ID: 339742
Cookbook: browseurl.jbs
Time: 16:25:22
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0 Key=14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0 01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0 &3e2753cd9a0ab6203622ba5a4b7371780a5f934e89c28a415b3c9bf7c56e5487 3
- Overview 3
  - General Information 3
  - Detection 3
  - Signatures 3
  - Classification 3
- Startup 3
- Malware Configuration 3
- Yara Overview 3
- Sigma Overview 4
- Signature Overview 4
  - AV Detection: 4
- Mitre Att&ck Matrix 4
- Behavior Graph 4
- Screenshots 5
  - Thumbnails 5
- Antivirus, Machine Learning and Genetic Malware Detection 6
  - Initial Sample 6
  - Dropped Files 6
  - Unpacked PE Files 6
  - Domains 7
  - URLs 7
- Domains and IPs 7
  - Contacted Domains 7
  - Contacted URLs 7
  - URLs from Memory and Binaries 7
  - Contacted IPs 7
  - Public 8
  - Private 8
- General Information 8
- Simulations 10
  - Behavior and APIs 10
- Joe Sandbox View / Context 10
  - IPs 10
  - Domains 10
  - ASN 10
  - JA3 Fingerprints 10
  - Dropped Files 10
- Created / dropped Files 10
- Static File Info 41
  - No static file info 41
- Network Behavior 41
  - Network Port Distribution 41
  - TCP Packets 41
  - UDP Packets 43
  - DNS Queries 43
  - DNS Answers 43
- Code Manipulations 44
- Statistics 44
  - Behavior 44
- System Behavior 44
  - Analysis Process: chrome.exe PID: 4792 Parent PID: 3528 44
    - General 44
    - File Activities 45
    - Registry Activities 45
  - Analysis Process: chrome.exe PID: 2852 Parent PID: 4792 45
    - General 45
    - File Activities 45
    - Registry Activities 45
- Disassembly 45

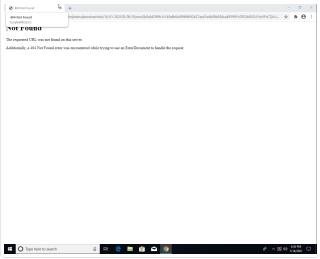
Analysis Report https://tuoyieefdcxz.ru/skjdncjksdncjke…

Overview

General Information

Sample URL:	https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c...rU3J2MHhW-&3e2753cd9a0ab6203622ba5a4b7371780a5f934e89c28a415b3c9bf7c56e5487
Analysis ID:	339742

Most interesting Screenshot:



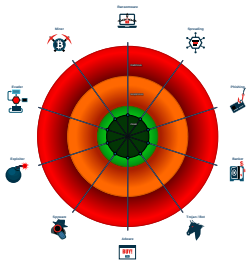
Detection

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 4792 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV/?Key=14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV&rand=13InboxLightaspxn_14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV_U1hrVFhCTjlrU3J2MHhW-&3e2753cd9a0ab6203622ba5a4b7371780a5f934e89c28a415b3c9bf7c56e5487' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2852 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1676,6103540828752338741,13537251628659214977,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

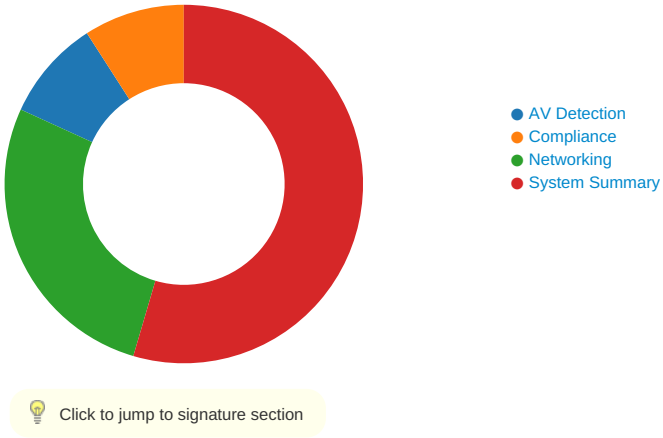
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

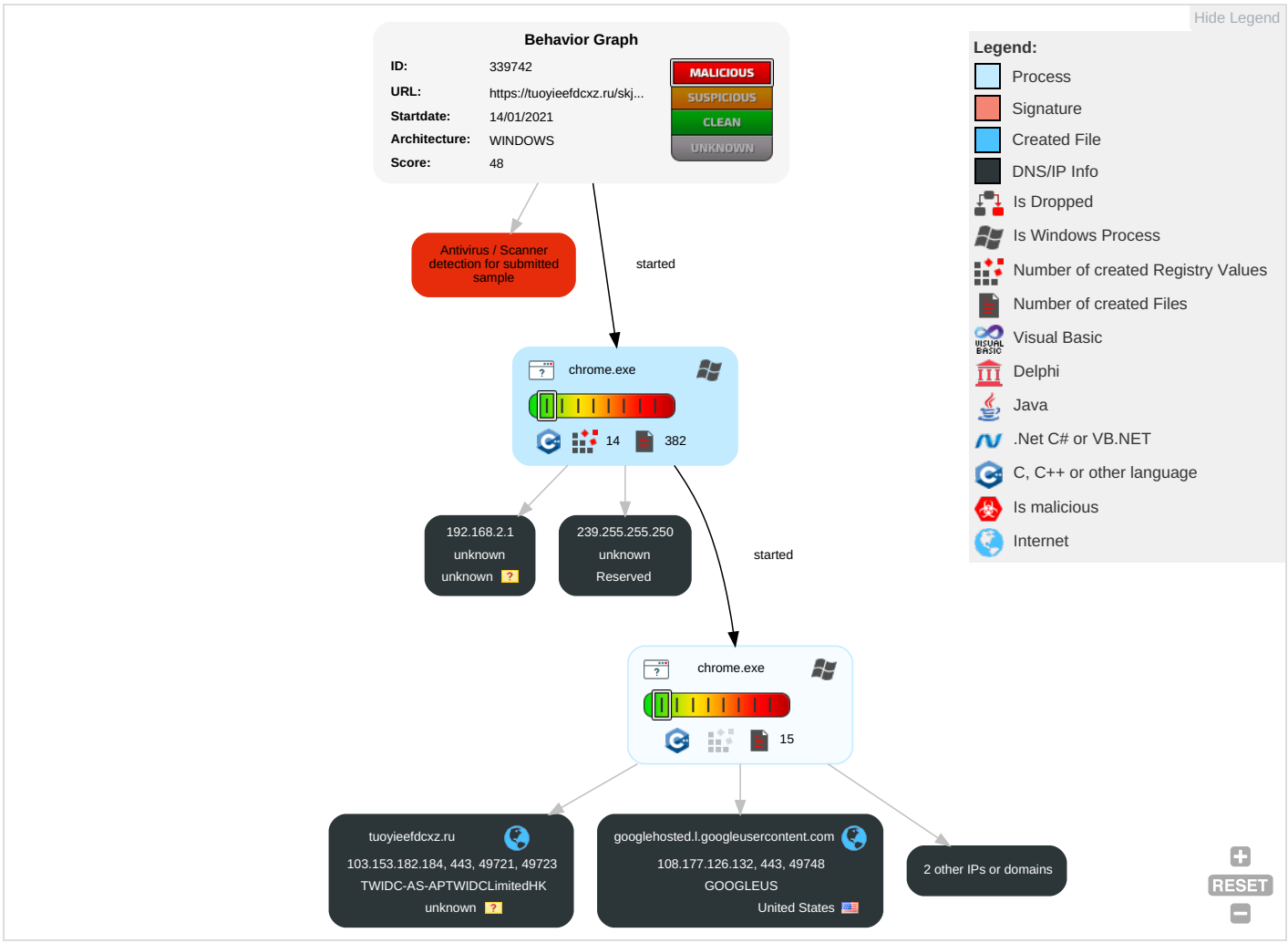
AV Detection:

Antivirus / Scanner detection for submitted sample

Mitre Att&ck Matrix

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

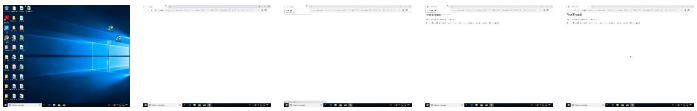
Behavior Graph

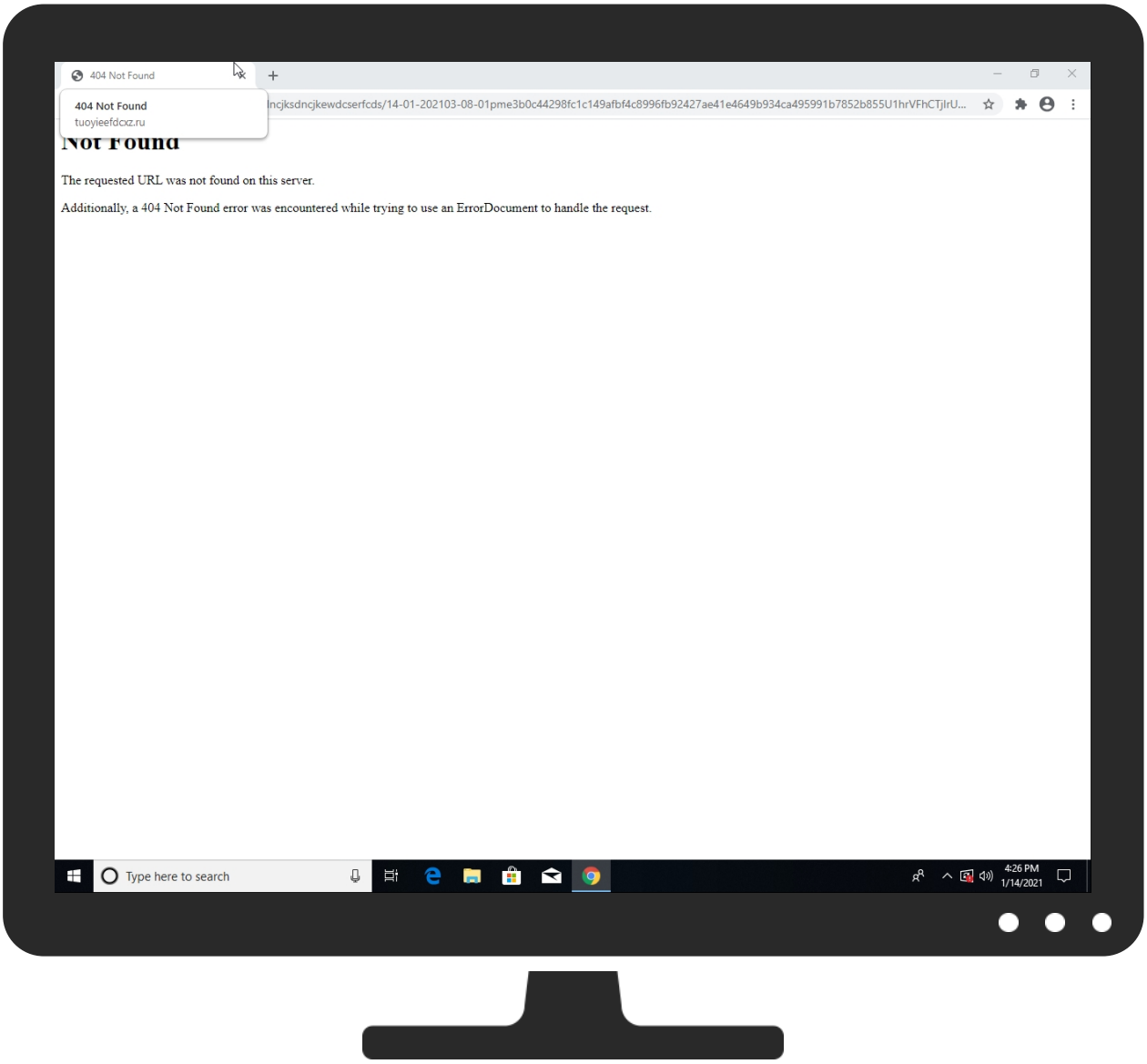


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV/?Key=14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV&rand=13InboxLightaspxn_14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV_U1hrVFhCTjlrU3J2MHhW-&3e2753cd9a0ab6203622ba5a4b7371780a5f934e89c28a415b3c9bf7c56e5487	0%	Avira URL Cloud	safe	
http://https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV/?Key=14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV&rand=13InboxLightaspxn_14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV_U1hrVFhCTjlrU3J2MHhW-&3e2753cd9a0ab6203622ba5a4b7371780a5f934e89c28a415b3c9bf7c56e5487	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

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	
http://https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb9	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tuoyieefdcxz.ru	103.153.182.184	true	false		unknown
googlehosted.l.googleusercontent.com	108.177.126.132	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

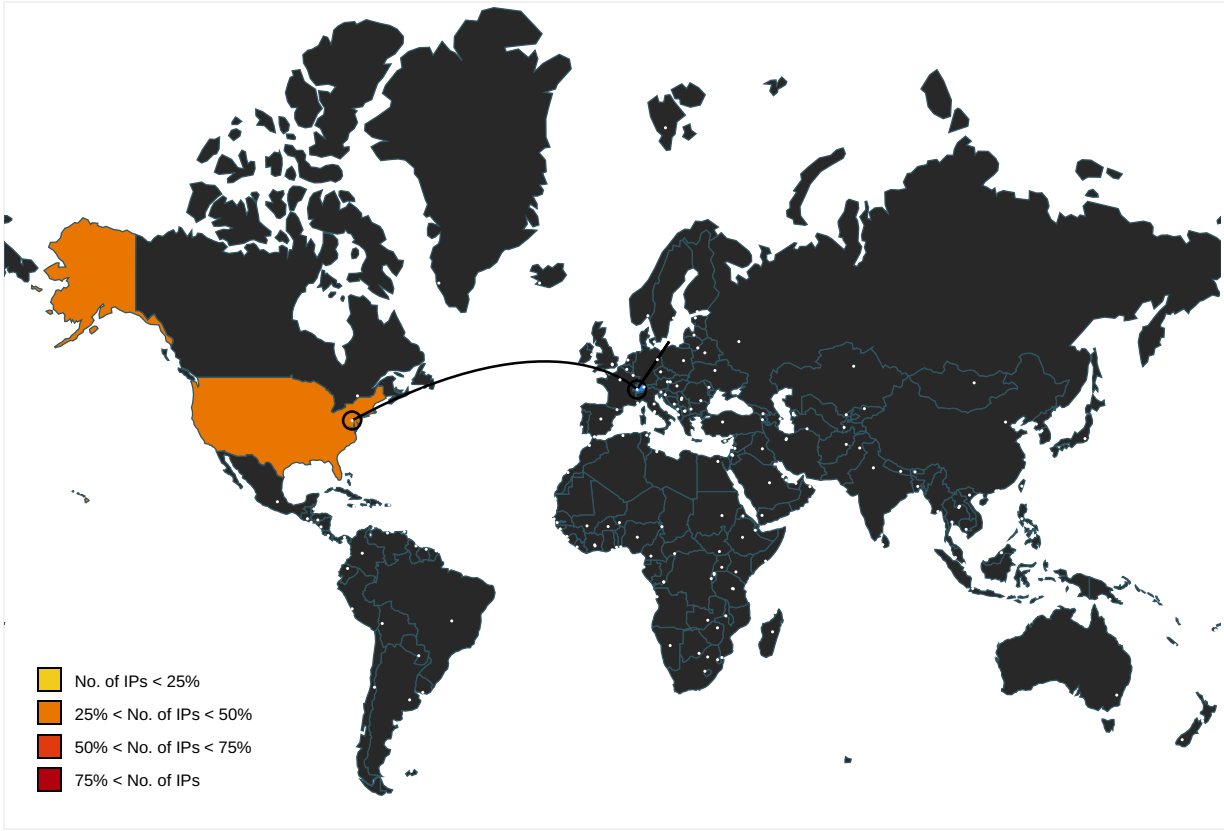
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV/?Key=14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV&rand=13InboxLightaspxn_14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV_U1hrVFhCTjlrU3J2MHhW-&3e2753cd9a0ab6203622ba5a4b7371780a5f934e89c28a415b3c9bf7c56e5487	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	8cecc3d9-1a60-48f9-85d8-698739c04173.tmp.1.dr, 8fb9e46e-fe4d-45ac-a636-fe67a25f4c27.tmp.1.dr, d722801a-4763-469e-88b5-239ae2661558.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients2.googleusercontent.com	d722801a-4763-469e-88b5-239ae2661558.tmp.1.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb9	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
103.153.182.184	unknown	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	false
108.177.126.132	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339742
Start date:	14.01.2021
Start time:	16:25:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV/?Key=14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV&rand=13InboxLightaspxn_14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV_U1hrVFhCTjlrU3J2MHhW-&3e2753cd9a0ab6203622ba5a4b7371780a5f934e89c28a415b3c9bf7c56e5487

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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@28/156@2/5
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 108.177.119.101, 108.177.119.138, 108.177.119.139, 108.177.119.113, 108.177.119.102, 108.177.119.100, 173.194.69.84, 108.177.119.94, 172.217.218.101, 172.217.218.102, 172.217.218.138, 172.217.218.139, 172.217.218.100, 172.217.218.113, 74.125.104.87, 173.194.188.234, 172.217.218.95, 108.177.119.95, 108.177.126.95, 108.177.127.95, 23.210.248.85, 51.11.168.160, 92.122.213.247, 92.122.213.194, 51.103.5.186 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, clients2.google.com, redirector.gvt1.com, r1.sn-4g5ednle.gvt1.com, emea1.notify.windows.com.akadns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, r5.sn-4g5ednsk.gvt1.com, client.wns.windows.com, fs.microsoft.com, accounts.google.com, e1723.g.akamaiedge.net, www.googleapis.com, skypedataprdcoleus16.cloudapp.net, r5---sn-4g5ednsk.gvt1.com, r1---sn-4g5ednle.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, par02p.wns.notify.trafficmanager.net, vip2-par02p.wns.notify.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. • VT rate limit hit for: https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV/?Key=14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV&rand=13InboxLightaspxn_14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV_U1hrVFhCTjlrU3J2MHhW-&3e2753cd9a0ab6203622ba5a4b7371780a5f934e89c28a415b3c9bf7c56e5487

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\13c13e68-05ad-4133-9597-ef33aee7fa12.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):	354244

C:\Users\user\AppData\Local\Google\Chrome\User Data\13c13e68-05ad-4133-9597-ef33aee7fa12.tmp	
Entropy (8bit):	6.015565998358825
Encrypted:	false
SSDEEP:	6144:DfmY28s8TWIWTkKD8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBM:hsll+wxzurRDn9nfNxF4ijZVtilBM
MD5:	84EE4CEA6CF2BA31A46D56A378645A01
SHA1:	8AF851A54E31C566C96DC9CBE638F0AC11FB268D
SHA-256:	76A399F3CDEFD4823CD61D43F06795EC66B54C8BDD058A4256A38200A1B01626
SHA-512:	82BFCF0F2C4B4DDD3B2EA24FBD64456751A46B7A40DFED08184FC6E0052BB0B6EF9E0186A35AACA8C5D51D25067CFAA64780478C7DA5B8ED894F809C672E05 1C
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.610670376043738e+12,"network":1.610637978e+12,"ticks":110022640.0,"uncertainty":4831621.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075768621"},"policy":{"last_statistics_update":"13255143972681

C:\Users\user\AppData\Local\Google\Chrome\User Data\29b9d9bc-0b12-4355-9a05-7b40ba09e5df.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.744262779420138
Encrypted:	false
SSDEEP:	384:PLq9J3gSfPIhkNxravVP325XOHfKGilrwzVBxObDLSrAtmojwPxFJiOfPlNc15YY:eKNlSjuCce353HUnbO/KVzppU
MD5:	28DBA74F5998AD6B6E2459BE1E21EFCA
SHA1:	2DB9DC478F0650B0E66FD296F87640F7C1B17D6C
SHA-256:	EE5133FC37C47915F5436C73FC6790DA53E2007935D77323774D3117856C2128
SHA-512:	92682C5E49B66005AEF80C241F0B6BDB2F0282F93AC7F9C117C0D6D0804AAFB0BDF6E196CC3165F5BC566DF05EAC71F3C2FF495CFD14FEA570B97B330FA762 6
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.....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:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\17d2b328-8e91-44c8-8159-a431afceb038.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):	5600
Entropy (8bit):	5.179908742294252
Encrypted:	false
SSDEEP:	96:npAEFbC4RYkHSV0LIk0JCKL8vkn11XbOTQVuwn:nyEM4GkHSaC4KWknj
MD5:	18A7D95CC9FB8A3C200FD94933CEA249
SHA1:	6483020A7EBB348B4BCD99E8C1F30EFAE3650E1B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\17d2b328-8e91-44c8-8159-a431afceb038.tmp	
SHA-256:	955EB669D486E94B107CF609574F14CFE812B5017946CCC77B59AEDB4FE1FC41
SHA-512:	E191C09913BF72DC97638DA8722692F4CBA43C1641E33CC310AE9521982C6CDB7F3077B6F2DB33501CDBBE06A7F42638482F455EED2DA41930D5BDC50F6DAA3
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13255143973090677","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\23e9e2c2-0e53-463e-8da1-e1dbe5e9acde.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):	22613
Entropy (8bit):	5.535205951673423
Encrypted:	false
SSDEEP:	384:Y43tTLlMvXJ1kXqKf/pUZNCgVLH2HfDQrUoHG6nTlLdR04u:tLlqJ1kXqKf/pUZNCgVLH2Hf8rUcG6nQ
MD5:	B6BF777BB4218A8F6EA049DF20CA1D50
SHA1:	E2E8ED7992A38BC59CDEA1188F2EDF4043D5C676
SHA-256:	255A40D748CFC4446CEDFF08C96F8140505E9F69123157D3E946FF132ABF1611
SHA-512:	C5D2FBD8A539CDB46B0F659EF6CFE391204DE95F79654AF69ED4A6A2A2655132A68115E7F24D7985E72C2EE426E3E9DBFEF6DDC92D6249C46F32FB17D37A5EBC
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":"13255143972759433","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\4773dc6b-18f1-43de-ad4c-bc831db8fb8f.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):	5.577938336952234
Encrypted:	false
SSDEEP:	384:Y43tOLlMvXJ1kXqKf/pUZNCgVLH2HfDQrU7Ln04R:ALlqJ1kXqKf/pUZNCgVLH2Hf8rU7b06
MD5:	486414EBAB2079445C3D6D8189DCC9D2
SHA1:	44081EA181DD2C525F9397172D1B8B8E47FC914D
SHA-256:	4A5EFE050F664860633698DDB424BE0AC4EBF97F43BECDA9464C73DCBBBF2CA7
SHA-512:	8E7A62C0A821D9C73C13C5683792EE22AB5A1ECB5E7E5A03505EA26930A5A548F755D1334A284F457D0D653EFEE40A1BCEF09ACFD536DF6431C222B43872C7DD
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":"13255143972759433","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\51209d81-c4ad-4e1e-9141-e73a84ce9a1e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\51209d81-c4ad-4e1e-9141-e73a84ce9a1e.tmp	
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\913cac2f-5ea7-4c8e-9bd5-ddad864240b9.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):	5003
Entropy (8bit):	4.965317647992244
Encrypted:	false
SSDEEP:	96:npAEF8G4pSV0LIk0JCKL8vkn11XbOTQVuwn:nyEd4pSaC4KWknj
MD5:	5F374535CED16BCADB90B7A2A085F6C3
SHA1:	3A85E08C4CC09BD42709B666F12BF898E7A8901A
SHA-256:	5F5C9ACA6E278426640B33072A3B0F28F1994CBC58CF863EEFA3147813EBE586
SHA-512:	0D9B23FDCCC44A60D20F5A99550DA708C4BE2D67DAF701924E2A31DB5B22F632895111F95427B1D3D062824BE1A603F9DF0ECF66E657276824AD15BFEDDAFE B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13255143973090677","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","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):	336
Entropy (8bit):	5.137194038761659
Encrypted:	false
SSDEEP:	6:mH+pq2P923iKKdK9RXXTZIFUtpK+bXZmwPK+QkwO923iKKdK9RXX5LJ:Ppv45Kk7XT2FUtp/L/P/Q5L5Kk7XVJ
MD5:	850955CC72FCACB10CA2C87000484BE7
SHA1:	2AD8F8EE5C723607030FCDAF4C99CA1D61207B00
SHA-256:	99C8CDD3CB2E2B9ABD6127E87D151B315322EDE67421355D4BC07269060266DD
SHA-512:	280F5386B1E5D00E6A001DEF750CB985EB4FA56F758879813E414C923F0EA0B6192BD946C70D68B2D50E7776A27986361B331654ED2540C713762A1DE2206777
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:31.236 1b40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/01/14-16:26:31.260 1b40 Recovering log #3.2021/01/14-16:26:31.261 1b40 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):	320
Entropy (8bit):	5.153531865991498
Encrypted:	false
SSDEEP:	6:mH+QHq2P923iKKdKyDZIFUtpK+2XZmwPK+DpkwO923iKKdKyJLJ:PQHv45Kk02FUtp/2/P/Dp5L5KkWJ
MD5:	4AB80ACAB04B523B9EC3592C6981F7F4
SHA1:	D84B56FE9310E874B80D6C6D479214C3B6A5D407
SHA-256:	F548959F40D4A92A4DCFC8DD9C20C7AF7F645CEA51C1AB54E081DD1467F5A079
SHA-512:	D86238936208897401A1A76BB459ABEB27A9BA397910E9262F3AD10AE200C45F79BCC9AFCA31690306E4E144C4657DFEC0C0FFD1CCCBC7D8D4CB44575F4344 3
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:31.158 1b40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/01/14-16:26:31.160 1b40 Recovering log #3.2021/01/14-16:26:31.163 1b40 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):	8192
Entropy (8bit):	1.3522352867864047
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwIG4rtEy8i:TekLLOpEO5J/Kn7ULNx
MD5:	6E69DB7D07E9598484B970BDD1398438
SHA1:	8B64F0C1E0AF8FAD6007A130467E25B729831474
SHA-256:	63E206A5BC4C6CA96897F9C2E75BD56D7542453FC5DC7AAB85D8979636EEF5EB
SHA-512:	20851DFCCB536AB818E5454245A0C41FD1813A6D291453FD27C2DA09E2C01D9E32FCB835341577BEA5837E5E532EF620E825B56256F4C2BE9EB74D7A5EE0EFA D
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):	8732
Entropy (8bit):	1.3147193248955562
Encrypted:	false
SSDEEP:	24:zIL4rtEy8/6nqLbJLbXaFpEO5bNmISHn06Uw2+9:zI+Dnq5LLOpEO5J/Kn7Us9
MD5:	8081EEED761EFBDB520F674520D78195
SHA1:	0C7CA5B2E87D4BF6FEF1982A9A9F46886FCBF85C
SHA-256:	4C087961CD51CBDDA96112272CE3D21E4EE9AA8635148AB336A7D67D16CFEADE
SHA-512:	E6B1027593F3A54606F5A64935B1EDFC2C9221FDC4E457FACB9A7E72B93CBF145F4B14A8BEEC5DB7B0135D27ED13E451ADAC6296A9100ABC059EC282B1A62A 27
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2883
Entropy (8bit):	4.540975021574652
Encrypted:	false
SSDEEP:	48:34Exec0022vttkttKgttBgwiMcIMG3MMBHGuvttkttKgttY:34r0XLkLpLzcTnomGLkLpLY
MD5:	1B4E3213164C35CA5833949767F991A7
SHA1:	0857742457265A88C8457126CA45649F9EE978AF
SHA-256:	D4A5A766DF9133C58EFF2B11355096F50ED74B883DE1D7378C9A02CC34482A42
SHA-512:	B715AA3902B192EF3ADB6E9DED3403E939702D73AAF48F49DEDCAEBD3FAF46BD039F815F44A583FD5E91398EFDD1D39577F1824FFB251A23E873829AF3E0BE FD
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...ab0ee2d2_2470_489a_b745_6a9585225c41.....{`..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....https://tuoyieefdcxz.ru/skjdncjksdncjkewdcserfcds /14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV/?Key=14-01-202103-0 8-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV&rand=13InboxLightaspxn_14-01-20210 3-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV_U1hrVFhCTjlrU3J2MHhW- &3e2753cd9a0ab6203622ba5a4b7371780a5f934e89c28a415b3c9bf7c56e5487....d...`.....X.....h.....`.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.124432946666287
Encrypted:	false
SSDEEP:	6:mH8klIL+q2P923iKKdK8aPrqIFUtpK88j1ZmwPK881LVkwO923iKKdK8amLJ:GIlv45KkL3FUtpa1/Pc5L5KkQJ
MD5:	DDB899E26996405EBF27AAE6DC7EB8BE
SHA1:	FA81CE0B99721A08E56BEEEE0CA2096C53C0D98B
SHA-256:	6EE07C95199478054F134C79F90A3A3B57DA8368886948B3C3A7D7831DF36044
SHA-512:	060CDE9EB6AE5D80B1B6CF95A5BFC9D515A7B33C26FAF06FE11CC34A840162A791F28C06465DD2E574B8A6D63849B5E42E0F690F5D1BAB1CF9A00815726089F
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:13.102 3e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/01/14-16:26:13.103 3e8 Recovering log #3.2021/01/14-16:26:13.103 3e8 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.164681933314147
Encrypted:	false
SSDEEP:	6:mH8Rq2P923iKKdK8NIFUtpK8rGZmwPK8r6kwO923iKKdK8+eLJ:jv45KkpFUtpo/Pw5L5KkqJ
MD5:	981FF6F9EC2334FA9B4B7F71B0C647DB
SHA1:	C39FA1DB710EECCAC1D45B9FDD7B515259D73AD6
SHA-256:	74B84EDDCDEEBEDFF492EEA995D5275226B7686A81A4E3FD0B8573C4141209EF
SHA-512:	8AF613158159CEDEC9989E5EF141539B4E4B406E3B9DCE2E55C3DE3137833595A7D700C5162344DBA76520F6B12E162BE2A4F5C1A8677C892D3F255E44018B8C
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:15.303 1470 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/01/14-16:26:15.305 1470 Recovering log #3.2021/01/14-16:26:15.305 1470 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:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49DC
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/aemUr2I/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/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

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.184732821620264
Encrypted:	false
SSDEEP:	6:mH+UaOq2P923iKKdK25+Xqx8chI+IFUtpK+cTZmwPK+cJkwO923iKKdK25+Xqx8E:PUaOv45KkTXfchI3FUtp/cT/P/cJ5L5G
MD5:	0261E56284747EC925F4E621276E20C1
SHA1:	D7831D5E502A887900F01AB24099AB858BFA2426
SHA-256:	65F008E7468C819D3422A229F39F12DC0F25C9326CAF5EF299011B3E591EE83B
SHA-512:	846C7495B09B232F2E3FAA5A5985254A43A2DEB0B569B691ECC5E18CBAD42C9F4F4BD415F7D57DCB60181BE1F6AD9304D1A9EA6378738C7B169ED88849026A0A
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:31.118 1b40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/01/14-16:26:31.120 1b40 Recovering log #3.2021/01/14-16:26:31.120 1b40 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):	360
Entropy (8bit):	5.202814782425501
Encrypted:	false
SSDEEP:	6:mH+VOKq2P923iKKdK25+XuoIFUtpK+VORFKZmwPK+VOxpkwO923iKKdK25+XuxWd:PIKv45KkTXYFUtp/IRFK/P/Ir5L5KkTZ
MD5:	2E4AC8D1BE4743C18E07818DA59FEEF5
SHA1:	A0347F915CCA200E42BEFFE346FE910CC3C0EF48
SHA-256:	C1C6C62A112A6E4ACC78810CC314CA47BF54A6B6D887403D6470EB88257C4B31
SHA-512:	6A2632B1A34703A887598A6D9FCB7F1FAAD23DD13C6A30BB53D0465164264E4697D9B63E50DE0F593F040120C91D702F84FFF27A21DE0200E3348DE7E7C672E7
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:30.963 1b40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/01/14-16:26:30.964 1b40 Recovering log #3.2021/01/14-16:26:30.965 1b40 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.192775942624294
Encrypted:	false
SSDEEP:	6:mH+VIsq2P923iKKdKWT5g1IdqIFUtpK+VUZmwPK+ViVFkwO923iKKdKWT5g1I3Ud:Pxv45Kkg5gSRFUtp/a/P/g5L5Kkg5gSu
MD5:	4EFAA4F1CC9975DDE8E323FBA58303BF
SHA1:	D480507F77B2DDC3260E331E15848948D8366524
SHA-256:	EC88ED30BD6B36AC588E10B61E460465F8245802B2EFF57DD54E94684771BE29
SHA-512:	28DC0998698807E44AEDD4539393FC2022C2052440F6B9B6931F70BB6CF4C2315EEE6F46A4F9A320F69B531082EFDD505CFCD8DF3C43E60FF77E2121B51C529
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:30.909 1b40 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/01/14-16:26:30.910 1b40 Recovering log #3.2021/01/14-16:26:30.912 1b40 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):	5.472535054932282
Encrypted:	false
SSDEEP:	48:WNmG19Pa7KM3q8dbv5SinbQSefgGELcNrS0U9RdiN9uN:mpa7KMZdbxSinbQ5fgGEorS0MN
MD5:	6FFBF5753FBDC093115FE17F68FFDE9F
SHA1:	173E7396CD86CD78976AACEAC368A0900F297EBA
SHA-256:	9BEB048EF3FDA103D27467DA27EEA83FEE7D846F44DE6D21D4CBBB32E07E7362
SHA-512:	46BAB935B079590D12BFDB344D1338948F9AB1CE7D538C2E68C3E7AB1CCCB2D885A204EA32B44E7B2F96E6E86ABA8D9CBBCEEE4EE2CE274B7A983908EBBAE627
Malicious:	false
Reputation:	low
Preview:	.I.....*.....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..217395000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-01-14 16:26:33.25][INFO][mr.Init] MR instance ID: 0f2978c9-b1a6-412d-ada4-4d42e8d6f738\n","[2021-01-14 16:26:33.25][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-01-14 16:26:33.25][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-01-14 16:26:33.25][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-01-14 16:26:33.25][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-01-14 16:26:33.26][INFO][mr.CastProvider] Query enabled: true\n","[2021-01-14 16:26:33.26][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):	334
Entropy (8bit):	5.104100329227829
Encrypted:	false
SSDEEP:	6:mH8X/ii+q2P923iKKdK8a2jMGIFUtpK8X5iXWZmwPK8XS6VkwO923iKKdK8a2jM4:Yi+v45Kk8EFUtp3iXW/PTV5L5Kk8bJ
MD5:	C349E4C9401D154ED544C78B8FBCDCE1
SHA1:	111BF939618ABBF0278E2B05068E464CB635E47E
SHA-256:	0EF5B5EF68112FC1639EE274CC545B1E326A7E155C288503E9B154E3EE7AE2D7
SHA-512:	196D370FA61AB40E23E1988FA0217275D1264CA85F06C38060F92ED28200CAEB3873AB6FED7E44BBA056DDF5C73091EB86C37362B683219C3D85AB5BC9D76E0
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:12.811 11cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/01/14-16:26:12.817 11cc Recovering log #3.2021/01/14-16:26:12.820 11cc 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):	336
Entropy (8bit):	5.166526239410282
Encrypted:	false
SSDEEP:	6:mH8TRSAq2P923iKKdKgXz4rRIFUtpK8GXZmwPK89kwO923iKKdKgXz4q8LJ:nTv45KkgXiuFUtpQX/PT5L5KkgX2J

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
MD5:	16D9CC04A4CE17EDB53152282A9FED19
SHA1:	8E3DAD2D8BCA992A35B6C124BF67F6138B0E0F09
SHA-256:	301A97FA35665408D4A18CA4E9B1F5A789B25E21E9352088A896D2636BD3F136
SHA-512:	A9E24C19CFC5160DB39A181552FECB86F9C7E79F24DB1BAFA4117F50C4A66854C9C85A8D3B44759A6CD841424018CE2B937AC5766A832CDA9F1FAC00C00A0DC
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:13.125 1470 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/01/14-16:26:13.127 1470 Recovering log #3.2021/01/14-16:26:13.128 1470 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
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl: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):	322
Entropy (8bit):	5.113810247847498
Encrypted:	false
SSDEEP:	6:mH8cq2P923iKKdKrQMxIFUtpK8uXZmwPK8pkwO923iKKdKrQMFLJ:ev45KkCFUtpMX/PL5L5KktJ
MD5:	40F134A11705E8684199E41D1A830671
SHA1:	9546A9F5BA7EA63241F75D3B8A884A8551127B1D
SHA-256:	4F0602B771261A3372B8DC1A8E43D2740BA2957BB19014A6F8983FA59784C8E4
SHA-512:	A09D75F27ACFDB4E25E2BEFBE579849C90EB23AD0B17FB1A953EAB8B77619FF433744C226D7954D861E7DFB8809E7D3066F1998139037F6EDE7EB6DABAB031E4
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:13.034 1470 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/01/14-16:26:13.035 1470 Recovering log #3.2021/01/14-16:26:13.036 1470 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):	350
Entropy (8bit):	5.127299091890712
Encrypted:	false
SSDEEP:	6:mH8XCp34q2P923iKKdK7Uh2ghZIFUtpK8XQUQ3JZmwPK8X/p3DkwO923iKKdK7UT:g4v45KklhHh2FUtpmvJ/P7D5L5KklhHd
MD5:	3DE18726502755400117DD8E387FFF3E
SHA1:	0612D184A5B94AE84F13BCB2F1A458A76CD670BB
SHA-256:	E7054085C3D4E774AEAAFC68CB00C50B2422D18B99B1A78596DEDECCF9B2E7D4
SHA-512:	1C206EDFD9CE50B087C07510DCF2F9AB32AC34E98464A38EB1DAF90117B056C347A5C779B2CB8D069A0304CD3A4A9FF473694D9F6235F1C9F531C5B718CFD9E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Preview:	2021/01/14-16:26:12.793 1760 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/01/14-16:26:12.801 1760 Recovering log #3.2021/01/14-16:26:12.811 1760 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\8fb9e46e-fe4d-45ac-a636-fe67a25f4c27.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):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.237523164327234
Encrypted:	false
SSDEEP:	6:mH8eTq2P923iKKdKusNpV/2jMGIFUtpK8MXZmwPK8/kwO923iKKdKusNpV/2jMmd:Mv45KkFFUtp+/Pl5L5KkOJ
MD5:	B072A184F808F0EB48694F5D06A43087
SHA1:	99E784E6419DDEF90848E24CE557872630BA0552
SHA-256:	96E226FA59E77381B0D146A9A5833AFA56E89B622213578B9E02365AC722B85C
SHA-512:	85D027384C18963656F7F9278283E3ABC9AE50C260B195FD6C4E66FCBEA28EAAA76187C40F694D62048D3DFA27E2BC2A8AFD776E714D980312C96CF1A68168F
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:13.076 1470 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/01/14-16:26:13.077 1470 Recovering log #3.2021/01/14-16:26:13.078 1470 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	5.2385362969978635
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
SSDEEP:	6:mH8Q4q2P923iKKdKusNpqz4rRIFUtpK8EZmwPK8MDkwO923iKKdKusNpqz4q8LJ:Vv45KkmiuFUtpG/PWD5L5Kkm2J
MD5:	930A6DA59211398AF6021AB74C9C657D
SHA1:	994609C19D49C9A6AE3ED8BED1911B66C1DC6B54
SHA-256:	92D7FD7A89243D55FF502BF2041C122462D0B9B45B5E74BDB8838774925DE04E
SHA-512:	6FBFDA3FDBE3A4D7C265B48CF188DDE00FC62B5D5F526A39364D6116587169A34F491ADDF9D40678DA7B3AE622EF65F083E29260CE0DA7ACBCB6A41BDF669FC
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:13.127 e90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/01/14-16:26:13.129 e90 Recovering log #3.2021/01/14-16:26:13.130 e90 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:	B0A7B194042859056638767 74A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	417
Entropy (8bit):	5.241181275939935
Encrypted:	false
SSDEEP:	6:mH+V6Oq2P923iKKdKusNpZQMxIFUtpK+VlBXZmwPK+VlBFkwO923iKKdKusNpZQq:P8Ov45KkMFUtp/jBX/P/jBF5L5KkTJ
MD5:	B51DD834075B0DE8E9DDD07FA387501B
SHA1:	4B870D48D023769619AD753AFF023C2393B11061
SHA-256:	C1235B2366E5D1B235230B7B4CC72A35CE383654CB3919B68C4AD98BF0E78ADB
SHA-512:	0A89BA92F0C2C637794C6C413FC7DFE84224D3E079BEDC8D5B99D3C16FF8D343145618FFC87A701C6363FAE57A33E34FC3F7155C03718B4E6DF9930F6B54CBF
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:30.054 d80 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/01/14-16:26:30.055 d80 Recovering log #3.2021/01/14-16:26:30.055 d80 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\8cecc3d9-1a60-48f9-85d8-698739c04173.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):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FB27
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.192802443051524
Encrypted:	false
SSDEEP:	12:PPudv45KkkGHArBFUtp/MI/P/MmF5L5KkkGHAryJ:Hs45KkkGgPgORkL5KkkGga
MD5:	F98CFC43CEAF6F18411AE6EC9B085EA6
SHA1:	5538F8E29AC73DE522528C2DF04E71C1D1D7C73C
SHA-256:	E173109BFB0465D21C6381AD33A410D6B9C0FED879ED212892EBFFBD6F832EA0
SHA-512:	CC54A8C05A13531876FFEA4FE2E3511E67222CD838D46282EBDF062E0AF1A4DFE51D39DD5F8503AECCC767A265171857743EE2376528A30D5B40794A2DEA07ED
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:31.328 1470 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/01/14-16:26:31.333 1470 Recovering log #3.2021/01/14-16:26:31.335 1470 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.147791341652052
Encrypted:	false
SSDEEP:	12:PMO+v45KkkGHArqiuFUtp/4FZ/P/jKNV5L5KkkGHArq2J:kH45KkkGgCgKFV8L5KkkGg7
MD5:	51D115C19F5E86D08728DCA33214BBED
SHA1:	F42948762B3656BA1895F197176445891A2CD29F
SHA-256:	3F4174B264F1A2AECB93AC703A62D1916FC2A5030CC5F6D2A5AD966AB404153F
SHA-512:	2760263E83422B6467729D0F878613E4BAFB50983D884F5DF33B05339368C5DC5F7E762A7560982067A7D6D1B1D3B0456392961E437596579B279577B2DD6C36
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:31.336 101c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/01/14-16:26:31.340 101c Recovering log #3.2021/01/14-16:26:31.342 101c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
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):	417
Entropy (8bit):	5.165463594009722
Encrypted:	false
SSDEEP:	12:734v45KkkGHArAFUtpw/P9D5L5KkkGHArfJ:e45KkkGgkgAVL5KkkGgV
MD5:	BB4E25970FEAFDE65BE3D8F33DF38B20
SHA1:	6FF27DE2B2E21AB640F936A0D6D986E94076786B
SHA-256:	50D7439CAC0AFADE1C0E55043929C80E37D625F384D45F7E7D0DD330897E06EB
SHA-512:	8C215A4926FBCE2D11C7D5597A5BA0C6D53DCFCB37C7BBBDCD9291E017952138F5F5FEE599BF92FCFE0FFD0D59590DC6618386F577B3CB7178DD5EB4EAAA5CCC
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:47.460 e90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/01/14-16:26:47.461 e90 Recovering log #3.2021/01/14-16:26:47.462 e90 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):	323
Entropy (8bit):	5.227096659654599
Encrypted:	false
SSDEEP:	6:mH8XWAq2P923iKKdKpIFUtpK8X2ZmwPK8XC7VzkwO923iKKdKa/WLJ:xv45KkmFUtpg/PAz5L5KkaUJ
MD5:	1C3C4D5E608A134960983D2C6C257B83
SHA1:	34BCC5202A2214C37AEB29F91DFEA859B4B8D738
SHA-256:	2E63275DDFCAA1EAE5989297E626DB13FB8607774E7924ED030B59E30925D6A8
SHA-512:	9DAC38DBDFD4C91923325BE009C996023CD9A25D5F8C8DE6DA02A8622C579EDDA75C54399802131A1C89C2FB4C2A069E6D96F39FC4FB87618A697BED7345A69
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:12.780 d80 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/01/14-16:26:12.784 d80 Recovering log #3.2021/01/14-16:26:12.793 d80 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Size (bytes):	401
Entropy (8bit):	5.2739917553493365
Encrypted:	false
SSDEEP:	12:PWRVx4v45KkkOrsFUtp/WRc/P/WRl5L5KkkOrzJ:oxK45Kk+gsL5Kkn
MD5:	8C9F8A247D55646FB2E4551BEB980D8C
SHA1:	30C4B16857866161E6BC4A29CC7F4DA1B713FE73
SHA-256:	5BA3B56BBAF102DC0F669A6392A5C43F3B1F6C17396EE782EEB846A51A8A0FDB
SHA-512:	679B04A111B6BC74A52B41DA9B4CE10F95E5F5DAB022B149A94F9F5F01418B44E6C3AA222187B6BCC79CD18C71D7B3444ED4B962731BF86C08C94167C87622F
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:33.242 e90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/01/14-16:26:33.243 e90 Recovering log #3.2021/01/14-16:26:33.244 e90 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\a2d55469-2d1c-459f-b06b-13edf16e9e79.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):	874
Entropy (8bit):	5.549545098730113
Encrypted:	false
SSDEEP:	12:YdDZ6Hk3O+UAnIvld06cY8rNgmh4r+UAnIElIWcNnYj+UAnIECm7yR7N+UAnIue0:YT6H0UhHPkG1KUe9aUeCe+7wUAHRUeIQ
MD5:	EBA63A25D9E1F209D82B9F383036888D
SHA1:	C15A7C9AD3A716AF8674DA93E62DD9F80EF2FE69
SHA-256:	8AF26C1DB3FA1D6D415F820C03C621F025A8020F001D1C94F7D6DD4AE723E291
SHA-512:	0D040F64DAA851D822779F24D196AF81A9A95E44BAD2B7816C01490DB9A183A8B39C93BA53ACEA4CFDB05BEB2B98C4550BB967E05164FD71FA7D1A72325F3F5
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1642206377.816362,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1610670377.816367},{"expiry":1633013028.952627,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.95263}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d722801a-4763-469e-88b5-239ae2661558.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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.431282696369548
Encrypted:	false
SSDEEP:	3:tUKnKb/sezAWZmwv3ZKb/HNDAR1V8sZKb/HNDAR1WGv:mHtZmwPK5A7VvK5A7tv
MD5:	1D28BB97721DA7EF5F9D87A0D5E0F2EE
SHA1:	41D2961AC7DEC597CF2A10C6730B4E227BDDE137
SHA-256:	859B20E67099169153866FD3245F54F84B54ED6B3447C151CB3BF13D6F554B53
SHA-512:	43725EED44C2532DB959248D83148542092448D9FF04AFB47DDAE1AEBC10D525835EB9F8378F139CDFA1ECCEF922299DA1799A45B0ACA2A69038DA45FE6DE9 9
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:25.279 1b40 Recovering log #3.2021/01/14-16:26:26.264 1b40 Delete type=0 #3.2021/01/14-16:26:26.264 1b40 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:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dedba624-db8b-4d95-b5e9-c872e1d72d38.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):	22614
Entropy (8bit):	5.53530363550066
Encrypted:	false
SSDEEP:	384:Y43tTLlMvXJ1kXqKf/pUZNCgVLH2HfDQrUoHGLnTlLw046:tLlqJ1kXqKf/pUZNCgVLH2Hf8rUcGLnt
MD5:	C42E7A10A0E2B5109996005454C27BCC
SHA1:	908059D3179A241836CBEF98B11BA02C40D06512
SHA-256:	0277698A638BA8AD29408CF62A752D1700FDFD982DE4443B83B8F4F18FC03007
SHA-512:	8850F7047DCF7302A5785F9FEC1E751FF15062F97745058741A00F0226044798F07EBF83733D3CBE4145810C883894490D13A9C8C31D5056F55EFB1404AA6885
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":"13255143972759433","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):	340
Entropy (8bit):	5.160287762184545
Encrypted:	false
SSDEEP:	6:mH+X57M+q2P923iKKdKfrzAdIFUtpK+XpZmwPK+X+MMVkwO923iKKdKfrzILJ:PX5I+v45Kk9FUtp/Xp/P/X+NV5L5Kk2J
MD5:	DE8137DCA7093BAB32AC6812D719C1D6
SHA1:	B4ED3339F5ACE1AA0E4959EFCD964D1AD4E2EB48
SHA-256:	81B2BFBC1BAED25E9D8A1CE4A5548D80FE9789FC08DA2607C94EB65D5359183C
SHA-512:	B8BFD7325CB2E686BF3262D412BFB91FF9371F55FCD9D85887C84AC55EDD1D2ED0B9D4DFF3B2BAB9FF35010BFE4D7F685763E6BF487135283B0742FFB61576 3
Malicious:	false
Reputation:	low
Preview:	2021/01/14-16:26:32.198 101c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.202 1/01/14-16:26:32.199 101c Recovering log #3.2021/01/14-16:26:32.200 101c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_prot o_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:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\cb285216-0430-41cd-8dce-ee0117f02cb6.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):	354244
Entropy (8bit):	6.015565722309393
Encrypted:	false
SSDEEP:	6144:rfmY28s8TWlWTkKD8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBM:ZsII+wxzurRDn9nfNxF4ijZVtilBM
MD5:	BC4B2BA5A0083ACD926850E9772742C6
SHA1:	0E7A371B8B8E97655F5747D254EA8F9D18499819
SHA-256:	9B5A4C6631D7F549E7ED8CB7722432DEC64CDF9F3A2DFF898D17D9097F011ADB
SHA-512:	BDD703D0BF11F6CB1AA6664C155724F705861DFE32290E283CE2C69F45DFAB150B2DF66ADE2DA3302EBAE24B116C423820387207DB6E3E99FBE7D877D67980 E

C:\Users\user\AppData\Local\Google\Chrome\User Data\cb285216-0430-41cd-8dce-ee0117f02cb6.tmp	
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.610670376043738e+12,"network":1.610637978e+12,"ticks":110022640.0,"uncertainty":4831621.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMlXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13255143972681

C:\Users\user\AppData\Local\Google\Chrome\User Data\da2b9183-a704-4d82-a891-81dd7820f5dc.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):	354244
Entropy (8bit):	6.015565457922247
Encrypted:	false
SSDEEP:	6144:NfmY28s8TWIWTkKD8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBM:Dsll+wxzurRDn9nfNxF4ijZVtilBM
MD5:	91538B9BC194111B84B2DBDE69B704BF
SHA1:	EBFE12E84034F988CDCCF341154018A52077788B
SHA-256:	2520DCF442F152FA34EA5B0BEE1BE81C6D1310B36CF4DA84FA0142D7A0E230D6
SHA-512:	8B8A41BA1AA5611D125A654BA74CC0CDD373F8D3B7C180ED15E56E67D1B572A6DE3E9BD8DA696B8230F0C2F6A2016C0E4EE33B985392CB53AC3B5C2782F29761
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.610670376043738e+12,"network":1.610637978e+12,"ticks":110022640.0,"uncertainty":4831621.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMlXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13255143972681

C:\Users\user\AppData\Local\Temp\2ef1aba1-5b32-43fb-bd8a-fe2f62484bc6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...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\80e8c5b1-60e1-43ea-a5e1-5060469ff7bc.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

C:\Users\user\AppData\Local\Temp\80e8c5b1-60e1-43ea-a5e1-5060469ff7bc.tmp	
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\e14fe71f-92f9-4cec-950d-b601371af144.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:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA56812320
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.I)N.|b.I....{.K@]6.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....Rl.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\f4a456bb-8292-47ce-81fe-5d506a3b44f7.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_dir4792_1577057514\2ef1aba1-5b32-43fb-bd8a-fe2f62484bc6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q...:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\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

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\CRX_INSTALL_locales\am\messages.json	
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\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",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\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": "..... .. .., ...".. },.. "155090406471082895 8": {.. "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_dir4792_1577057514\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:IPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\CRX_INSTALL_locales\bn\messages.json	
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ... .".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\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:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7ADB
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_dir4792_1577057514\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

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\CRX_INSTALL_locales\da\messages.json	
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "180276274658945717 7": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $ START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\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:	96:2MKUOp5N7GTNMRuv6M0blt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\CRX_INSTALL_locales\mr\messages.json	
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".... ....".. },.. "1636686747687494376": {.. "message": "....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "..... $START_LINK$ Goo

C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\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?".. },.. "1282768764603190 75": {.. "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_dir4792_1577057514\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?".. },.. "1282768764603190 75": {.. "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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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_dir4792_1577057514\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

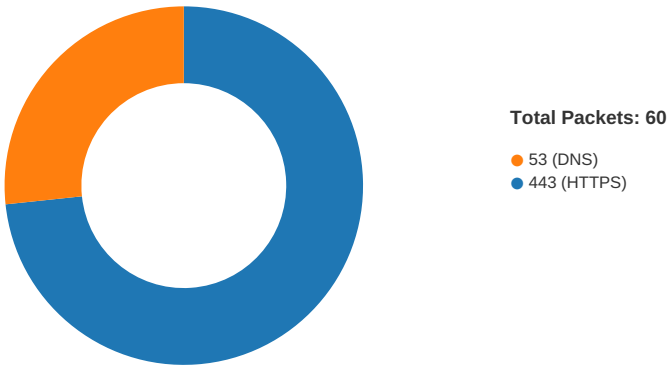
C:\Users\user\AppData\Local\Temp\scoped_dir4792_1577057514\CRX_INSTALL_locales\sl\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": "Zamrzne".. },.. "1213957982723875920": {.. "message": "Kaj od tega najbolje opi.e va.e omre.je?".. },.. "12 8276876460319075": {.. "message": "Odkrivanje 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".. },.. "18027627465894571 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".. },.

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 16:26:18.297010899 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.298783064 CET	49723	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.474275112 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.474389076 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.475557089 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.475826979 CET	443	49723	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.475930929 CET	49723	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.476146936 CET	49723	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.652991056 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.653194904 CET	443	49723	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.657361984 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.657438993 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.657469034 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.657509089 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.657516003 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.660829067 CET	443	49723	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.660872936 CET	443	49723	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.660900116 CET	443	49723	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.660989046 CET	49723	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.660991907 CET	443	49723	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.666462898 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.667089939 CET	49723	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.667650938 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.844120026 CET	443	49721	103.153.182.184	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 16:26:18.844197035 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.844257116 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.845055103 CET	443	49723	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.845349073 CET	443	49723	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.845402956 CET	49723	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:18.845793962 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:18.964155912 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:19.046452045 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:19.275859118 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:19.464128971 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:24.230503082 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:24.230608940 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:24.230668068 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:25.383435965 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:25.386115074 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:25.560585976 CET	443	49721	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:25.560770988 CET	49721	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:28.619910955 CET	49723	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:28.797584057 CET	443	49723	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:28.797636032 CET	443	49723	103.153.182.184	192.168.2.5
Jan 14, 2021 16:26:28.797772884 CET	49723	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:28.797808886 CET	49723	443	192.168.2.5	103.153.182.184
Jan 14, 2021 16:26:31.451045036 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.500845909 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.501074076 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.512890100 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.577440023 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.577480078 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.577507019 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.577533007 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.577557087 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.580630064 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.597482920 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.597517014 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.597521067 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.645715952 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.645816088 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.647635937 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.647660017 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.661237955 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.661268950 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.661288977 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.661308050 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.661344051 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.661379099 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.663597107 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.663620949 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.666153908 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.666228056 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.666251898 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.666382074 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.668803930 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.668823004 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.668941021 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.678160906 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.678180933 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.678193092 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.678209066 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.678224087 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.678240061 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.678258896 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.678289890 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.679343939 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.679368973 CET	443	49748	108.177.126.132	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 16:26:31.679441929 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.699105978 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.699130058 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.699187040 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.699209929 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.700246096 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.700263977 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.700304031 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.700340033 CET	49748	443	192.168.2.5	108.177.126.132
Jan 14, 2021 16:26:31.703638077 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.712991953 CET	443	49748	108.177.126.132	192.168.2.5
Jan 14, 2021 16:26:31.713022947 CET	443	49748	108.177.126.132	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 16:26:11.215735912 CET	55161	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:11.275146008 CET	53	55161	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:16.506692886 CET	55016	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:16.563206911 CET	53	55016	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:18.236686945 CET	50463	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:18.237828970 CET	50394	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:18.237907887 CET	58530	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:18.241332054 CET	53813	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:18.245779037 CET	63732	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:18.292125940 CET	53	53813	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:18.294188023 CET	53	50394	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:18.297028065 CET	53	58530	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:18.302768946 CET	53	63732	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:18.303972006 CET	53	50463	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:18.740566969 CET	57344	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:18.807781935 CET	53	57344	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:18.896245003 CET	54450	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:18.960855961 CET	53	54450	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:31.384933949 CET	56432	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:31.449429035 CET	53	56432	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:33.929580927 CET	52929	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:33.986165047 CET	53	52929	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:34.171211958 CET	64317	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:34.228790045 CET	53	64317	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:45.060611010 CET	61004	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:45.108606100 CET	53	61004	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:53.407581091 CET	56895	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:53.465564013 CET	53	56895	8.8.8.8	192.168.2.5
Jan 14, 2021 16:26:57.531090975 CET	62372	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:26:57.587673903 CET	53	62372	8.8.8.8	192.168.2.5
Jan 14, 2021 16:27:01.932598114 CET	61515	53	192.168.2.5	8.8.8.8
Jan 14, 2021 16:27:01.980448961 CET	53	61515	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 16:26:18.241332054 CET	192.168.2.5	8.8.8.8	0x28c8	Standard query (0)	tuoyieefdcxz.ru	A (IP address)	IN (0x0001)
Jan 14, 2021 16:26:31.384933949 CET	192.168.2.5	8.8.8.8	0x46fa	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)

DNS Answers

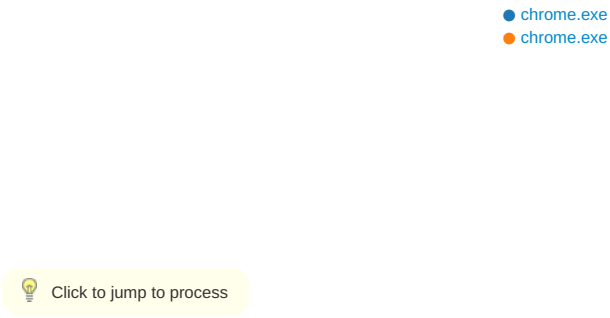
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 16:26:18.292125940 CET	8.8.8.8	192.168.2.5	0x28c8	No error (0)	tuoyieefdcxz.ru		103.153.182.184	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 16:26:31.449429035 CET	8.8.8.8	192.168.2.5	0x46fa	No error (0)	clients2.google.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 16:26:31.449429035 CET	8.8.8.8	192.168.2.5	0x46fa	No error (0)	googlehosted.l.googleusercontent.com		108.177.126.132	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4792 Parent PID: 3528

General

Start time:	16:26:11
Start date:	14/01/2021
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://tuoyiefdcxz.ru/skjdncjksdncjkewdcserfcds/14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV/?Key=14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV&rand=13InboxLightaspxn_14-01-202103-08-01pme3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855U1hrVFhCTjlrU3J2MHhWSXkTXBN9kSrv0xV_U1hrVFhCTjlrU3J2MHhW-&3e2753cd9a0ab6203622ba5a4b7371780a5f934e89c28a415b3c9bf7c56e5487'
Imagebase:	0x7ff677c70000
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 Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 2852 Parent PID: 4792

General

Start time:	16:26:13
Start date:	14/01/2021
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=1676,6103540828752338741,13537251628659214977,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8
Imagebase:	0x7ff677c70000
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	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly