ID: 338157
Cookbook: browseurl.jbs
Time: 18:23:56
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

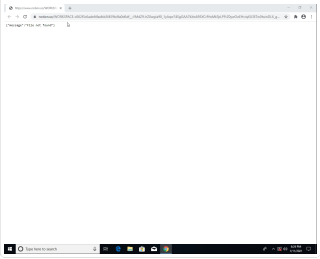
Analysis Report https://www.notion.so/WORKSPACE-c0…

Overview

General Information

Sample URL:	https://www.notion.so/WORKSPACE-c062f3c6adef4fadbb3f459b4fa0d6df__;!!MdZ9-h...!a90_1yAqw74SgGAA7kXe4i93XCrFfwMkTpLPFrZ0ywOoEHviqXU3ETw0IwinDLX_gcs$ >(s).
Analysis ID:	338157

Most interesting Screenshot:



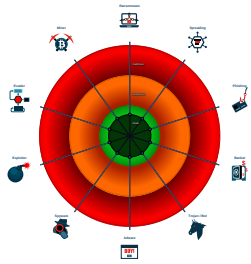
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 7064 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://www.notion.so/WORKSPACE-c062f3c6adef4fadbb3f459b4fa0d6df__;!!MdZ9-hZ0wg!a90_1yAqw74SgGAA7kXe4i93XCrFfwMkTpLPFrZ0ywOoEHviqXU3ETw0IwinDLX_gcs$ >(s).' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5964 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1624,3718329257152011507,15757246875424185 32,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1732 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

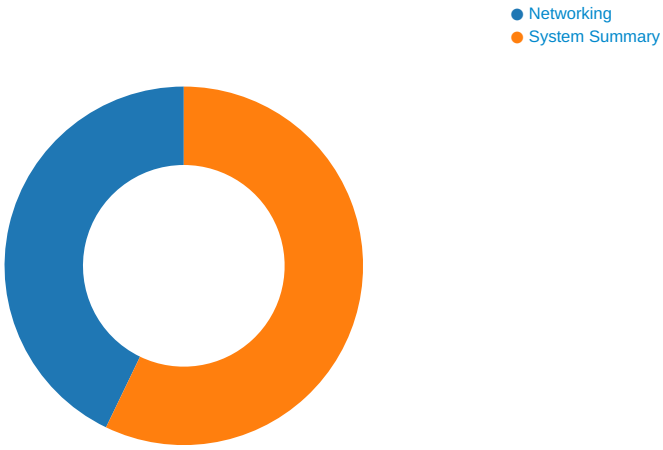
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



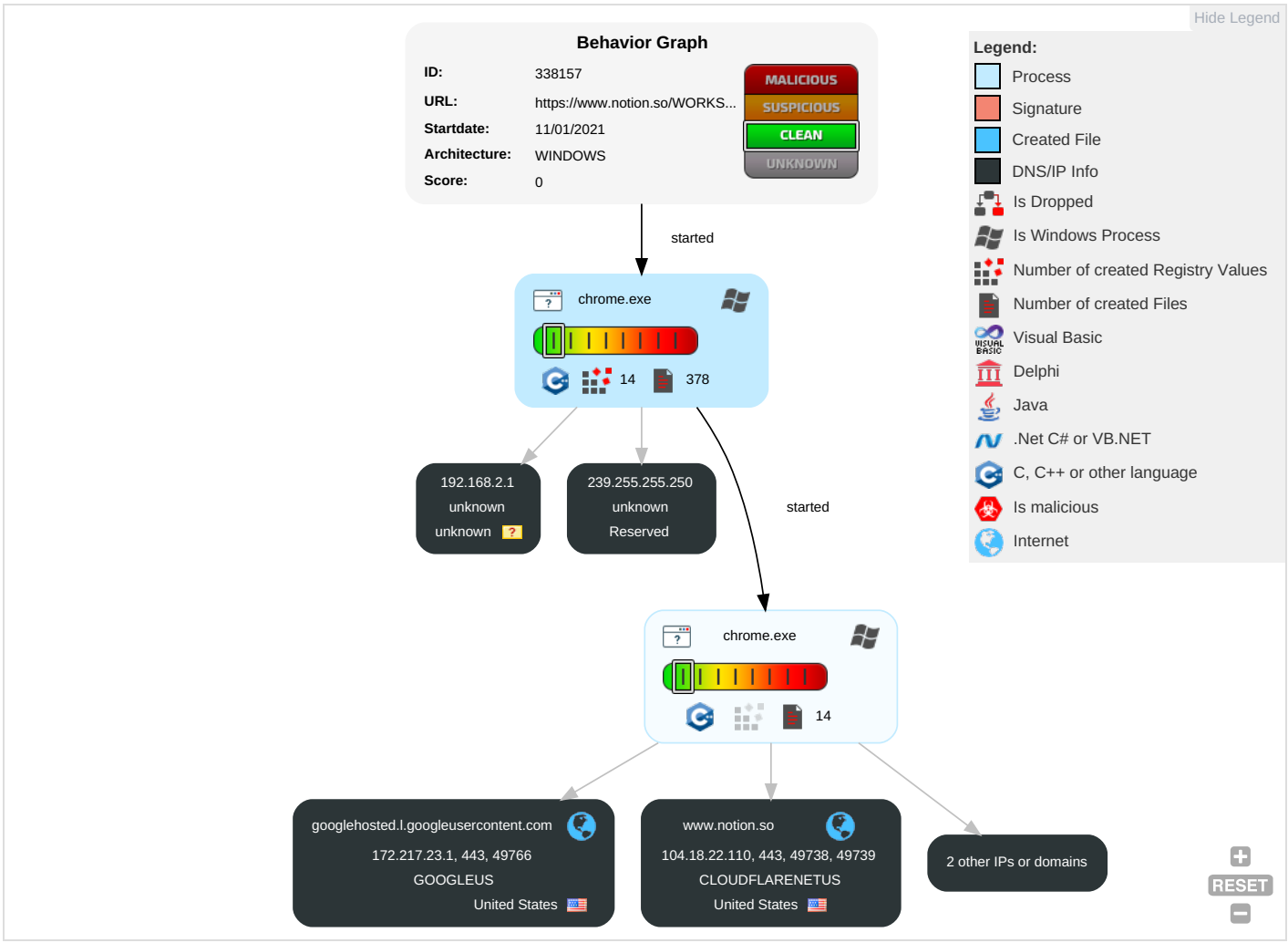
Click to jump to signature section

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 1	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

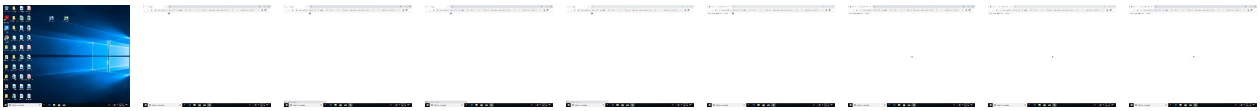
Behavior Graph

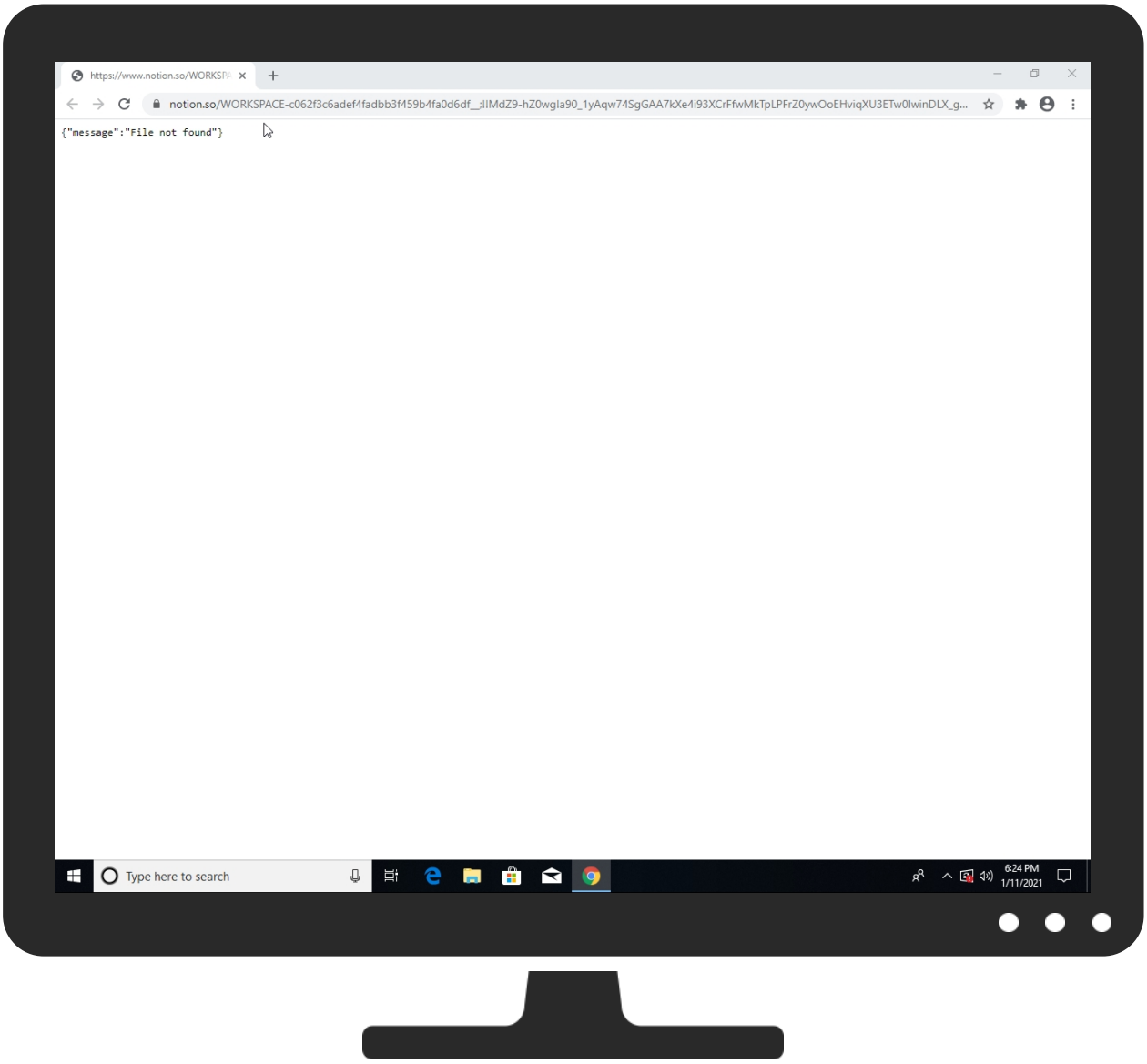


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.notion.so/WORKSPACE-c062f3c6adef4fadbb3f459b4fa0d6df__;!!MdZ9-hZ0wg!a90_1yAqw74SgGAA7kXe4i93XCrFfwMkTpLPFrZ0ywOoEHviqXU3ETw0lwinDLX_gcs$ >(s).	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://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.notion.so	104.18.22.110	true	false		high
googlehosted.l.googleusercontent.com	172.217.23.1	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

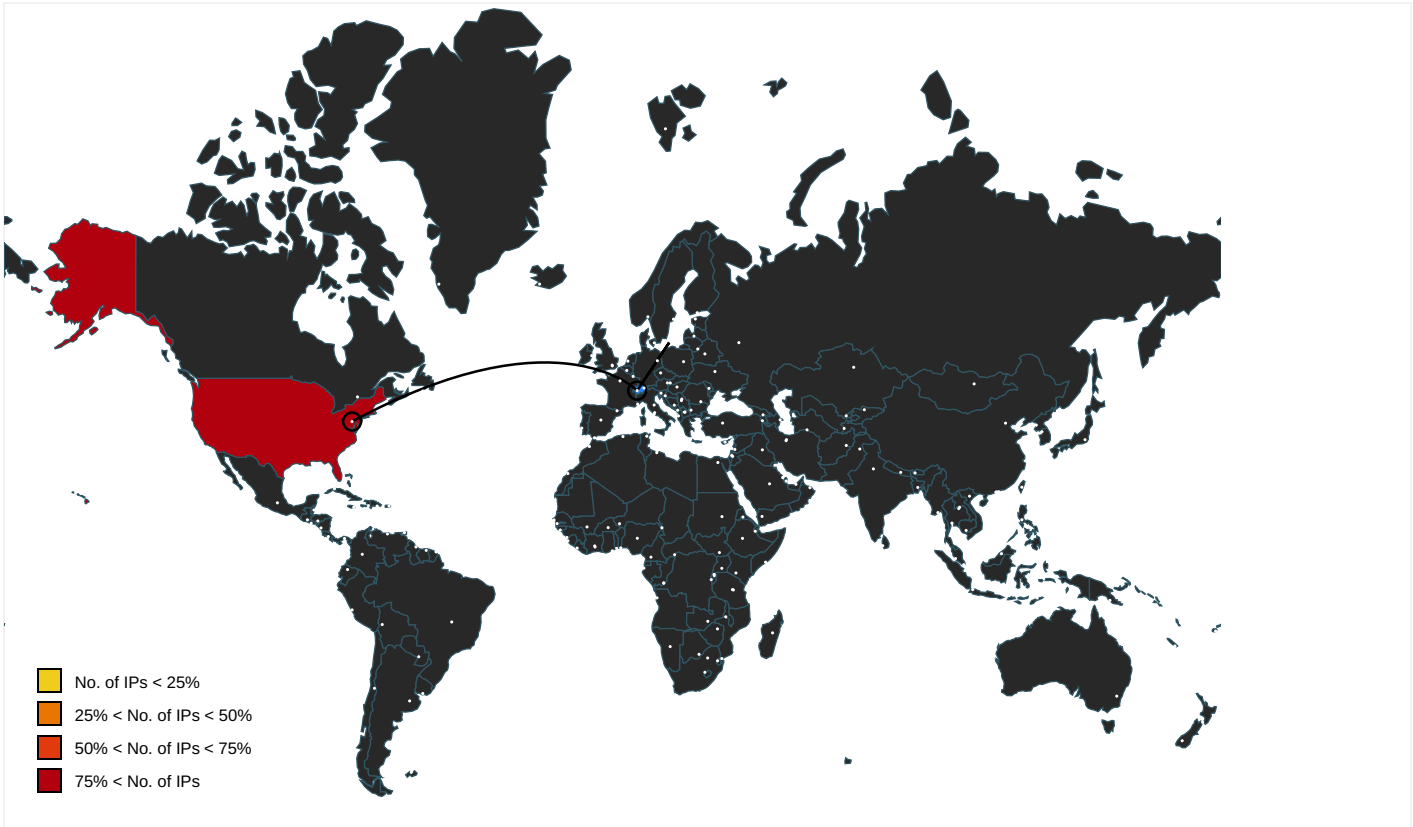
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.notion.so/WORKSPACE-c062f3c6adef4fadbb3f459b4fa0d6df__;!!MdZ9-hZ0wg!a90_1yAqw74SgGAA7kXe4i93XCrFfwMkTpLPFrZ0ywOoEHviqXU3ETw0lwinDLX_gcs$%20%3E(s).	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	b6ba2ac4-6d70-4f63-ac01-9968f3bdc2c2.tmp.1.dr, 8a246231-56bb-40de-bdb2-4d71ba0987c8.tmp.1.dr, 567755ea-cea5-434f-a851-0393fd22db3d.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients2.googleusercontent.com	567755ea-cea5-434f-a851-0393fd22db3d.tmp.1.dr	false		high
http://https://www.notion.so/WORKSPACE-c062f3c6adef4fadbb3f459b4fa0d6df__;	Current Session.0.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.1	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.22.110	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338157
Start date:	11.01.2021
Start time:	18:23:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.notion.so/WORKSPACE-c062f3c6adef4fadbb3f459b4fa0d6df__;!!MdZ9-hZ0wg!a90_1yAqw74SgGAA7kXe4i93XCrFfwMkTpLPFrZ0ywOoEHviqXU3ETw0IwinDLX_gcs$ >(s).
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@27/154@2/5
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 13.88.21.125, 172.217.20.238, 172.217.22.205, 172.217.23.78, 173.194.187.106, 216.58.207.131, 172.217.20.234, 172.217.23.42, 172.217.23.74, 172.217.22.202, 172.217.22.234, 216.58.207.138, 216.58.207.170, 51.104.139.180, 92.122.213.194, 92.122.213.247, 8.248.133.254, 67.26.75.254, 8.248.121.254, 8.253.204.121, 67.26.139.254, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, accounts.google.com, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, clientservices.googleapis.com, ctldl.windowsupdate.com, www.googleapis.com, r5---sn-4g5e6nsr.gvt1.com, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, clients2.google.com, redirector.gvt1.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, clients.l.google.com, r5.sn-4g5e6nsr.gvt1.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

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:\Users\user\AppData\Local\Google\Chrome\User Data\012cff24-b5fd-4921-bb49-3dc144265ace.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):	163030
Entropy (8bit):	6.082364079410256
Encrypted:	false
SSDEEP:	3072:7pFFh/DYC/ddlBuZ92QklEFFcbXafIB0u1GOJmA3iuR1:1BsC/ddlBuZswaqfIlUOoSiuR1
MD5:	A3BD8E96F8DFC37ABD5A913A3A3A905D
SHA1:	8BD39D164D018929C619F6C231674945BBCB697D
SHA-256:	9D6AE6592BE06A5B1F4EDD7F44E07C544432901A8903352AFD9951F3125C1307
SHA-512:	3CFBCC3284FF1768FB01B204AF6FF96C193D9EE7B3450BA98F2FCDB0DDB2D53AE788BDB728161FBB7BAEA08AF585C3E4BC15C7009FE82853C7E11C5099BC9E08
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.610385887840172e+12,"network":1.610385889e+12,"ticks":304245116.0,"uncertainty":4641773.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBljSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\1d2bc0c4-70e5-41ef-9f22-eb20a66db179.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):	163030
Entropy (8bit):	6.082363917490341
Encrypted:	false
SSDEEP:	3072:7v1Fh/DYC/ddlBuZ92QklEFFcbXafIB0u1GOJmA3iuR1:DxsC/ddlBuZswaqfIlUOoSiuR1
MD5:	928715EBEBFD1C157D3FB24C51C536D7
SHA1:	850038D71C2FD725BFC751DDC17DEF4303F73C4B
SHA-256:	FC2E802A0C150702F5FBA70D85F13CEABA211FFB5366042AA5746E958F4C60AC
SHA-512:	7FFF70055B76BEEDB4FAD942AE5F926D964B6D3E604E01CD23E189968665CCF4EA744721DA0913C2867A0B7F9E8A5A993EC00DEAC6CC696CA4BA6C391224FE03
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.610385887840172e+12,"network":1.610385889e+12,"ticks":304245116.0,"uncertainty":4641773.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBljSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\8dafb4ef-29cf-4d95-a6f8-4e1e2b48b2a9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.74456373920437
Encrypted:	false
SSDEEP:	768:zLCXFJSSkp8CHrmJFqeLQqsidmwjeeKwCKy6pb:PCraeLD7Ms
MD5:	A20226613E6D19D9E9724995DEE04580
SHA1:	AD8101F7CBE02B8885F109166771853FD49EBEBF
SHA-256:	A52E19E55EE8BA76E2B667DD407BB73DCEEE6C9E178EE383755A39DB675ACD8C
SHA-512:	50696D09D2ED5EB7F3D5FC073ECB6FFA1C121DB440B69A6732B35237B04B727E21F76B5F36CE52A75EF0A117D5EB5D09CB074090ADE12DE0CD844D0AC66FB89

C:\Users\user\AppData\Local\Google\Chrome\User Data\8dafb4ef-29cf-4d95-a6f8-4e1e2b48b2a9.tmp	
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...q.8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1939cb49-63bb-41fd-b1d5-332fafa0cfa7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\559861d1-a343-4e85-8a13-e3fe17ac103e.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):	1208
Entropy (8bit):	5.554077452103018
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeioao1dkUF3zkq/HeUe8zUeqHs7wUyOX8RUeiQ:Ym6UUhyKUeiZnUF4qPeUekUeqawUyOXU
MD5:	EED623D41763B30EA28F978880B1EB57
SHA1:	6F418700355F89557623BAA38713103E5D2E9014
SHA-256:	83C96C0A94A7EA0823AD6A81AF7B28251645D81B299881B21C4B098A5E546212
SHA-512:	263EC1460C5C5E48C19E297D5FA981ECAE386F75B31214D507C4E13932C11A1F86E63893B6ABB535F7FF440672126F105049769F19991F4E079671C3ED8AC96B
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1615569893.054439,"host":"yjc2lUdW14pVMogZeveQt+31M9j2pW5MsV83ny8rR7A=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1610385893.054448},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1641921887.933609,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\567755ea-cea5-434f-a851-0393fd22db3d.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\622a3b26-1abe-48e8-98a9-fb89dc454063.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):	22619
Entropy (8bit):	5.536178318794515
Encrypted:	false
SSDEEP:	384:rfjtPLlukXb1kXqKf/pUZNCgVLH2HfD6rUNHG0nZfXOIf4j6:NLlZb1kXqKf/pUZNCgVLH2Hf2rUxG0nt
MD5:	A4B655D1330D534DD6DCEDCF863903FC
SHA1:	408A4379F81D008DB293EEA9D7FF845BC047A45F
SHA-256:	BB36D63C0650D47CEF25E8F2F28BDBC963A5F394690A253FE71708DCD90D2CB6
SHA-512:	9E62CB30766F60544AE8378F3134DD20953FFA724BD5D83089EA9AC6EBB52F993982B52E0849E0440597570EC9410D3C72D4B1D2D1DD4B1BFD77E4575BBFB3E
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":"13254859484880717","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\8094fd3b-1e9f-4611-9b30-75951e8efbf1.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):	5653
Entropy (8bit):	5.152348288810193
Encrypted:	false
SSDEEP:	96:nKvOal4lP087aIVe5k0JCKL8nIku1HubOTlVuHn:nKvZl4lcoaI8h4K+Iku5S
MD5:	9C46BAF42DB4C2EEA969D3CB6C42BB51
SHA1:	1E98EF37D5225A014C22963A09A1554BCA51806D
SHA-256:	E510C4B1B666DF1A4221DE8E5DDC1EA17B7B66E382CB04FE2A3B2AB3F7BD33D4
SHA-512:	75FAE6A8E80527115F32646AB6C3E0AA0E11C79BFDA00F257DFCD29BA86575FD2F28CA83592B116DFB6D81C99AF39EC3DDEE74207561BD34B176CDC7E0ED7 53
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13254859485144023","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\980df6bf-ad0c-4bba-ac80-d43fc3ae9278.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\980df6bf-ad0c-4bba-ac80-d43fc3ae9278.tmp	
Category:	dropped
Size (bytes):	5056
Entropy (8bit):	4.958112899049432
Encrypted:	false
SSDEEP:	96:nKv9t4pIVe5k0JCKL8nIku1HubOTlVuHn:nKvv4pI8h4K+Iku5S
MD5:	131ADEE7456D4C6404B9CED9447A40BE
SHA1:	65F81209F34973618355B19B35E49EB58F2230EE
SHA-256:	298CD736F6890D5EA11A21FE4FC5E74D76BE6A31A258538AA1C8423A538A5414
SHA-512:	82C8B1B50A36D9576C9C76676EC06ABB9F548FF040347368C7754017D072399181432C9B60B222F3A1FEA2411764BA1C611BB500034D45D5AE77DD52DA13988E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13254859485144023","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

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):	5.2139855717949946
Encrypted:	false
SSDEEP:	6:ms3+q2Pwkn23iKKdK9RXXTZIFUtpYjXZmwPYEVVkwOwkn23iKKdK9RXX5LJ:5+vYf5Kk7XT2FUtpe/PjV5Jf5Kk7XVJ
MD5:	A70418EFBC19A94A494FA83F14F0A542
SHA1:	5BB1BBD6E16B0322D2E2F5B542473D11036725B8
SHA-256:	82F9FCDD4DBEC7651FE40DDFA6C60F0D9CD32E547EFEAC99C9067142A7DFE2B8
SHA-512:	4596C3AD0AF9464925ED68DE2312027FA363476C5AC12BCBCB6151574B262A8D4C1CFE276D43311ED1C65CC0C00B8736AD9C871310CD28730BE0BADAD9AB1/ 39
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:57.960 127c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/01/11-18:24:58.012 127c Recovering log #3.2021/01/11-18:24:58.028 127c 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):	5.230718435594493
Encrypted:	false
SSDEEP:	6:mS/N+q2Pwkn23iKKdKyDZIFUtp3UXPZZmwPqVkwOwkn23iKKdKyJLJ:v+vYf5Kk02FUtp3U/Z/PqV5Jf5KkWJ
MD5:	1B6983A36856EC2F61F910B8B4C45D3B
SHA1:	FC6AA9756E6307EC04CAF83F7FADA1EACDA97680
SHA-256:	617E33DC3A48DE1492DE8A20BCC366506B84AB072ED4330832698CFDA7875EC4
SHA-512:	A0BAFA5A7E8EC2EAE1D7D139B741A6257EB42379CEFF6F73CA3A517FFE6C48AFEB649C3AE5AF3C9209FD2CF40372AC85D6EE520FA4DD05B05268DA1047769 4A
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:57.944 127c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/01/11-18:24:57.949 127c Recovering log #3.2021/01/11-18:24:57.950 127c 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):	1.2940260784530149
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7U1yBPGfrs/sWfvoNYsTO:dNwSOfrBNl6
MD5:	BC77CAE3D57C46ECD36A522A9F2D1686

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
SHA1:	8B197406B809CB37710C55764FADF8A35C1BED9B
SHA-256:	A2D88EEFB62CBE6E2C5206AC91C50521076B122163519AB87BB2F81CE2FBEF09
SHA-512:	8D93D6A04F2F62438D86274B1A592A24A29B5BE272C96B56506B8B399254BAA4BE10BCDD5CABD860ADF509FF4276C28A7E460B2423DFE166AD05EBC79F184D C
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):	0.9729604620376362
Encrypted:	false
SSDEEP:	24:9e9H6pf1H1oNsyqLbJLbXaFpEO5bNmISHn06Uw/8:9bfvoNvq5LLOpEO5J/Kn7Us8
MD5:	1ADBABFC8336359E3B9A17DA71DA9D88
SHA1:	2C29D8486D4C5EF43632FAC937352ED95173677F
SHA-256:	D0D1252DC9E5B2875059F0DFE8550AD784A3DD84C1094AB581C6BF73A15DC805
SHA-512:	2CFF8B3D15ADFC330AEC15B2E9D0380EF7EA5FAF286A478BC0C2589421777B7BC4FAA5E49090E0A2AB232D765253896009FEB9DF9AB264E0B847E9041C78227 3
Malicious:	false
Reputation:	low
Preview:	.....0.0..... ....

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):	1468
Entropy (8bit):	4.1901433740149905
Encrypted:	false
SSDEEP:	24:34Su+CgQlrlJXl7JaGI66gTj0mJRE8mlSetOtNKJaGI66gVlr:34N4wxT1a/6bkmJR1mlSetawa/6bPr
MD5:	1D0F7287D283AF2D40CAD226964822F2
SHA1:	AB8EE3AB1C68815692172C8CE79D92FF6D2355A8
SHA-256:	62A45EB807FE54674E6EA5C0C717EEB7CA3592B45E2952EEC2539420BE66D961
SHA-512:	5D4F83BF6381D3972579843248B29FBDA644770AF7F6612FB3C9F8E905C790532563DFF93970B10D0E089BC2BAEEFFB87BD653F639CFB48A5DF1AF06D27E9AA2
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...9a294d96_5e84_4d0d_9324_adb6162dada7.....`..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....1.,.....https://www.notion.so/WORKSPACE-c062f3c 6adef4fadbb3f459b4fa0d6df__;!!MdZ9-hZ0wg!a90_1yAqw74SgGAA7kXe4i93XCrFfwMkTpLPFrZ0ywOoEHviqXU3ETw0IwinDLX_gcs$%20%3E(s)..... .....h.....`...../.....D.....h.t.t.p.s.:././.w.w.w...n.o.t.i.o.n...s.o./.W.O.R.K.S.P.A.C.E.-.c.0.6.2.f.3.c.6 .a.d.e.f.4.f.a.d.b.b.3.f.4.5.9.b.4.f.a.0.d.6.d.f._._;.!.!.M.d.Z.9.-.h.Z.0.w.g.!.a.9.0._.1.y.A.q.w.7.4.S.g.G.A.A.7.k.X.e.4.i.9.3.X.C.r.F.f.w.M.k.T.p.L.P.F.r.Z.0.y.w.O.o.E.H.v.i.q.X .U.3.E.T.w.0.I.w.i.n.D.L.X._.g

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

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.196646842647682
Encrypted:	false
SSDEEP:	6:mFU0uTSVq2Pwkn23iKKdK8aPrqIFUtpcUiOgZmwPcUiOIkwOwkn23iKKdK8amLJ:WuTSVvYf5KkL3FUtpJg/PJI5Jf5KkQJ
MD5:	BFFA36CD10F7AB24EF5FC4AEDD0577C9
SHA1:	6E74FE32F0950ADC3CFDF06C4D0F447A3736E448
SHA-256:	0A979CCBF87ADE9C3A3A8A26789CD945619C576A98C65048B627099BCB5E134A
SHA-512:	737707594172211A36D966A77072B736EC450F7C88FA40199C7CF709CE1AB682C381C19971D13B1E3F9E1619172421E763886692B15957015229751B3870F247
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:45.147 16d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/01/11-18:24:45.148 16d4 Recovering log #3.2021/01/11-18:24:45.148 16d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.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):	5.203804636570973
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
SSDEEP:	6:m/E9+q2Pwkn23iKKdK8NIFUtpinnNJZmwPiW9VkwOwkn23iKKdK8+eLJ:SE4vYf5KkpFUtpinNJ/PiWD5Jf5KkqJ
MD5:	D81A51E7F2E28F951D3E0AFB73378E31
SHA1:	E19ED000076EBBF73277968F0B59256C26B879AB
SHA-256:	7C08C8BC5470D936236C46B4BC1EA9FD1200F6D6ACBB0636006955DDB0475C70
SHA-512:	12F6A34407F81F38B36B9687518D4F71A514989817FB6994A2D65538EC1CCA5555C07A3C8B200B1F61875ED504964B36BE65A1A3BF4B2C8FF47EF3D383118465
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:47.175 17b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/01/11-18:24:47.176 17b8 Recovering log #3.2021/01/11-18:24:47.177 17b8 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\1.0.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49IC
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2l/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9l/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.255739945432129
Encrypted:	false
SSDEEP:	6:mSF+q2Pwkn23iKKdK25+Xqx8chI+IFUtpuYBZmwPfFVkwOwkn23iKKdK25+Xqx8E:f+vYf5KkTXfchI3FUtpue/PfFV5Jf5KN
MD5:	9E386FE79C3CB99CD27D4D55204C48C7
SHA1:	2FF9E37A62370DDC32E910F04B370C4A68CD4DB5
SHA-256:	CDC87197EFBF156D93CE8E3BADF6A91A792B9A7E0D2BF0161601C2D3300BC4F3
SHA-512:	495EFCBD25E42A71DEC6FDAF946C20FF86A3B25BA91B513FBBA1707108AA9E1D29E2D741484B59B13F68A940D71B26CCA246EA31186A7B779F855EFE911C384 5
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:57.908 127c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/01/11-18:24:57.915 127c Recovering log #3.2021/01/11-18:24:57.920 127c 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):	5.201476565730596
Encrypted:	false
SSDEEP:	6:mDF+q2Pwkn23iKKdK25+XuoIFUtp+SSZZmwP9CiVkwOwkn23iKKdK25+XuxWLJ:M+vYf5KkTXYFUtptm/P9CiV5Jf5KkTXp
MD5:	11D5C06B4957E4A5829F98658E90C824
SHA1:	1258F1350B25134984DFF668F8995E4C8BFE7D44
SHA-256:	1848AB421AFBB681A91BF2B071E00F647A43D7D639D42F740C3E5668CBAC709C
SHA-512:	EC3D1ED4C3019CC0268E9B3DF1AD83EB7D2C0082C89DBB63DC30976536D2A3C2AC0443E2D3C671C115D605B161496E849C77D628A78ADE7ACC715A130BA54 AB
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:57.880 127c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST- 000001.2021/01/11-18:24:57.884 127c Recovering log #3.2021/01/11-18:24:57.885 127c 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):	5.226900961592747
Encrypted:	false
SSDEEP:	6:mE4Iq2Pwkn23iKKdKWT5g1IdqIFUtpIZZmwP7kwOwkn23iKKdKWT5g1I3ULJ:JvYf5Kkg5gSRFUtpIZ/P75Jf5Kkg5gSu
MD5:	4BE88FC0390F61046C79F27274A62352
SHA1:	0E96BA88E54E8F2BA68C46A961B9973346AAE35F
SHA-256:	8B42F403535E0634F9E9EDF56046975C4D3E9F5A9E90E50942BCAA0CB5D2B5D6
SHA-512:	3247E8F9C9D8A95D5DB694CC5C05ACC39155B7D5EE2128044AB3B2ABCC7E18FFC7FB3923C33D6331E33EC1D1F0F56DD7290C33E64E7B44D88BB2FCAC80BF4 1D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Preview:	2021/01/11-18:24:57.700 1ad0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/01/11-18:24:57.797 1ad0 Recovering log #3.2021/01/11-18:24:57.798 1ad0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.480937603247322
Encrypted:	false
SSDEEP:	48:cwGxxRTa7oMg8dbvQgvbQSefgG3NrS0U9RdiN9Cxn:+a7oMbdbvQgvbQ5fgG9rS0i
MD5:	D049C778AA40049D794A33FA7EB57ABA
SHA1:	6AB3C0D912F141B9BDC1BF5A1F71BA59A3EA1740
SHA-256:	C09CB151D0227A29A359B4D26CD432C84296F560F574FFB2D2A84F2797E4D2BD
SHA-512:	57D21C8A6455A1237BE133B11B117645B68F2011A1E79665EFFE3B88AF7A373699A97F1B103402EA37E45288E02CEF4B1E2323B819BF2222FC7C89151B3F7B0A
Malicious:	false
Reputation:	low
Preview:	.(E....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..482346000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-01-11 18:24:59.71][INFO][mr.Init] MR instance ID: b4357a74-9b03-4923-9cb4-81cee1390653\n","[2021-01-11 18:24:59.71][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-01-11 18:24:59.71][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-01-11 18:24:59.71][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-01-11 18:24:59.71][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-01-11 18:24:59.72][INFO][mr.CastProvider] Query enabled: true\n","[2021-01-11 18:24:59.72][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.197927696578464
Encrypted:	false
SSDEEP:	6:mUGjIq2Pwkn23iKKdK8a2jMGIFUtpWZmwPjzkwOwkn23iKKdK8a2jMmLJ:NzvYf5Kk8EFUtpW/Pjz5Jf5Kk8bJ
MD5:	800E517167B4A229378D6762A4DF15B4
SHA1:	B76D8C3255F82F99918F2952530F0916B9CD99E7
SHA-256:	A1C58B29CFDF6CD3BBB37C650C75144197839753D107FF850BD81977F758BF5F
SHA-512:	DABDC8A4C85379179BF502AD91F6899E0B3609C5EDDF980EDD482CC98ADAC3AE13832B2AE286BBAD418D399E67606FC32CE514C0819044D09E05DF2B3A3266B
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:44.936 17c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/01/11-18:24:44.938 17c4 Recovering log #3.2021/01/11-18:24:44.939 17c4 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.214164664312957
Encrypted:	false
SSDEEP:	6:mFUqn39+q2Pwkn23iKKdKgXz4rRIFUtpcUdJZmwPcUj9VkwOwkn23iKKdKgXz4qG:W34vYf5KkgXiuFUtpDJ/P9D5Jf5KkgXS
MD5:	C296315FBF9160BBEC5548612729360A
SHA1:	651CD43648A71DF53FA1FFBAF797949B811945A2
SHA-256:	7A8B06AF7493F9C9D4BA39CFC80CEE00CCE9BDBB72268863B40AEF2926FD7EE6
SHA-512:	EABA1D18B8E0C76EB788072E4695949CC2869F843990DE5FACF4A6AB35CC5F941841B58190390DF1E5CBA9C2E667988ABC0FE694B54FC77DCC46F2ADA4829BD
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:45.178 17b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/01/11-18:24:45.180 17b8 Recovering log #3.2021/01/11-18:24:45.182 17b8 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\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.175580608314841
Encrypted:	false
SSDEEP:	6:mFlVq2Pwkn23iKKdKrQMxIFUtpc6FKB0gZmwPcUGOIkwOwkn23iKKdKrQMFLJ:QVvYf5KkCFUtpA0g/PdI5Jf5KktJ
MD5:	BBB01751EB9CA10DFBCF7FA05A89317D
SHA1:	742B1DCD1031AB94A340AA9A66D6C9D8176156F4
SHA-256:	ADF5A590F148F46DCA2F1F1ED9919ECECF398F7A5C69777BFF40A4849B70F3EF
SHA-512:	F1483F54C357DC3EF1349A3F61BAB2CAC496784AF28DA022DECFB7FF66BAF2A56AE102CAFBA5B9AA6C8A6C060A33A0B59E825A4069A238D62D39C7AF6648F9B2
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:45.097 16d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/01/11-18:24:45.098 16d4 Recovering log #3.2021/01/11-18:24:45.100 16d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.155337213446722
Encrypted:	false
SSDEEP:	6:mfpM+q2Pwkn23iKKdK7Uh2ghZIFUtpQNZmwPpqMVkwOwkn23iKKdK7Uh2gnLJ:H+vYf5KkIhHh2FUtpQN/PJV5Jf5KkIh9
MD5:	C828BBC28CBCA26B9DBE7D4A9EDA90BE
SHA1:	BC67178B56813AE99BCD7662155592021BEAA26A
SHA-256:	F7BC4B97796E7104827D00933ABCB5D2EACED552DBAFEBB58A01D048275B2160
SHA-512:	30D61F46BAFE21185D019C534C6F31F57DAFC827CA4CF8C87F57EE0E5FDDCC740D1D995179C3CBB47D641A477AAA2903C60BBD72313B9E39C4358922DA12D39
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:44.866 171c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/01/11-18:24:44.867 171c Recovering log #3.2021/01/11-18:24:44.868 171c 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\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
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):	5.247475955260791
Encrypted:	false
SSDEEP:	6:mFUeVq2Pwkn23iKKdKusNpV/2jMGIFUtpcUsSgZmwPcUsSIkwOwkn23iKKdKusNA:oVvYf5KkFFUtpRg/PRI5Jf5KkOJ
MD5:	AF768366BE1A392424232AD69184332D
SHA1:	68C63F7138EE32AD6B240587948C5A2B8DC05A4F
SHA-256:	1D5FD4ECF1A77CD0AA24EB2E2C8DFA5D1A8CE5D292364FBCA0D12F17AE3BC617
SHA-512:	03E82B3BD4CECA1A3611A5E0EAD8A346080EFFE7D8265F2760B2704BC4EE75F178FCF13ECD950D2E3317730990EA55C44C6EC81CDEB31680F9D9EA04FBD821 1E
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:45.134 16d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/01/11-18:24:45.135 16d4 Recovering log #3.2021/01/11-18:24:45.135 16d4 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.290268989543254
Encrypted:	false
SSDEEP:	6:mFUda+q2Pwkn23iKKdKusNpqz4rRIFUtpcU2ZmwPcUUFq39VkwOwkn23iKKdKusX:HvYf5KkmiuFUtp0/P2aD5Jf5Kkm2J
MD5:	49C592F9A7F572779227D9EDD930041B
SHA1:	D8F0AFCCC7832D39B06721A891AFBCB9421C20BD
SHA-256:	F3F2C8F0CB8959ABBB5A72F95C7F3A17B0FC0CBC2212F9D2D89720AA4534C4BA
SHA-512:	2A0FA42468D79BC03DDCF1251AF19BE0CBA3FF014FFFBA2607FE0AFCE9E492CD1DFE81BFE3408CDD17F27580EEF366B5E4775A95E6D485823416AB91CBC3B 0A
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:45.179 b78 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/01/11-18:24:45.182 b78 Recovering log #3.2021/01/11-18:24:45.183 b78 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Size (bytes):	418
Entropy (8bit):	5.207023303305375
Encrypted:	false
SSDEEP:	6:mV9+q2Pwkn23iKKdKusNpZQMxIFUtpoIVE2WZmwP8S39VkwOwkn23iKKdKusNpZb:09+vYf5KkMFUtpf+J/PV39V5Jf5KkTJ
MD5:	23CBB59FA645D660D626AD2E660495C4
SHA1:	4D778A9523EDED425AC7E1D1A8995BE3930E506D
SHA-256:	5489A0A8671004F880651A6023888E434ECFA3F2F389EB5394F5AEBDD8934D13
SHA-512:	F31D5C85C67470D3E46C0087D6186D36383AD2BA20FAE05F74FB0696D80A465A6BBD6CFE9CEC386C659757A2A4698F395995F9E35BF2EE3B3ADD8DDEC681083
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:25:01.849 140c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/01/11-18:25:01.850 140c Recovering log #3.2021/01/11-18:25:01.851 140c 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\b6ba2ac4-6d70-4f63-ac01-9968f3bdc2c2.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):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\8a246231-56bb-40de-bdb2-4d71ba0987c8.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):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.223582633249853
Encrypted:	false
SSDEEP:	12:w+vYf5KkkGHArBFUtpRKW/PaV5Jf5KkkGHAryJ:ZYf5KkkGgPg2ZJf5KkkGga
MD5:	B0A94D7797394117910825FB66C82B64
SHA1:	F4200A85D6D125528BC9A7B629BAB08D1172FBED
SHA-256:	3C67FBA9251B875B9C49F4B472D0CE642716623CBD3201EF3C6847FDC7855DAB
SHA-512:	E4B3C41C6B77D22CC665E0A58B41E0F12769A7643DD5263E24EC6CD213C1350DE7AF17EBF8CBF1B4F7E93ACABA65E32B396796940F13FDA8672882A491019BE 5
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:57.979 175c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/01/11-18:24:57.981 175c Recovering log #3.2021/01/11-18:24:57.982 175c Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.239734207751449
Encrypted:	false
SSDEEP:	12:fIvYf5KkkGHArqiuFUtpO/PN5Jf5KkkGHArq2J:f6Yf5KkkGgCgwJf5KkkGg7
MD5:	280A8F897845AFF6F8700A5EF3B90474
SHA1:	941A6671B9A757BC8FBDA6ED5CE1FD9E6CC84EE1
SHA-256:	F2C34BACE59AA5A8A43ECCCBF6815788CEB37A8421ED240C1E9B920455FE8B1C
SHA-512:	CB00F90D2A0B3925EACF428A8BDCF65A9C28AF10BC53D603C0A7996C0EA8C51838FFA37889E70E97C9E94038DF26B477E2251B7A3FD0DC3234E01926B219173
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:57.979 17c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/01/11-18:24:57.981 17c4 Recovering log #3.2021/01/11-18:24:57.982 17c4 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Entropy (8bit):	5.153654049320909
Encrypted:	false
SSDEEP:	12:ep9+vYf5KkkGHArAFUtpuQF3J/PuQF39V5Jf5KkkGHArfJ:cKYf5KkkGgkg/F37F3VJf5KkkGgV
MD5:	DDAFE56FC703B2887B964EE33680D025
SHA1:	BD4FDABC439D0136F5DBB61FA10752F646A2B15F
SHA-256:	9278ED81A59F99940AA0220DF4C516F967946E1CC4120FD7032F7D987CAE392D
SHA-512:	1429AF7EB5328C3D9B4D167F62952CCDEBD2C5F2AA9282A246AE425030A7564E9D72F7F5E967287E7E742D32851A04D4957B2E07E7F6CCDBE821C4DAB1F4B2A7
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:25:13.260 140c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/01/11-18:25:13.261 140c Recovering log #3.2021/01/11-18:25:13.261 140c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.207283893399994
Encrypted:	false
SSDEEP:	6:m3pM+q2Pwkn23iKKdKpIFUtp1ZmwPgeMVkwOwkn23iKKdKa/WLJ:T+vYf5KkmFUtp1/PAV5Jf5KkaUJ
MD5:	EEBA00C03AB0EB6E349C0FBBDDDFDCAB
SHA1:	379E431A937A49713B57F2836D9582B6E07B7AAB
SHA-256:	1C96297B6D691A10B5AA65F2558C1FE96001B6257441CA4012D1E8182EFDED32
SHA-512:	CFA73EA0143A6E766ECB7BEA591120BB5F7A4FAF05E98999656C6EA16375E25877B188C221E7E837F77D4DCDFA6B78CDE79A20C12FA55F50782645D9337D8F7
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:44.905 171c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/01/11-18:24:44.907 171c Recovering log #3.2021/01/11-18:24:44.908 171c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.324660407366461
Encrypted:	false
SSDEEP:	12:rz9+vYf5KkkOrsFUtp7UJ/P7B9V5Jf5KkkOrzJ:rzKYf5Kk+ghUNBVJf5Kkn
MD5:	7B5ECD7F626F51234BFA664FE6616CE2
SHA1:	F0403E4750E1A298FABC02BD9A592300761923F1
SHA-256:	9B1CDF8B6AD92D7DEDA76DF0C62BC4679A7897AC0619C4411D607563C4CA1C23
SHA-512:	641D24FBBC4CCCA6832F8C9795E4AF633F0D277848B18F992D533D21358105E78E52ED53943D326F323971AA5124A70F48491C297C12025E559CD338A5B5B33D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Preview:	2021/01/11-18:24:59.736 140c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/01/11-18:24:59.737 140c Recovering log #3.2021/01/11-18:24:59.738 140c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.543027170378416
Encrypted:	false
SSDEEP:	3:tUK/9zFmWZmwv3J9aFUovvR1V8sJ9aFUovvR1WGv:mGFZZmwPqFLv7VvqFLv7tv
MD5:	29715ADC383FED619E4A464A8D85AE9E
SHA1:	4F4B546DD42B81AF3A3FC5FE7820E5E72A4D9084
SHA-256:	B590DB7AE7DD67D21B1371E16B4E556D46F35FA2E730090E309A2031FDF98FB7
SHA-512:	52FFC2DB5B67A217CA207C479C5F6730956FD8193942138F7C474FB469BBF17C8D3935BDE20DB0AF1B04BFF19488973D032D33AA811D2C993A38F48C0AD9195
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:57.190 1ad0 Recovering log #3.2021/01/11-18:24:57.335 1ad0 Delete type=0 #3.2021/01/11-18:24:57.335 1ad0 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e51f4bae-b35f-43ca-9e87-b6227ced9453.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	22620
Entropy (8bit):	5.536188078355338
Encrypted:	false
SSDEEP:	384:rfjtPLlukXb1kXqKf/pUZNCgVLH2HfD6rUNHGpnZfXOGf4e:NLlZb1kXqKf/pUZNCgVLH2Hf2rUxGpnT
MD5:	2E7A2386DF59BC968C10217559931262

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e51f4bae-b35f-43ca-9e87-b6227ced9453.tmp	
SHA1:	FB5DDC85B5249AAEF41E2105F0009E27FA1505B9
SHA-256:	2E0104E2BF815205531B768E6A2E7688A5CD17578494796A6C6EA041142C7EC9
SHA-512:	98C46135DB037BF17E08E0BC0B70A6A1E774A1882E620CF42BA24CFB784B1CA172FD3847129501106DC67F0FEF2A770C3A1EE367A7B411746C452A079B51708E
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":"13254859484880717","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f61f8358-5809-4cee-bad7-8aa042aaf5e3.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):	16763
Entropy (8bit):	5.578214809550983
Encrypted:	false
SSDEEP:	384:rfjtyLlukXb1kXqKf/pUZNCgVLH2HfD6rUlXOCf4b:wLlZb1kXqKf/pUZNCgVLH2Hf2rUZfQ
MD5:	7C5E27D49D563986041EFC42F9D8B02C
SHA1:	6DB605FC9354D93605D88153AE6567EC73511D4F
SHA-256:	E9542B7703A245FFFFF69085E9378E9732D822E748D49473A34F7EB74C647A27
SHA-512:	0C9C8AB36998163592DA561E6F4ADC855E9914D7AD18E0B21AA0BE33C9CC0AB34BAD307D8056E55C79F3F7412425F6B33B6495268215ED8F22AF7C096D32898
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":"13254859484880717","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	5.246988446178435
Encrypted:	false
SSDEEP:	6:m3LdL+q2Pwkn23iKKdKfrzAdIFUtpYxoKWZmwPYJS+LVkwOwkn23iKKdKfrzILJ:M+vYf5Kk9FUtp2oKW/PaSiV5Jf5Kk2J
MD5:	7D233B9A0F843B0F8832ADA163C4EAE4
SHA1:	5620A3C419EA1EE02388EB3813920120218139EB
SHA-256:	82D30C38ADED2324FA4D11083EFBB58F91222EE02848C6308BD9E2DDC0195E43
SHA-512:	B477422F2A32F673B23F5C3BA15BF9419EA9FBB05D83B8E7EF7FD2B1D82FCED0961F5E485B2E1F8937ADAA20FD378F6EFEA4408F40C99CB62D92F2F61297CC1A
Malicious:	false
Reputation:	low
Preview:	2021/01/11-18:24:58.095 175c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/01/11-18:24:58.096 175c Recovering log #3.2021/01/11-18:24:58.097 175c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Temp\19e53796-a8ad-472d-9b57-b2eb0c450f21.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\254d2d20-9432-4c35-8737-0876bb060551.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	300953
Entropy (8bit):	7.973503294353402
Encrypted:	false
SSDEEP:	6144:0sb1v/4nxPbqqBbWbFsw+wh3bC5NFv++S/hup0XcaxlnJ9:7l/4nxPZbOFsw+y3d+S6WnX
MD5:	1FE8E0AEB768437A23CEEAE6053E5822
SHA1:	5529A275644B729009E22035F6125879450F4ABB
SHA-256:	25A2F515CEC98CF2ACF11B34C59723D76820A4B5734E223D7EBEA55E5A851468
SHA-512:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA5681232O
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.....L.18..Y.~..%...~._.....O\..p,...eY.0=.!..+.SoZA7...:t.G...VZ<..d....MN.....T..{1\.T...P,...i...NrD...e.2..u....5.....1.n.Zu.E...!..XR..j.:.E.gUw.-s7:T.c_...(.i..iU.).M=yF<..`.....F...@)..IK.. b.4.o..mC'...N.*@OtT...`.&|.8.M;.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.l)N.|b.l....{.K@]6.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....RI.G.,2.....[..T'....."ct.).s#.(/.D..C..4..RKf.W....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...H0F.!...L..\.j.1.d.....==v.....-

C:\Users\user\AppData\Local\Temp\412f23cd-3026-489b-ab68-6e13762141ae.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**

C:\Users\user\AppData\Local\Temp\412f23cd-3026-489b-ab68-6e13762141ae.tmp	
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.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\78ee64ed-de72-4c1e-9f43-cef3bd18735d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\412f23cd-3026-489b-ab68-6e13762141ae.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.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\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

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\am\messages.json

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_dir7064_1931342275\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_dir7064_1931342275\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:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA 2
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_dir7064_1931342275\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:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4 C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\bn\messages.json	
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_dir7064_1931342275\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:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE 1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522 140683318860351": {.. "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_dir7064_1931342275\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\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

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\da\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": "Fryser".. },.. "12139579827238759 20": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "12827687646031907 5": {.. "message": "Enhedsregistrering".. },.. "14284488690781267 31": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "15509040647108289 58": {.. "message": "Problemfri".. },.. "16366867476874943 76": {.. "message": "Perfekt".. },.. "18027627465894571 77": {.. "message": "Lydstyrke".. },.. "18503975003120203 88": {.. "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_dir7064_1931342275\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:	{.. "10189845614885205 17": {.. "message": "H.ngenbleiben".. },.. "12139579827238759 20": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "12827687646031907 5": {.. "message": "Ger.teerkennung".. },.. "14284488690781267 31": {.. "message": "Videowiedergabequalit.t".. },.. "15221406833188603 51": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "15509040647108289 58": {.. "message": "St.rungsfrei".. },.. "16366867476874943 76": {.. "message": "Perfekt".. },.. "18027627465894571 77": {.. "message": "Lautst.rke".. },.. "18503975003120203 88": {.. "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_dir7064_1931342275\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C013
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": "..... ....".. },.. "18503975003120203 88": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\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

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\en\messages.json	
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_dir7064_1931342275\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_dir7064_1931342275\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB11202723566
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "1522140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\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

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\fa\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": ".... .... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\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:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A5261952050321
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "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_dir7064_1931342275\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C000
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-smooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "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_dir7064_1931342275\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:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\fr\messages.json	
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".. },.. "1636866747687494376": {.. "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_dir7064_1931342275\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": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636866747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636868747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\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".. },.. "1522140683318860351": {.. "message": "Povezivanje nije uspjelo. Poku.ajte ponovo.".. },.. "1550904064710828958": {.. "message": "Glatko".. },.. "1636868747687494376": {.. "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_dir7064_1931342275\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":

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15070
Entropy (8bit):	5.190057470347349
Encrypted:	false
SSDEEP:	192:GsprMtChjkWfrEWL0KRCnEOWV6c8TEKdl:9rtAEr3LTRuWV6uml
MD5:	7ADF9F2048944821F93879336EB61A78
SHA1:	C3DA74FB544684D5B250767BB0CB66FFB7C58963
SHA-256:	3630947E1075E3663AD3E4824D0BE42CB47C0D615D8053E83B9595047C8BA9BE
SHA-512:	1F28BB80E1839C5581106BEA3AE2501C7618249D7E3115819F5A9A87771D59F5DE346C1B9C87F7FFC390604D5B9888CE738E25F2F04A094002A0FB3B22CBEC95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Membeku".. },.. "1213957982723875920": {.. "message": "Dari berikut ini, manakah yang paling mendeskripsikan jaringan Anda?".. },.. "128276876460319075": {.. "message": "Penemuan Perangkat".. },.. "1428448869078126731": {.. "message": "Kelancaran Video".. },.. "1522140683318860351": {.. "message": "Sambungan gagal. Coba lagi.".. },.. "1550904064710828958": {.. "message": "Lancar".. },.. "1636686747687494376": {.. "message": "Sempurna".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Bisakah Anda melihat Chromecast di $START_LINK$aplikasi Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15256
Entropy (8bit):	5.210663765771143
Encrypted:	false
SSDEEP:	192:lYprk52dAaykVza8rE0QWBKD9+vq0hKEV6c8TEKdl:qrlA8r6DalV6uml
MD5:	BB3041A2B485B900F623E57459AE698A
SHA1:	502F5EA89F9FB0287E864B240EA39889D72053A4
SHA-256:	025737EF8FA06706B3F26D0F52B4844244A6D33DAE1D82FEF2931A14C003D57E
SHA-512:	BA51784073BEF82F3A116B33DA406FDB10EC823B9EE74375C46036DAD8BDCB4141F60845DE141ABE42CEEF9251572F6AB287CA5FC7669C60E4F68071D5AB8CD
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Si blocca".. },.. "1213957982723875920": {.. "message": "Quale delle seguenti definizioni descrive meglio la tua rete?".. },.. "128276876460319075": {.. "message": "Rilevamento dispositivi".. },.. "1428448869078126731": {.. "message": "Uniformit. video".. },.. "1522140683318860351": {.. "message": "Connessione non riuscita. Riprova.".. },.. "1550904064710828958": {.. "message": "Fluido".. },.. "1636686747687494376": {.. "message": "Perfetta".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Riesci a vedere il tuo dispositivo Chromecast nell'$START_LINK$app Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\ja\messages.json	
Category:	dropped
Size (bytes):	16519
Entropy (8bit):	5.675556017051063
Encrypted:	false
SSDEEP:	192:nkprPhQdxkRWrZe1wYpMR5wnAV6c8TEKdl:YrLRWri65wAV6uml
MD5:	6F2CC1A6B258DF45F519BA24149FABDC
SHA1:	8A58C7880C6D22765DCBB6BCE22A192C1B109AE1
SHA-256:	42ECFEE727CFC4F2845FEFDACE5EDC2E0A40AFAD69973A3B950CE653A7633342
SHA-512:	F7454F0E14301C59CC54361ACC0A1C6D072EF9BDF5DEA60646FB90B1CE47612785938C784A4CF1DE3E62648A14420374933B5F5DA43907BC00D3799FF163A3D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..".. },.. "1213957982723875920": {.. "message": "..".. },.. "128276876460319075": {.. "message": "..".. },.. "1428448869078126731": {.. "message": "..".. },.. "1522140683318860351": {.. "message": "..".. },.. "15509040 64710828958": {.. "message": "..".. },.. "1636686747687494376": {.. "message": "..".. },.. "1802762746589457177": {.. "message": "..".. },.. "18503975 00312020388": {.. "message": "$START_LINK$Google Home ...END_LINK. Chromecast .....$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_ LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\kn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20406
Entropy (8bit):	5.312117131662377
Encrypted:	false
SSDEEP:	384:a6C5rBSzvrZreGnla9ZBHRUDYr9yRwEcAa4rSeD5BSz0hJz8qbbM3gbr//Hkr44c:a6C5rBSzvFreGnla9ZBHRUDYr9yRwEcC
MD5:	2E3239FC277287810BC88D93A6691B09
SHA1:	FC5D585DA00ADC90BF79109C7377BD55E6653569
SHA-256:	5FC705AD19761204D8604EA069936A23731B055D51E7836CAAF16AC7719FBEEA
SHA-512:	DF8BC9E577D3ECB0E6C303E1D2C9E9A4A8317CAE810A9DFC88D91B373A4B665722C5A9AB5A589BB947FDA4C7CD9A6DF39DDD13EA47FE9EFF7E0AC43E49FF 3479
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..... .....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "1 28276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "180276274658 9457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... $

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	15480
Entropy (8bit):	5.617756574352461
Encrypted:	false
SSDEEP:	192:kWprGvSQtkxWffrnl5JuFBWVZV6c8TEKdl:TrkuxKfrlT4YVZV6uml
MD5:	E303CD63AD00EB3154431DED78E871C4
SHA1:	3B1E5B8E2CF5EBDF5D33656EF80A46563F751783
SHA-256:	FDE602BFDB1AFD282682DA5338C4F91D8A2F6CB5411DB8F62F4583D629CE67A6
SHA-512:	18BA1D5A25FBC1829AD957A531B0CC490AFCBD20AC22181021363AA3CFB916270B8732E824463C9B0897220E8AE86EB1BE561D6540E6C625F08F228F61DDFFA
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..".. },.. "1213957982723875920": {.. "message": ".. . .. .?".. },.. "128276876460319075": {.. "message": ".. ..".. },.. "1428448869078126731": {.. "message": "... ..".. },.. "1522140683318860351": {.. "message": ".... ....".. },.. "155090406471082 8958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "...".. },.. "1802762746589457177": {.. "message": "..".. },.. "1850397500312020 388": {.. "message": "$START_LINK$Google Home .END_LINK. Chromecast. .....? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15802
Entropy (8bit):	5.354550839818046
Encrypted:	false
SSDEEP:	192:lGxSprfkiRR+2zJckS1khrnPI85+80p3DWReV6c8TEKdl:lG4rlq0OkSmhrwbpIeV6uml
MD5:	93BBBE82F024FBCB7FB18E203F253429

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\lt\messages.json	
SHA1:	83F4D80F64FA2ADCE6C515C5F663BD38A76C51DB
SHA-256:	E7A8570922CCC4F2CA3721C4E61F426158C4E7BC90274FBC8BE4040FF8B6CA9B
SHA-512:	B7E7878106B466CE95069141DF1DE387E847348B62E9C4D548006452F3E164B3AD842E9673A56DC011A5ECC3346B5863E2034EE477A9D1F3E0ABD76B2D0F640A
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Stringa".. },.. "1213957982723875920": {.. "message": "Kuris i. toliau pateikt. teigini. geriausiai apib.dina j.s. tinkl. ?".. },.. "128276876460319075": {.. "message": ".renginio suradimas".. },.. "1428448869078126731": {.. "message": "Vaizdo .ra.o sklandumas".. },.. " 1522140683318860351": {.. "message": ".vyko ry.io klaida. Bandykite dar kart..".. },.. "1550904064710828958": {.. "message": "Leid.iama skland.iai".. },.. "1636686747687494376": {.. "message": "Puiki".. },.. "1802762746589457177": {.. "message": "Garsumas".. },.. "1850397500312020388": {.. "message": "Ar .Chromecast. rodomas $START_LINK$programoje .Google Home.END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\lv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15891
Entropy (8bit):	5.36794040601742
Encrypted:	false
SSDEEP:	192:y18prUkm15wkLDG2raqhnZDuvyI762V6c8TEKdl:RrAL7rte62V6uml
MD5:	388590CE5E144AE5467FD6585073BD11
SHA1:	61228673A400A98D5834389C06127589F19D3A30
SHA-256:	05CA14196CA5D90B228C0F03684E03EBE403A3E7B513AE0A059244AE12B51164
SHA-512:	BF83AC90BC56CEB1CA12DCB47BCE542FB8CFE0BC14E34DE4FE1A84F7CDB4B54E36C125CEA7EE06EA6244F7795A0957A8A20DB30CA4C60FC6E96EF2A73544 8521
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".lesald.ts. att.ls".. },.. "1213957982723875920": {.. "message": "Kur. no t.l.k min.tajiem apgalvojumiem vislab.k raksturo j.su t.klu?".. },.. "128276876460319075": {.. "message": "Ier.ces atra.ana".. },.. "1428448869078126731": {.. "message": "Video vienm.r.ba".. },.. "1522140683318860351": {.. "message": "Neizdev.s izveidot savienojumu. L.dzu, m..iniet v.lreiz.".. },.. "1550904064710828958": {.. "message": "Vienm.r.gs a tt.ls".. },.. "1636686747687494376": {.. "message": "Nevainojama".. },.. "1802762746589457177": {.. "message": "Ska.ums".. },.. "1850397500312020388": {.. "message": "Vai j.su Chromecast ier.ce ir redzama $START_LINK$lietotn. Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2"..

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\ml\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	20986
Entropy (8bit):	5.347122984404251
Encrypted:	false
SSDEEP:	384:6pQrdbhWHZ3wOn1HbxytQdroExFVRnTPV6uml:X5hUtz6uml
MD5:	2AF93901DE80CA49DA869188BCDA9495
SHA1:	E60DF4F2FB12BD3F1CA869DAD9F6BDE0C17CEB11
SHA-256:	329E80AEE1212F634E180DEF7E16D6E38D9C9FDA9AC9DB1D99B8AE1626EF304E
SHA-512:	DD1711B017DC65E1272972A1BEBD7A1B1769E1F22B37B20582573392CD432725D19DCE134145B3C031428BC0B5948B02A9AA93C8A651BEAA189B686B7BC2AD4
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..........".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. " 1802762746589457177": {.. "message"

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\mr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19628
Entropy (8bit):	5.311054092888986
Encrypted:	false
SSDEEP:	192:PbrpprGy+RmIosTmidpzlF1Akk03LQYOkQrjNjP8hZYiEQ5z+excV6c8TEKdl:PbfrGUIos7dpzxbP7KrjNjaBEYuV6uml
MD5:	659F5B4ACA112D3ECBB6EC1613DDE824
SHA1:	5DEE35FCD260554999F8DDEC489FBA9F81FA8EEE
SHA-256:	C8B765E7A07578BC078A952E151E3B866506959E15E79E9E5E1DBB98F9C4008F
SHA-512:	F74B36C1B6160E444F4969D13788A9C60637BDC11DC5065B2518B668E8D638384E00557ACDC88B3EA225D9231B6BED4B227BFB2E12C92773073B256F62ADDE6
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\mr\messages.json	
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".... ....".. },.. "1636686747687494376": {.. "message": "....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "..... $START_LINK$ Goo

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\ms\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):	15330
Entropy (8bit):	5.193447909498091
Encrypted:	false
SSDEEP:	192:rCprBbx+Fkc4kYPr/pEt4EpXlIoV6c8TEKdl:CrYjer/mOE4oV6uml
MD5:	09D75141E0D80FBD3E9E92CE843DA986
SHA1:	B24EAB4B1242C31B69514D77BC1DB36A3F648F40
SHA-256:	8F1DBDEFD910AD88BEEC7956619CDB34391D6E69254C3A7497E8F87134AE8B5C
SHA-512:	935C69481F1555787FCB9A5490B3188B348284B600359239742A7D802ADD5CC8A30CC1F0942D52E620DFB388787FCD69B548BBAC590110245DF5763367A2DD5A
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Tidak bergerak".. },.. "1213957982723875920": {.. "message": "Antara yang berikut, manakah yang terbaik menggambarkan rangkaian anda?".. },.. "128276876460319075": {.. "message": "Penemuan Peranti".. },.. "1428448869078126731": {.. "message": "Kelancaran Video".. },.. "1522140683318860351": {.. "message": "Sambungan gagal. Sila cuba lagi.".. },.. "1550904064710828958": {.. "message": "Lancar".. },.. "1636686747687494376": {.. "message": "Sempurna".. },.. "1802762746589457177": {.. "message": "Kelantangan".. },.. "1850397500312020388": {.. "message": "Adakah anda dapat melihat Chromecast anda dalam $START_LINK$ apl Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content":

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\nb\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):	15155
Entropy (8bit):	5.2408655429422515
Encrypted:	false
SSDEEP:	192:5Pvl9prfckKJ+3kEUroBsL78Z4XyfhV6c8TEKdl:9vhrkDJ+UEUroE78OCJV6uml
MD5:	ED99169537909291BCC1ED1EA7BB63F0
SHA1:	5F72D51B6DBE8C622EF33D2B2AEBD7E9E20DAFB3
SHA-256:	65B6598225ADA1E14EE9CB76CA863708E8F9EE0724B4EDC8F9508532BD631BAB
SHA-512:	452704BFC109EEBDE7C9D83CFC9EADA7471989CA7D30F5C8754B6C2B026100A87C8D9ED49A09E398CEBA8B837829E2D9C6772EEEAF1AFA506F35BDDF25C20C23
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket av f.lgende eksempler beskriver nettverket ditt best?".. },.. "128276876460319075": {.. "message": "Enhetsgjenkjenning".. },.. "1428448869078126731": {.. "message": "Videojevnhet".. },.. "1522140683318860351": {.. "message": "Tilkoblingen mislyktes. Pr.v p. nytt.".. },.. "1550904064710828958": {.. "message": "Jevn".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Ser du Chromecasten din i $START_LINK$Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START_SPAN":

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\nl\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):	15327
Entropy (8bit):	5.221212691380602
Encrypted:	false
SSDEEP:	192:0Yiepr1oh/Kd1sko8MrIpL72Izq8pXL2vVRmdKV6c8TEKdl:04r60Xo8MrIpLpRXL0G0V6uml
MD5:	E9236F0B36764D22EEC86B717602241E
SHA1:	DE82B804B18933907095DEF3F2EF164C1BB5F9B6
SHA-256:	300F4F7C45EBE39EAAF40776C28D0A399A710699AAB58E9A8D43A6FD2DD00376
SHA-512:	BB8A81D5D1C3FB3CA05149137852CAC213DEECB0437DA85472D5C03DAEFFE28D73007D7921740E56FE8B79544F529670600D47B86C4F27BF45C090B4D55F23F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\nl\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Loopt vast".. },.. "1213957982723875920": {.. "message": "Welke beschrijving past het beste bij je netwerk?".. },.. "128276876460319075": {.. "message": "Apparaatdetectie".. },.. "142844886978126731": {.. "message": "Vloeiendheid van de video".. },.. "152214 0683318860351": {.. "message": "Kan geen verbinding maken. Probeer het opnieuw.".. },.. "1550904064710828958": {.. "message": "Vloeiend".. },.. "1636686 747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Zie je je Chromecast in de $START_LINK$Google Home appEND_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_dir7064_1931342275\CRX_INSTALL_locales\pl\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):	15418
Entropy (8bit):	5.346020722930065
Encrypted:	false
SSDEEP:	192:PBUprktnFwP5GkzF0r2Q3SdIucDGGmPlTV6c8TEKdl:ur2CDur2kT9aGydV6uml
MD5:	8254020C39A5F6C1716639CC530BB0D6
SHA1:	A97A70427581ADA902CA73C898825F7B4B4FAC8F
SHA-256:	2F4E4FC6AEB4A8E7F0E0DCE220D66E763F4EBF1FA79985834D636C6692FEA3E8
SHA-512:	9A2CD0F061A943CE04789FF259ECE5B3CCA11EBB6C1DF16C703F70394A5F89415E8EFB79CFB4646FC07FD261170A74602644FFF02ABD38548895CDF7DAB68E 6
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Zatrzymuje si.".. },.. "1213957982723875920": {.. "message": "Kt.ra z tych opcji najlepiej opisuje Twoj. sie.?".. },.. "128276876460319075": {.. "message": "Wykrywanie urz.dze.".. },.. "142844886978126731": {.. "message": "P.ynno.. obrazu".. },.. "1522140683318860351": {.. "message": "Nie uda.o si. nawi.za. po..czenia. Spr.buj ponownie.".. },.. "1550904064710828958": {.. "message": "P.ynna".. },.. "1636686747687494376": {.. "message": "Idealna".. },.. "1802762746589457177": {.. "message": "G.o.no..".. },.. "1850397500312020388": {.. "message": "Czy Chromecasta wida. w.$S TART_LINK$aplikacji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\pt\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):	15475
Entropy (8bit):	5.239856689212255
Encrypted:	false
SSDEEP:	192:L9PpriI0RYHf8kfrvvI/99T+BEsV6c8TEKdl:LrkYPfrgsV6uml
MD5:	FABD5D64267F0E6D7BE6983AB8704F8C
SHA1:	D4DAAD0FF5C461C51E6C1FD22B86AFC5B13E123F
SHA-256:	D82DCA262FF005668B252B478DEDAAC4A5C1E417AF9DE57C22F169A6680183AE
SHA-512:	AD8B2129DCB4F232AEDD7A2B90AF2EFA43497F9118C27AB843D279F7B0EDF70AF95251B46C8098AA831FEC0B2AF6AB0308D3DCFD9AE87BEA8AD9E0D1032E0 F8B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Congela".. },.. "1213957982723875920": {.. "message": "Qual das seguintes alternativas melhor descreve sua rede?".. },.. "128276876460319075": {.. "message": "Detec..o de dispositivos".. },.. "142844886978126731": {.. "message": "Suavidade da reprodu..o do v.deo ".. },.. "1522140683318860351": {.. "message": "Falha na conex.o. Tente novamente.".. },.. "1550904064710828958": {.. "message": "Suave".. },.. "163 6686747687494376": {.. "message": "Perfeita".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": ". poss.vel encontrar seu Chromecast no $START_LINK$app Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\ro\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):	15655
Entropy (8bit):	5.288239072087021
Encrypted:	false
SSDEEP:	192:rpzpr34BALdvonekYFJr2RlYh7YU95cep3AnjYCV6c8TEKdl:HrlqLdv0VYFJrT95c8VCV6uml
MD5:	75E16A8FB75A9A168CFF86388F190C99
SHA1:	C27CE4C1DB3DF2D232925C73DC9AC1FA24DAD396
SHA-256:	9C4716FF42A730F1E7725F0D9E703F311E79FDA31F85B4BB0B8863FC3C27AB9D
SHA-512:	9E0BF56560B1D73F9706FF6AA2D5628CBE58EFCE197899A7EE686B2395D0FA2F9927538DD9B7B152CE2DED4708A210DA3DD6F5350E62AF853E809782997B192
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\ro\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Redare cu bloc.ri".. },.. "1213957982723875920": {.. "message": "Care dintre urm.toarele descrie cel mai bine r e.eaua ta?".. },.. "128276876460319075": {.. "message": "Descoperirea dispozitivelor".. },.. "1428448869078126731": {.. "message": "Calitatea red.rii vi deoclipului".. },.. "1522140683318860351": {.. "message": "Conexiunea nu s-a stabilit. .ncerca.i din nou.".. },.. "1550904064710828958": {.. "message": "Redare lin.".. },.. "1636686747687494376": {.. "message": "Redare perfect.".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500 312020388": {.. "message": "Chromecastul dvs. apare .n $START_LINK$ aplica.ia 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_dir7064_1931342275\CRX_INSTALL_locales\ru\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):	17686
Entropy (8bit):	5.471928545648783
Encrypted:	false
SSDEEP:	192:Pu6PQpr19XtZkmVpFQkeVBSr/7Nq5k8TyIeBcrvV6c8TEKdl:ir7Q+LASrWk8CirvV6uml
MD5:	8EF94823972EA8D2FC9BB7EC09AB1846
SHA1:	4171DC9CE9D82FDA5A280517A1FE58C907D75CE3
SHA-256:	1009DB9FFA64E411B31E0780EBA43B9C9F8B05B5AC8CCA9A38514650261ABB0A
SHA-512:	83CEC6CF43F4A5A998B987DA6B6F236B36078C560F1CD79366AEBF2950ECD881F0B3ECC1C0769D911381B4A1D5901121E3620CA1AC2401BDE12642BE64EFD6A
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... .. ..?".. },.. "128276876460319075": {.. "message": "..... . ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": ".. ....".. },.. "1550904064710828958": {.. "message": "..... .....".. },.. "1636686747687494376": {.. "message": "... .....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".. .... Chromecast . $START_LINK$.....

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\sk\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):	15740
Entropy (8bit):	5.409596551150113
Encrypted:	false
SSDEEP:	192:PIwprzrAXVZdrkF9PMZq6rTxnfKVSk7bVV6c8TEKdl:jrojd4F94q6rRsdVV6uml
MD5:	C314FAC15AFF6A2EE9C732C64AB5A66D
SHA1:	D51F3362B5FDD2F3756DE42D7D6227DC818C6344
SHA-256:	8EE2A25A09D6D0F89063FAA34BA2BC4DB505DD31FE6D5064C5D6E1E153721484
SHA-512:	C0387992BFD6D5EA7781A6A8112DDAF9759A3FCE0B0D954F024B4368EBAE132EB5FB6D59DE69F7C015E049339F6A170F1B41236E222D09FF41020F912E9DCD3
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Zam.za".. },.. "1213957982723875920": {.. "message": "Ktor. z nasleduj.cich skuto.nost. najlep.ie popisuj. va.u sie.?".. },.. "128276876460319075": {.. "message": "Vyh.ad.vanie zariaden.".. },.. "1428448869078126731": {.. "message": "Plynulos. videa".. },.. "1522140683318860351": {.. "message": "Pripojenie zlyhalo. Sk.ste to znova.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "V.born.".. },.. "1802762746589457177": {.. "message": "Hlasitos.".. },.. "1850397500312020388": {.. "message": "Vid.te svoj Chromecast v.$START_LINK$aplik.cii 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_dir7064_1931342275\CRX_INSTALL_locales\sl\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):	15628
Entropy (8bit):	5.292871661441512
Encrypted:	false
SSDEEP:	192:Ppp0prwFOhNkcUw4kjkNOD7r31RdeYqakV6c8TEKdl:0rXjYwy4Xr34AkV6uml
MD5:	F60AB4E9A79FD6F32909AFAC226446B3
SHA1:	07C9E383D4488BEBE316CA86966FC728F55A2E32
SHA-256:	CDE581E6E7CF0136B003B45549E3BBEE7B67B74ADD786A8D5607BFDAD1DE7B87
SHA-512:	F6A7673A8EFDB7FF74D7B83DD4BCB3683031DB7FBFE6654F6311CBA53EC42F3E45CE2B42A6E385F868271BBDD348272ACF9CE304E2DB52A10B36D24C7B03114F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\sl\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": "Zamrzne".. },.. "1213957982723875920": {.. "message": "Kaj od tega najbolje opi.e va.e omre.je?".. },.. "12 8276876460319075": {.. "message": "Odkrivanje naprav".. },.. "1428448869078126731": {.. "message": "Teko.e predvajanje videoposnetka".. },.. "1522140683 318860351": {.. "message": "Vzpostavitev povezave ni uspela. Poskusite znova.".. },.. "1550904064710828958": {.. "message": "Teko.e".. },.. "16366867476 87494376": {.. "message": "Odli.no".. },.. "18027627465894577 77": {.. "message": "Glasnost".. },.. "1850397500312020388": {.. "message": "Ali je Ch romecast viden v $START_LINK$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_dir7064_1931342275\CRX_INSTALL_locales\sr\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):	17769
Entropy (8bit):	5.433657867664831
Encrypted:	false
SSDEEP:	192:AtUpr9riVEviVutkeV74ErlLfWloyWR5Roxj2V6c8TEKdl:AGr1pvtuWDrS9Sj2V6uml
MD5:	4E233461D805CA7E54B0B394FFF42CAB
SHA1:	77F30833FC73A4C02C652C9E5A6EAFE9C3988A30
SHA-256:	E1E1C64213EBF2CFEB7BA83E51B697CEA449B3A8B279B1024B859228DE869879
SHA-512:	7288B11E9F46CF8138E0F8305E5E43CCCCCAD75F2D37EB2515C6BD54064FDC511A5872F0A940FA44A0B1B2355D2E0AED12A0D53267AC501B4E5CB6DDE43B00 0D
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "..... .."..},.. "1213957982723875920": {.. "message": ".... .. ..?"..},.. "12827687646 0319075": {.. "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",.. "placeholders": {.

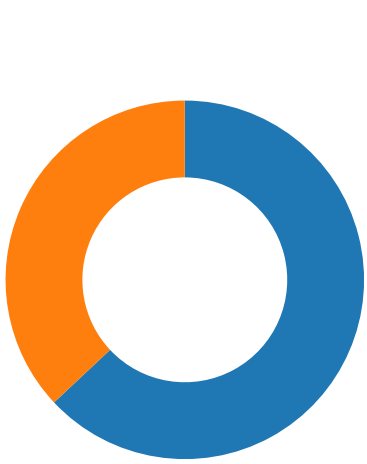
C:\Users\user\AppData\Local\Temp\scoped_dir7064_1931342275\CRX_INSTALL_locales\sv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15135
Entropy (8bit):	5.258962752997426
Encrypted:	false
SSDEEP:	192:LY5pr2y3Lm3kONgMr6nxJNuyF5JTpg2NOV6c8TEKdl:Yr5DMrAfpOV6uml
MD5:	897DAE6B0CF0FDE42648F0B47CB26E06
SHA1:	E1F5F5F65AF34FF9484AB2B01E571EAF19BA23D0
SHA-256:	52656C24F6F6D0F3B3FC01E9504C4D5CEB85624F1B22E974CA675DD0E94EB82D
SHA-512:	399DEACFE61F4AF9B24AAA0357D30149CC49DA7825295933D3AE006714B5DE7AC5FCB9EC5340B0E3AB4ABF25641032BBBB5B7D578CD204F4EDEAFE6E08C55 663
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Fastnar tillf.lligt"..},.. "1213957982723875920": {.. "message": "Vilket av f.ljande beskriver ditt n.tverk b.st?"..},.. "128276876460319075": {.. "message": "Enhetsidentifiering"..},.. "1428448869078126731": {.. "message": "J.mn videouppspelning"..},.. "1522140683 318860351": {.. "message": "Det gick inte att ansluta. F.rs.k igen."..},.. "1550904064710828958": {.. "message": "Flyter p."..},.. "1636686747687494376": {.. "message": "Perfekt"..},.. "1802762746589457177": {.. "message": "Volym"..},.. "1850397500312020388": {.. "message": "Visas 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"..},..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:24:47.045450926 CET	49738	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.046189070 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.086304903 CET	443	49738	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.086420059 CET	49738	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.086646080 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.086757898 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.097485065 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.097601891 CET	49738	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.137521982 CET	443	49738	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.137708902 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.139559984 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.139595985 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.139723063 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.157504082 CET	443	49738	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.157542944 CET	443	49738	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.157613993 CET	49738	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.634953976 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.635620117 CET	49738	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.635684967 CET	49738	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.635787964 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.636097908 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.675692081 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.675735950 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.676141024 CET	443	49738	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.676522017 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.676547050 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.676676989 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.677095890 CET	443	49738	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.677170038 CET	49738	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.679419041 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:47.716866970 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:47.759859085 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:52.670384884 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:52.670413017 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:52.670449018 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:52.670475960 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:52.670644999 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:52.670779943 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:52.769624949 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:52.809849977 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:52.822907925 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:52.822945118 CET	443	49739	104.18.22.110	192.168.2.4
Jan 11, 2021 18:24:52.823057890 CET	49739	443	192.168.2.4	104.18.22.110
Jan 11, 2021 18:24:57.218103886 CET	49766	443	192.168.2.4	172.217.23.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:24:57.260556936 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.260672092 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.260987043 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.303555965 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.316934109 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.316962004 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.316977978 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.316992998 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.317114115 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.317157984 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.338562012 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.338643074 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.338779926 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.381202936 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.381588936 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.381911039 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.382081985 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.384825945 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.384857893 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.384874105 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.384886980 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.385001898 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.385042906 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.386965990 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.386998892 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.387101889 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.387140989 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.389112949 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.389137030 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.389252901 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.389292955 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.391248941 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.391271114 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.391367912 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.391401052 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.393362045 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.393414021 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.393505096 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.393544912 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.395593882 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.395617962 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.395726919 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.395766020 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.397629976 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.397659063 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.397716045 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.397758007 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.399746895 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.399770021 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.399878025 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.399916887 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.424529076 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.424551964 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.424694061 CET	49766	443	192.168.2.4	172.217.23.1
Jan 11, 2021 18:24:57.427700996 CET	443	49766	172.217.23.1	192.168.2.4
Jan 11, 2021 18:24:57.427721977 CET	443	49766	172.217.23.1	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:24:39.666054010 CET	55854	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:39.722498894 CET	53	55854	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:40.624921083 CET	64549	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:40.672990084 CET	53	64549	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:24:41.880654097 CET	63153	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:41.929750919 CET	53	63153	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:43.149883032 CET	52991	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:43.197859049 CET	53	52991	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:45.223875999 CET	53700	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:45.271807909 CET	53	53700	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:46.979471922 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:46.983057976 CET	56627	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:46.989435911 CET	56621	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:47.036055088 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:47.050352097 CET	53	56627	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:47.056869030 CET	53	56621	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:48.037501097 CET	64078	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:48.104212999 CET	53	64078	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:48.214768887 CET	64801	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:48.233601093 CET	61721	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:48.279292107 CET	53	64801	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:48.281650066 CET	53	61721	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:49.004632950 CET	51255	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:49.071820974 CET	53	51255	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:52.135030985 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:52.182842970 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:53.329265118 CET	49285	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:53.377008915 CET	53	49285	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:54.255306959 CET	50601	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:54.306066036 CET	53	50601	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:55.434892893 CET	59172	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:55.485708952 CET	53	59172	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:57.140290022 CET	60579	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:57.217056036 CET	53	60579	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:57.547514915 CET	50183	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:57.595855951 CET	53	50183	8.8.8.8	192.168.2.4
Jan 11, 2021 18:24:58.878382921 CET	61531	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:24:58.937638044 CET	53	61531	8.8.8.8	192.168.2.4
Jan 11, 2021 18:25:03.824222088 CET	49228	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:25:03.883719921 CET	53	49228	8.8.8.8	192.168.2.4
Jan 11, 2021 18:25:06.597099066 CET	59794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:25:06.644995928 CET	53	59794	8.8.8.8	192.168.2.4
Jan 11, 2021 18:25:08.903635979 CET	55916	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:25:09.020581007 CET	53	55916	8.8.8.8	192.168.2.4
Jan 11, 2021 18:25:14.643843889 CET	52752	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:25:14.704608917 CET	53	52752	8.8.8.8	192.168.2.4
Jan 11, 2021 18:25:28.680063009 CET	60542	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:25:28.691040039 CET	60689	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:25:28.730775118 CET	53	60542	8.8.8.8	192.168.2.4
Jan 11, 2021 18:25:28.747164011 CET	53	60689	8.8.8.8	192.168.2.4
Jan 11, 2021 18:25:29.273297071 CET	64206	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:25:29.321455956 CET	53	64206	8.8.8.8	192.168.2.4
Jan 11, 2021 18:25:29.437067986 CET	50904	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:25:29.484956026 CET	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 18:24:46.979471922 CET	192.168.2.4	8.8.8.8	0x2b3f	Standard query (0)	www.notion.so	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:57.140290022 CET	192.168.2.4	8.8.8.8	0xc73f	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)

DNS Answers

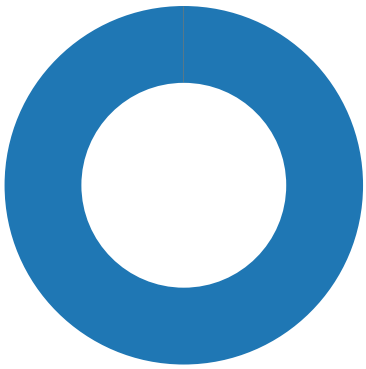
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 18:24:47.036055088 CET	8.8.8.8	192.168.2.4	0x2b3f	No error (0)	www.notion.so		104.18.22.110	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 18:24:47.036055088 CET	8.8.8.8	192.168.2.4	0x2b3f	No error (0)	www.notion.so		104.18.23.110	A (IP address)	IN (0x0001)
Jan 11, 2021 18:24:57.217056036 CET	8.8.8.8	192.168.2.4	0xc73f	No error (0)	clients2.google.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 18:24:57.217056036 CET	8.8.8.8	192.168.2.4	0xc73f	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.1	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 7064 Parent PID: 2216

General

Start time:	18:24:43
Start date:	11/01/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://www.notion.so/WORKSPACE-c062f3c6adef4fadbb3f459b4fa0d6df__;!!MdZ9-hZ0wg!a90_1yAqw74SgGAA7kXe4i93XCrFfwMkTpLPFrZ0ywOoEHviqXU3ETw0lwinDLX_gcs$ >(s).'
Imagebase:	0x7ff609c80000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF609CBFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: 5964 Parent PID: 7064

General

Start time:	18:24:45
Start date:	11/01/2021
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=1624,3718329257152011507,15757246875424185 32,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1732 /prefetch:8
Imagebase:	0x7ff609c80000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly