5A1
SHA-256:	17818832FF4D5ECA145A58127B3099969CC2F9B3289F9D9003BF8062E3519BCB
SHA-512:	87CBC634F825F4718864A20AEC84AE21AE44FBC665DC8EEA15D74E02F87CA9C8C4DBDC688F0B110CDF175D14DDAC14E39CDAE038B79585178EFFD2DC9629C0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.402 f50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/08/03-23:50:07.407 f50 Recovering log #3.2021/08/03-23:50:07.410 f50 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\6135dcf3-2bd0-4063-8acd-ff21039c283f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.236456494666434
Encrypted:	false
SSDEEP:	6:mx+q2PWXp+N23iKKdKusNpV/2jMGIFUtpBZmwPW9VkwOWXp+N23iKKdKusNpV/23:xva5KkFFUtpB/Py5f5KkOJ
MD5:	D1F525404C65BE1EB836BC02B9B1E11A
SHA1:	096324161D38303F2C672425ACB28198E9C02095
SHA-256:	91FBDF32EF8B3C732A043FD5B2274323CC7B8B268281E673B61A1102DC655AE9
SHA-512:	6E1F26185A25A7C84FF08AAA19A2A72C74EEB2E5D8A98081BB9608AD3426944F53DBD5BE97BA26F9AA785ED4D5A181E51F1626AD4BCBA12F3E81827E6601A458
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Preview:	2021/08/03-23:50:07.721 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:50:07.722 12b8 Recovering log #3.2021/08/03-23:50:07.723 12b8 Reusing old log C:\Users\user\A ppData\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):	5.236456494666434
Encrypted:	false
SSDEEP:	6:mx+q2PWXp+N23iKKdKusNpV/2jMGIFUtpBZmwPW9VkwOWXp+N23iKKdKusNpV/23:xva5KkFFUtpB/Py5f5KkOJ
MD5:	D1F525404C65BE1EB836BC02B9B1E11A
SHA1:	096324161D38303F2C672425ACB28198E9C02095
SHA-256:	91FBDF32EF8B3C732A043FD5B2274323CC7B8B268281E673B61A1102DC655AE9
SHA-512:	6E1F26185A25A7C84FF08AAA19A2A72C74EEB2E5D8A98081BB9608AD3426944F53DBD5BE97BA26F9AA785ED4D5A181E51F1626AD4BCBA12F3E81827E6601A45 8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.721 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:50:07.722 12b8 Recovering log #3.2021/08/03-23:50:07.723 12b8 Reusing old log C:\Users\user\A ppData\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 State3f (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.283268553043629
Encrypted:	false
SSDEEP:	6:mWK3+q2PWXp+N23iKKdKusNpqz4rRIFUtpzcIjmWZmwPzEVkwOWXp+N23iKKdKua:jK3+va5KkmiuFUtpzeW/PzEV5f5Kkm2J
MD5:	79067CDCD2BF823C3781946D682A01A3
SHA1:	394E7E6041FF3C5D61A25BBA8FF6B049EC5A0DA5
SHA-256:	172A91BD4F4D89618F3A608D2FAF1B867400C55F4865AA0D58BDF2257530B979
SHA-512:	11524926766C1077D2EB1FB03F1AC0B1BBFE898629CB10CFF60DA67BC5A8A457AF2CE246A5C5EC109E5AB8C80852EC7BDCBB1492B4313D8EF9FB353040AE6E 2A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.750 14cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-23:50:07.751 14cc Recovering log #3.2021/08/03-23:50:07.752 14cc Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.283268553043629
Encrypted:	false
SSDEEP:	6:mWK3+q2PWXp+N23iKKdKusNpqz4rRIFUtpzcIjmWZmwPzEVkwOWXp+N23iKKdKua:jK3+va5KkmiuFUtpzeW/PzEV5f5Kkm2J
MD5:	79067CDCD2BF823C3781946D682A01A3
SHA1:	394E7E6041FF3C5D61A25BBA8FF6B049EC5A0DA5
SHA-256:	172A91BD4F4D89618F3A608D2FAF1B867400C55F4865AA0D58BDF2257530B979
SHA-512:	11524926766C1077D2EB1FB03F1AC0B1BBFE898629CB10CFF60DA67BC5A8A457AF2CE246A5C5EC109E5AB8C80852EC7BDCBB1492B4313D8EF9FB353040AE6E2A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.750 14cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:50:07.751 14cc Recovering log #3.2021/08/03-23:50:07.752 14cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.264399092620179
Encrypted:	false
SSDEEP:	6:mp2FUT+q2PWXp+N23iKKdKusNpZQMxIFUtpmUpmWZmwPmUm3VkwOWXp+N23iKKd0:vuT+va5KkMFUtpwW/PS3V5f5KkTJ
MD5:	24C0A70BA9FD3B1FEE4DB55F1B07A6CD
SHA1:	23120315A1892BE00A32F6BCB4D1EE32B48A7A72
SHA-256:	D1BDADDEEDFA0E170CABFF997F66E17B4CF55AB8F0513DE94344442BFC8D91ED
SHA-512:	4F378D65D96777D13F6525E0DF3B3D96CCDB122950EA794F55F6BB4F2917FE54CD4EE698C5DCF5049C8A3C51C2C17B29307E79BECD2E0EDBC823A7C19515C39
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:23.909 14cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-23:50:23.913 14cc Recovering log #3.2021/08/03-23:50:23.914 14cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old97 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.264399092620179
Encrypted:	false
SSDEEP:	6:mp2FUT+q2PWXp+N23iKKdKusNpZQMxIFUtpmUpmWZmwPmUm3VkwOWXp+N23iKKd0:vuT+va5KkMFUtpwW/PS3V5f5KkTJ
MD5:	24C0A70BA9FD3B1FEE4DB55F1B07A6CD
SHA1:	23120315A1892BE00A32F6BCB4D1EE32B48A7A72
SHA-256:	D1BDADDEEDFA0E170CABFF997F66E17B4CF55AB8F0513DE94344442BFC8D91ED

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old97 (copy)	
SHA-512:	4F378D65D96777D13F6525E0DF3B3D96CCDB122950EA794F55F6BB4F2917FE54CD4EE698C5DCF5049C8A3C51C2C17B29307E79BECD2E0EDBC823A7C19515C9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:23.909 14cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-23:50:23.913 14cc Recovering log #3.2021/08/03-23:50:23.914 14cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.208842146049338
Encrypted:	false
SSDEEP:	12:7zva5KkkGHArBFUtpLn/PL2xz5f5KkkGHAryJ:7Ta5KkkGgPgB7ef5KkkGga
MD5:	9FE8416098EBDD1174D025A932A6C5FA
SHA1:	13E5109D7B20F0E5C84122576673DC0CEBF7799D
SHA-256:	84825C2A7C7A226D14C4570DA70C7F059E1BA3DDC134F2A0005CEC7A90DF56D9
SHA-512:	8612BF451E94CF37EED641C4E940956671AD3D1FC66EA6E77807C8DCC8ED7DDE591DB77A59D7D2D91A901458EE5EE18B0E009E58507B9B279014E3E7F9E248F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.491 4f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:50:40.494 4f4 Recovering log #3.2021/08/03-23:50:40.497 4f4 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.oldd (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.208842146049338
Encrypted:	false
SSDEEP:	12:7zva5KkkGHArBFUtpLn/PL2xz5f5KkkGHAryJ:7Ta5KkkGgPgB7ef5KkkGga
MD5:	9FE8416098EBDD1174D025A932A6C5FA
SHA1:	13E5109D7B20F0E5C84122576673DC0CEBF7799D
SHA-256:	84825C2A7C7A226D14C4570DA70C7F059E1BA3DDC134F2A0005CEC7A90DF56D9
SHA-512:	8612BF451E94CF37EED641C4E940956671AD3D1FC66EA6E77807C8DCC8ED7DDE591DB77A59D7D2D91A901458EE5EE18B0E009E58507B9B279014E3E7F9E248F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.491 4f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:50:40.494 4f4 Recovering log #3.2021/08/03-23:50:40.497 4f4 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):	5.1846079935233105
Encrypted:	false
SSDEEP:	12:+Iva5KkkGHArqiuFUtph/Po5f5KkkGHArq2J:+6a5KkkGgCgWf5KkkGg7
MD5:	06191E599C764D8335FB9124A8A4BF3E
SHA1:	E378F09962F23720F2BDCC32D90D9E10B28F6F1E
SHA-256:	9AC69248CF01F5444E4AA723BBFF6008C7A1579193109ECB343912C2D40542EC
SHA-512:	B283D50E97A7634EA9A7E43D5D65BD81EBA665E7858146B29D5FF6C78E53EE9567BE508C5DD4BB22E76FE7DFA5EDF638E335FA71DB7AAC16256C8CE12BF6AF1F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.512 13d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:50:40.513 13d0 Recovering log #3.2021/08/03-23:50:40.514 13d0 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):	5.1846079935233105
Encrypted:	false
SSDEEP:	12:+Iva5KkkGHArqiuFUtph/Po5f5KkkGHArq2J:+6a5KkkGgCgWf5KkkGg7
MD5:	06191E599C764D8335FB9124A8A4BF3E
SHA1:	E378F09962F23720F2BDCC32D90D9E10B28F6F1E
SHA-256:	9AC69248CF01F5444E4AA723BBFF6008C7A1579193109ECB343912C2D40542EC
SHA-512:	B283D50E97A7634EA9A7E43D5D65BD81EBA665E7858146B29D5FF6C78E53EE9567BE508C5DD4BB22E76FE7DFA5EDF638E335FA71DB7AAC16256C8CE12BF6AF1F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.512 13d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:50:40.513 13d0 Recovering log #3.2021/08/03-23:50:40.514 13d0 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:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.246939465005096
Encrypted:	false
SSDEEP:	6:mSB9+q2PWXp+N23iKKdKpIFUtpoJZmwPu9VkwOWXp+N23iKKdKa/WLJ:hiva5KkmFUtp6/Pw5f5KkaUJ
MD5:	BF3C97A0C9DFA7A62921038028BB2037
SHA1:	36612D33C61F529A8D29D974AFDEAF1B94B99E70
SHA-256:	CB36742E714649DD1D820E893B4CFF825C87B61003B0F207BF30D7DCE797C5C5
SHA-512:	FC89E913DFE832478A63FBEF8EE58A44524A40DCC564C256AC7126338A70E65CFB32E4C72192535F1D70F9B8C24067BB7851F32CE3F0B58FCA0898F78D853DF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.409 12d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-23:50:07.413 12d8 Recovering log #3.2021/08/03-23:50:07.424 12d8 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):	5.246939465005096
Encrypted:	false
SSDEEP:	6:mSB9+q2PWXp+N23iKKdKpIFUtpoJZmwPu9VkwOWXp+N23iKKdKa/WLJ:hiva5KkmFUtp6/Pw5f5KkaUJ
MD5:	BF3C97A0C9DFA7A62921038028BB2037
SHA1:	36612D33C61F529A8D29D974AFDEAF1B94B99E70

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old (copy)	
SHA-256:	CB36742E714649DD1D820E893B4CFF825C87B61003B0F207BF30D7DCE797C5C5
SHA-512:	FC89E913DFE832478A63FBEF8EE58A44524A40DCC564C256AC7126338A70E65CFB32E4C72192535F1D70F9B8C24067BB7851F32CE3F0B58FCA0898F78D853DF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:07.409 12d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-23:50:07.413 12d8 Recovering log #3.2021/08/03-23:50:07.424 12d8 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\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.567510434396337
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvFj7wU3IHRUenHQ:YI6UUhVseKUewqPeUer2UefFfwU4xUew
MD5:	12724D3179B62102A8A961ECDFD1E2E3
SHA1:	99DC3D43EA0822E314C4364A58E2CAB928860C74
SHA-256:	5B1700D7AC08E249926792AD0C56E303715DF40F6C42B57432FDEF2A689EFF3B
SHA-512:	3369A2424C70CDCAF58C010A1B555BF5950B0F6D0CE8FA1BFB0B81164F5566C59FFA7ACC80539EB1A45A1006F9E316CBDDEF984287C7AB00C19D9CEE3622246
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659595811.942149,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628059811.942155},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bf21dda3-4975-45e9-a84e-4901832b167a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.567510434396337
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvFj7wU3IHRUenHQ:YI6UUhVseKUewqPeUer2UefFfwU4xUew
MD5:	12724D3179B62102A8A961ECDFD1E2E3
SHA1:	99DC3D43EA0822E314C4364A58E2CAB928860C74
SHA-256:	5B1700D7AC08E249926792AD0C56E303715DF40F6C42B57432FDEF2A689EFF3B
SHA-512:	3369A2424C70CDCAF58C010A1B555BF5950B0F6D0CE8FA1BFB0B81164F5566C59FFA7ACC80539EB1A45A1006F9E316CBDDEF984287C7AB00C19D9CEE3622246
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659595811.942149,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628059811.942155},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

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

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.549001766844434
Encrypted:	false
SSDEEP:	3:tUK6xWcLX9ddEAgZmwv3IxWcLWSTu0SVV8sIxWcLWSTu0SVWGv:mi8jWAgZmwPfwYVVvfwYVtv
MD5:	D5FD96C5564690769F33A57E524E3791
SHA1:	42C1078DC6F090F11B8BCB7D12E92E74F104EAFD
SHA-256:	89ED7D875094F9F47703A8A4D0B3A5E69447C138EBBD936DC73EE5BAA38DD587
SHA-512:	5234A430EEC77F11AC9F1731315D169A9DB54813604B339B47ECFAB537F88BFFDF07A6A7FC74A0D3A86FBB7B61C75B148DE7D9002632C99FCD16E7A7D41EB7I 9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:39.213 1a8c Recovering log #3.2021/08/03-23:50:39.376 1a8c Delete type=0 #3.2021/08/03-23:50:39.376 1a8c Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old6 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.549001766844434
Encrypted:	false
SSDEEP:	3:tUK6xWcLX9ddEAgZmwv3IxWcLWSTu0SVV8sIxWcLWSTu0SVWGv:mi8jWAgZmwPfwYVVvfwYVtv
MD5:	D5FD96C5564690769F33A57E524E3791
SHA1:	42C1078DC6F090F11B8BCB7D12E92E74F104EAFD
SHA-256:	89ED7D875094F9F47703A8A4D0B3A5E69447C138EBBD936DC73EE5BAA38DD587
SHA-512:	5234A430EEC77F11AC9F1731315D169A9DB54813604B339B47ECFAB537F88BFFDF07A6A7FC74A0D3A86FBB7B61C75B148DE7D9002632C99FCD16E7A7D41EB7I 9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:39.213 1a8c Recovering log #3.2021/08/03-23:50:39.376 1a8c Delete type=0 #3.2021/08/03-23:50:39.376 1a8c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
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\f24bcec3-7020-43bc-9ad2-a07a7ea471f6.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):	16746
Entropy (8bit):	5.577566093446622
Encrypted:	false
SSDEEP:	384:mFFtALl3oXL1kXqKf/pUZNCgVLH2HfDgrUR7mki4H:ZLlCL1kXqKf/pUZNCgVLH2Hf8rUvis
MD5:	475F3D4BBC3119DF82AB5B783EA98A62
SHA1:	217437F465582E891601243E3B5E5CC6654DBCC6
SHA-256:	72241BC661F27033B2E6D61D1D2F239C4D39D1AF2F5AA33D96FD391651F981CC
SHA-512:	E58E8F3C7A95EEB7434BD1D73049E0053F95DED6A7665310019B775F69129A16BFBE96457A26907E91F07E842D0F12C4D36F5D7B6A3821AC36D05EEA0F4F7314
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":"13272533407402468","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f33600a0-b641-497d-834e-096628884d12.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577525404226197
Encrypted:	false
SSDEEP:	384:mFFtJLl3oXL1kXqKf/pUZNCgVLH2HfDgrUH7mki4zk:SLlCL1kXqKf/pUZNCgVLH2Hf8rUdiz
MD5:	87AFFC51BE0233BBC3102CD0D97F2B3C
SHA1:	966FD6F81EF899E7DDBAAEC14A9CC8441B5114F9
SHA-256:	DEAB50A89BB1C2B5339C93495FE8B585377C25772C349825E3FCB74D588DB915
SHA-512:	FFD22017672A5765719210FB4462ECA51394A1C65455FF9B67BAAD0E1F05DA1A5EB4BB46646D6EEAB85064B681EF179153CAFBF1B1FB3203A62EBEBC652CD5F3
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":"13272533407402468","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fab39d00-3328-46a0-9ef2-79f4ac781043.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):	4865
Entropy (8bit):	4.957635176551404
Encrypted:	false
SSDEEP:	48:Yc/UklSLklwHjvc2qA8qqTlYqlQKHoTw0PWH3CH3G/s8C1Nfct/9BhUJo3KhmeSz:n/CmHX9pcKI2ok0JCKL8VbOTQVuwn
MD5:	31BB33A20B7B6B33296D3C13B2523AB9
SHA1:	B5CC0B56533416E6AE796631E97AB55C3BA8D8E9
SHA-256:	458D90DA00DB9F5A2287073B7B3E89690B2A8A16919C875C678478D9959D82E8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fab39d00-3328-46a0-9ef2-79f4ac781043.tmp	
SHA-512:	43624FE4068E9A5B4AF2266A761177DB617AAF1C98A5323FD544EA4F34F57619060D7D3D18AE3124F0B44158CB91AD97A678254DF4DDE778A22EDE997E7E1BA!
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272533407727857","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.217729521154463
Encrypted:	false
SSDEEP:	6:mDN+q2PWXp+N23iKKdKfrzAdIFUtpnRgFZZmwPnRgFNVkwOWXp+N23iKKdKfrzId:UN+va5Kk9FUtpRAZ/PRANV5f5Kk2J
MD5:	A913AAB97697B4AB71AB57B831AAF3A8
SHA1:	CE3F202546AA5207A9CE907A99655B9A9C7F5267
SHA-256:	08AF1F01449747655F445816E373283E84E3395F0EADE4684B7F0A0CA715E329
SHA-512:	560ACF3690AFEC9644BBCFB8D5CAEB08440096BD2D90C0601179BD36C8CF2EE35A104DC55DB5A86B48807D3F13CAE47099103E909FA9CF8232BC409953434CE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.745 144c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-23:50:40.747 144c Recovering log #3.2021/08/03-23:50:40.747 144c 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.old8f (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.217729521154463
Encrypted:	false
SSDEEP:	6:mDN+q2PWXp+N23iKKdKfrzAdIFUtpnRgFZZmwPnRgFNVkwOWXp+N23iKKdKfrzId:UN+va5Kk9FUtpRAZ/PRANV5f5Kk2J
MD5:	A913AAB97697B4AB71AB57B831AAF3A8
SHA1:	CE3F202546AA5207A9CE907A99655B9A9C7F5267
SHA-256:	08AF1F01449747655F445816E373283E84E3395F0EADE4684B7F0A0CA715E329
SHA-512:	560ACF3690AFEC9644BBCFB8D5CAEB08440096BD2D90C0601179BD36C8CF2EE35A104DC55DB5A86B48807D3F13CAE47099103E909FA9CF8232BC409953434CE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:50:40.745 144c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-23:50:40.747 144c Recovering log #3.2021/08/03-23:50:40.747 144c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174336
Entropy (8bit):	6.079351421192836
Encrypted:	false
SSDEEP:	3072:LUVGaYTJQE+mugy9+QV1T7IRwdfLSNPHFcbXafIB0u1GOJmA3iuRA:QAxaV+QfT7GSmhlaqfIlUOoSiuRA
MD5:	8CC158CA3A0C7848196DB60A5A9F5719
SHA1:	96834E7B5EC4D769E807A47ED48822969735621F
SHA-256:	550E4E53E4AE2889382D35525B3FD9B0E12896F666AF0CFE45B7F1BCD1844842
SHA-512:	4FD8BD1ED6F5502D27A40D942954AD535FEC43BA202E08986340894B4273B3CC3273D698C187B79AF11632DEA60A2FDEC270E1488337A01D3A35D8DA2735D99
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628059810237143e+12,"network":1.628027412e+12,"ticks":5115804561.0,"uncertainty":4575038.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\a2706294-a71c-4cb6-aaf9-8ad572980a7d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174336
Entropy (8bit):	6.079351605951816
Encrypted:	false
SSDEEP:	3072:LNuGaYTJQE+mugy9+QV1T7IRwdfLSNPHFcbXafIB0u1GOJmA3iuRA:JDxaV+QfT7GSmhlaqfIlUOoSiuRA
MD5:	ADB95D299606736A2FD09C4B4FAEA30C
SHA1:	1F592215DBF307EE0359A4F4B87EEB70091821A9
SHA-256:	004571134A78BA4376F11692BC85F1710D101F6EE26D619F20FEDDDEE6CD39B5
SHA-512:	22D5B5F23EA28DF552F3DBDE8BD2C508B39C58830A7C7436AB08DC7C23AA1EC284B001804C59CB2B5C4C8C565B03AE899304ED28C5FE537BDAF7A2A906798(30
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628059810237143e+12,"network":1.628027412e+12,"ticks":5115804561.0,"uncertainty":4575038.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Temp\16dc31c6-a9cb-4ca6-a126-83126ce938c0.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

C:\Users\user\AppData\Local\Temp\16dc31c6-a9cb-4ca6-a126-83126ce938c0.tmp	
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\76772ec3-5571-48d8-9959-44ad51ffe706.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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.-l..`.Q.{...F0D. .0...!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\a560c9d0-2165-470c-8a3d-f174243cb113.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;..._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q...:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	4668
Entropy (8bit):	4.642876069737353
Encrypted:	false
SSDEEP:	96:VFF1Sf2hK2k/J1Jg+5A202AI2iQrIMprXCb2dyfqJrhAYi6lv1WIv0FW:VFHSbjurICrXe2cwreYVTXP
MD5:	5045E40AD94AB9CCF3CDF9B1F6A8E7F2
SHA1:	AEB73F3C96285693579D7BFC1C607CDEA86C97BA
SHA-256:	D8A6B06E5A8DBF60210EA75CE59785141D1748212DD4C5E78FE3667A23B0CA3C
SHA-512:	B0C8540D80EFB54516C37D94F2D2ED8D4085AE1B6A9339555B27BD60143661556F88E2270ECC9D0E2B28268969FCD8ED07493FE8FDDE15E16C5EEE791279786
Malicious:	false

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 6ceb9ee02519a526fe4d805699792062d4b86c71cd1f39b723a6d168b490e163 28e6616b7b7bdc5f1aca97c386c6406cb 0db99a1121b041067c9a6ca2a9e4eac.SERVER_HANDSHAKE_TRAFFIC_SECRET 6ceb9ee02519a526fe4d805699792062d4b86c71cd1f39b723a6d168b490e163 7 6af871f97864d6ba2b32199892956babae19dbf17177c4b887414322dd7e586.CLIENT_HANDSHAKE_TRAFFIC_SECRET e93811f83887f977c171f545b94411dc6b 25f39d8d8db80c6b3b0af0cd886311 cc0b0ab9eff83d0f57b504d643679b5a7525d9bd951c73f248be3545e67cdbad.SERVER_HANDSHAKE_TRAFFIC_SECRET e9 3811f83887f977c171f545b94411dc6b25f39d8d8db80c6b3b0af0cd886311 2283c0170bf27ae185732253ece585a4f533062f84527f7388995e07039223b5.CLIENT_HANDS HAKE_TRAFFIC_SECRET 87b9145b40b14cbab442d35eefba699e433982bb7d4e7ccf8368816f11f90f91 f0025ade6a050ee7c882116c2552723d1c2829a28517a 0ba53b79598eef1057d.SERVER_HANDSHAKE_TRAFFIC_SECRET 87b9145b40b14cbab442d35eefba699e433982bb7d4e7ccf8368816f11f90f91 925514c5d0368 8c18efa6e4758332776b8a7f4ffe4715143f4ed4e4365e8406d.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\c2bf007a-cb49-4124-9079-74984806fea0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\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:	{.. "1018984561488520517": {.. "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_dir1048_1945874024\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:	192:0IprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
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",.. "pl aceholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\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:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".... .. ....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\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:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\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
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1
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_dir1048_1945874024\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

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\CRX_INSTALL_locales\cs\messages.json	
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_dir1048_1945874024\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".. },.. "152214068331 8860351": {.. "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_dir1048_1945874024\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
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "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_dir1048_1945874024\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

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\CRX_INSTALL_locales\el\messages.json	
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djlV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C013
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": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\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:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "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_dir1048_1945874024\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
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_dir1048_1945874024\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

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\CRX_INSTALL_locales\et\messages.json	
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB1120272356
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_dir1048_1945874024\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": ".... .. ..".. },.. "1282768764603190 75": {.. "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_dir1048_1945874024\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
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "1282768764603190 75": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "1522140683318860351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "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_dir1048_1945874024\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

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\CRX_INSTALL_locales\fil\messages.json	
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_dir1048_1945874024\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_dir1048_1945874024\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
Preview:	{.. "1018984561488520517": {.. "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_dir1048_1945874024\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

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\CRX_INSTALL_locales\hi\messages.json	
Preview:	{.. "1018984561488520517": {.. "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_dir1048_1945874024\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:	{.. "1018984561488520517": {.. "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".. },.. "1636686747687494376": {.. "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": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir1048_1945874024\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:	E9A4AF31B1A276F395599BB620A3164CABF3459F3C102DD3F57DFEA734510BD985DE65CB409E1975559ACCC615075439A08E1DEBE22C90A0ABCAA3CAFEE79AC7
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "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 $START_LINK$Google Home alkalmaz.sbanEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

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 3, 2021 23:50:11.921334982 CEST	192.168.2.3	8.8.8.8	0x347b	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:50:11.926991940 CEST	192.168.2.3	8.8.8.8	0xbb5c	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:50:39.884252071 CEST	192.168.2.3	8.8.8.8	0x94e4	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 3, 2021 23:50:11.957514048 CEST	8.8.8.8	192.168.2.3	0x347b	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 23:50:11.970314980 CEST	8.8.8.8	192.168.2.3	0xbb5c	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:50:11.970314980 CEST	8.8.8.8	192.168.2.3	0xbb5c	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 23:50:39.927423954 CEST	8.8.8.8	192.168.2.3	0x94e4	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:50:39.927423954 CEST	8.8.8.8	192.168.2.3	0x94e4	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: 1048 Parent PID: 2792

General

Start time:	23:50:06
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://125.47.255.248'
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: 2588 Parent PID: 1048

General

Start time:	23:50:08
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,275807099243823227,4504885289812018906,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1832 /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