ID: 350539
Cookbook: browseurl.jbs
Time: 15:03:32
Date: 09/02/2021
Version: 31.0.0 Emerald

Table of Contents

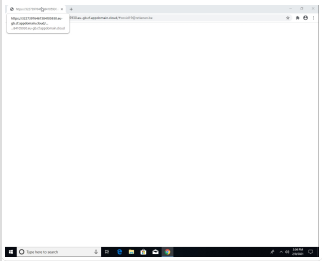
Analysis Report https://894f2824690f4f688cb014399e893…

Overview

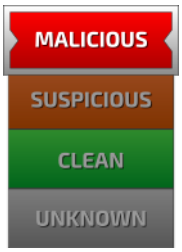
General Information

Sample URL:	http://https://894f2824690f4f688cb014399e893234.svc.dynamics.com/t/r/vb3XY_VLx7l-xHga3YHy8JRbFYUbDDzXt6qsDcUtzO0#covid19@rztienen.be
Analysis ID:	350539

Most interesting Screenshot:



Detection

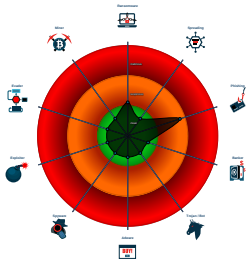


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Form action URLs do not match mai…
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- Submit button contains javascript call
- Suspicious form URL found
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5152 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://894f2824690f4f688cb014399e893234.svc.dynamics.com/t/r/vb3XY_VLx7l-xHga3YHy8JRbFYUbDDzXt6qsDcUtzO0#covid19@rztienen.be' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1364 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,17904341760629683302,56983860043845185 43,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1684 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

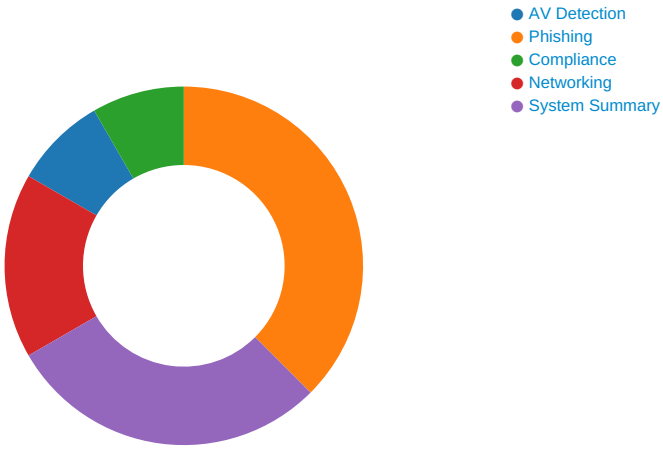
Yara Overview

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

Antivirus detection for URL or domain

Compliance:

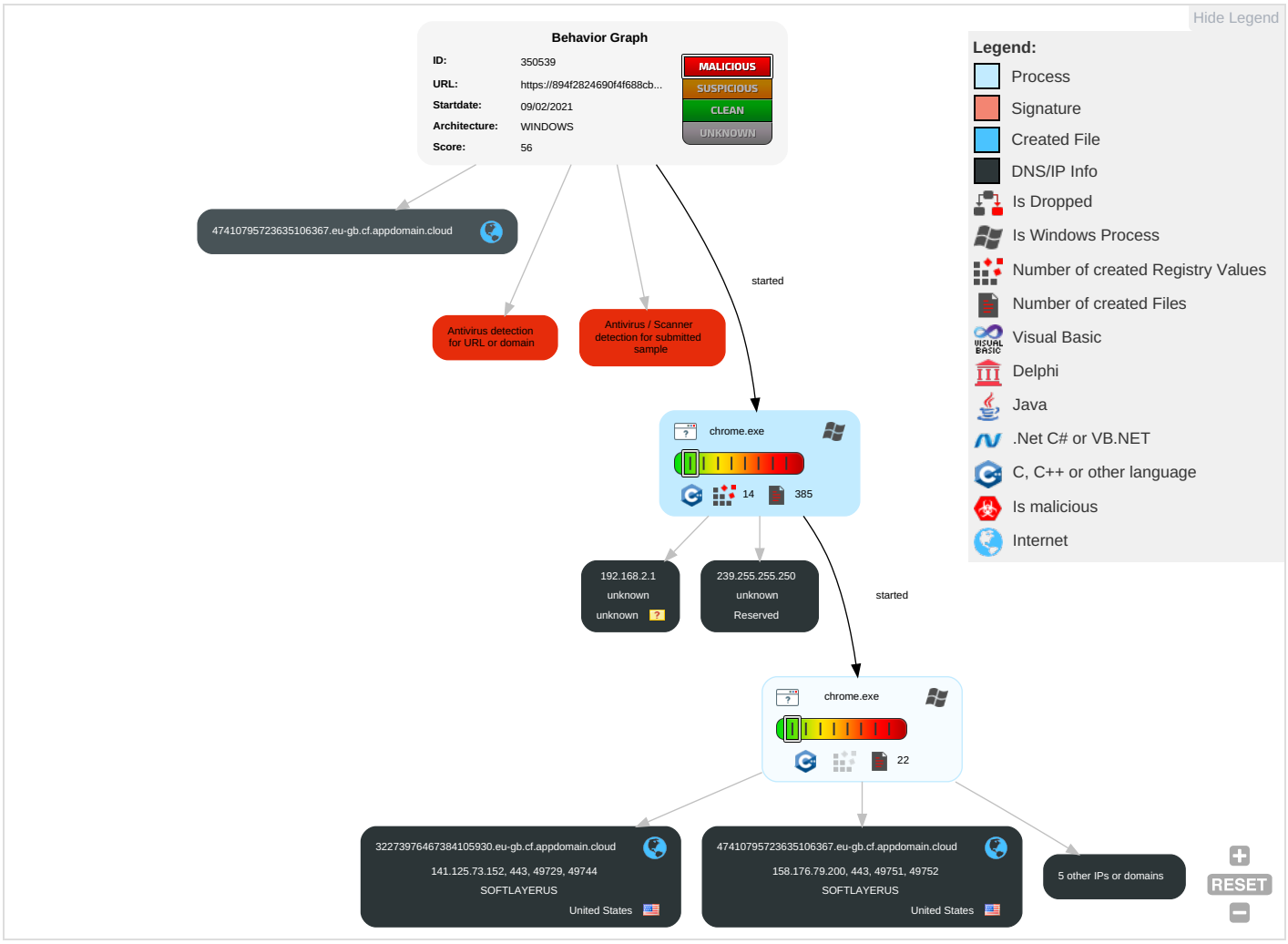
Creates a directory in C:\Program Files

Uses secure TLS version for HTTPS connections

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
Drive-by Compromise 1	Scripting 1	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
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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

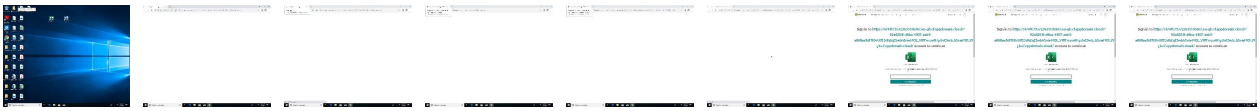
Behavior Graph

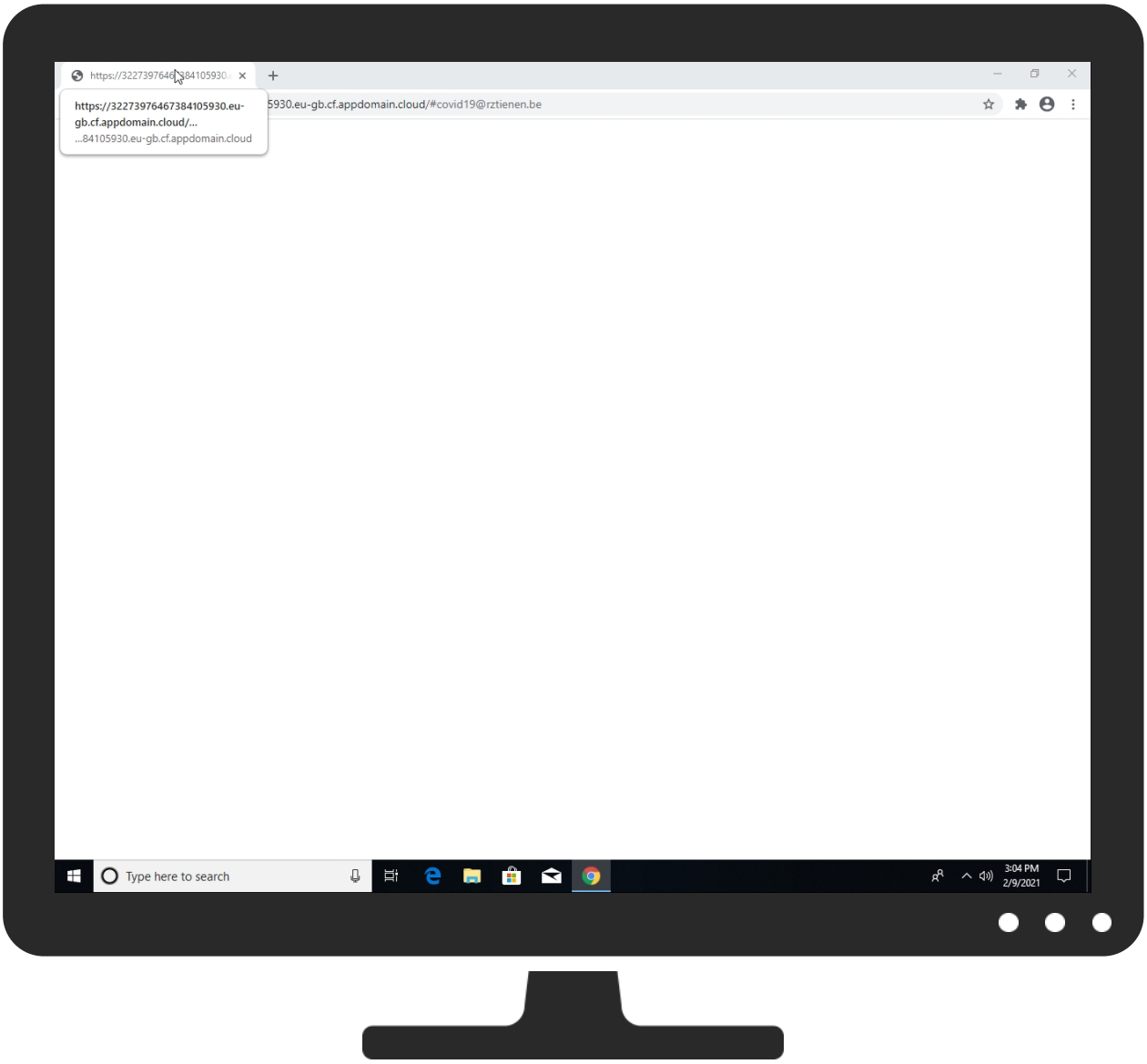


Screenshots

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://894f2824690f4f688cb014399e893234.svc.dynamics.com/t/r/vb3XY_VLx7l-xHga3YHy8JRbFYUbDDzXt6qsDcUtzO0#covid19@rztienen.be	0%	Virustotal		Browse
http://https://894f2824690f4f688cb014399e893234.svc.dynamics.com/t/r/vb3XY_VLx7l-xHga3YHy8JRbFYUbDDzXt6qsDcUtzO0#covid19@rztienen.be	0%	Avira URL Cloud	safe	
http://https://894f2824690f4f688cb014399e893234.svc.dynamics.com/t/r/vb3XY_VLx7l-xHga3YHy8JRbFYUbDDzXt6qsDcUtzO0#covid19@rztienen.be	100%	UrlScan	phishing brand: microsoft	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://32273976467384105930.eu-gb.cf.appdomain.cloud/#covid19@rztienen.be	100%	UrlScan	phishing brand: microsoft	Browse
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud/?92a6281f-d6ba-4907-aeb5-a668ae5df160vU053dh2qESwbhSnief4OL_VfRFmzw6HgUoESwb_hSnief4OLVfRFm#://32273976467384105930.eu-gb.cf.appdomain.cloud/:903092a6281f-d6ba-4907-aeb5-a668ae5df160vU053dh2qESwbhSnief4OL_VfRFmzw6HgUoESwb_hSnief4OLVfRFm37784=w020--2u	100%	UrlScan	phishing brand: microsoft	Browse
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud/	100%	Avira URL Cloud	phishing	
http://https://32273976467384105930.eu-gb.cf.appdomain.cloud	0%	Avira URL Cloud	safe	
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://47410795723635106367.eu-gb.cf.appdomain.cloud/?92a6281f-d6ba-4907-aeb5-a668ae5df160vU053dh2q	100%	Avira URL Cloud	phishing	
http://https://47410795723635106367.eu-gb.cf.appdomain.cloudh	0%	Avira URL Cloud	safe	
http://https://32273976467384105930.eu-gb.cf.appdomain.cloud/	0%	Avira URL Cloud	safe	
http://https://32273976467384105930.eu-gb.cf.appdomain.cloud/#covid19	0%	Avira URL Cloud	safe	
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud	100%	Avira URL Cloud	phishing	
http://https://appdomain.cloud/	0%	Avira URL Cloud	safe	
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud=5https://32273976467384105930.eu-gb.cf.appdoma	0%	Avira URL Cloud	safe	
http://https://32273976467384105930.eu-gb.cf.appdomain.cloud/perl/token/reactjs/?92a6281f-d6ba-4907-aeb5-a6	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
47410795723635106367.eu-gb.cf.appdomain.cloud	158.176.79.200	true	false		unknown
32273976467384105930.eu-gb.cf.appdomain.cloud	141.125.73.152	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.23.33	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
894f2824690f4f688cb014399e893234.svc.dynamics.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud/css/storage.html	true		unknown
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud/?92a6281f-d6ba-4907-aeb5-a668ae5df160vU053dh2qESwbhSnief4OL_VfRFmzw6HgUoESwb_hSnief4OLVfRFm#://32273976467384105930.eu-gb.cf.appdomain.cloud/:903092a6281f-d6ba-4907-aeb5-a668ae5df160vU053dh2qESwbhSnief4OL_VfRFmzw6HgUoESwb_hSnief4OLVfRFm37784=w020--2u	true	• 100%, UrlScan, Browse	unknown
http://https://32273976467384105930.eu-gb.cf.appdomain.cloud/#covid19@rztienen.be	true	• 100%, UrlScan, Browse	unknown
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud/css/dest5.html	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud/	Network Action Predictor-journal.0.dr	false	• Avira URL Cloud: phishing	unknown
http://https://32273976467384105930.eu-gb.cf.appdomain.cloud	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	b835b65e-20f3-4464-8424-2379eda66ff8.tmp.1.dr, 806b53b5-432d-474e-8896-c81c2150adad.tmp.1.dr, 54c0d32b-b64d-4ac6-8909-bd7dffab1345.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud/?92a6281f-d6ba-4907-aeb5-a668ae5df160vU053dh2q	History.0.dr	false	• Avira URL Cloud: phishing	unknown
http://https://47410795723635106367.eu-gb.cf.appdomain.cloudh	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud/css/storage.html	Current Session.0.dr	false		unknown
http://https://894f2824690f4f688cb014399e893234.svc.dynamics.com/t/r/vb3XY_VLx7l-xHga3YHy8JRbFYUbDDzXt6qsDc	History.0.dr	false		high
http://https://32273976467384105930.eu-gb.cf.appdomain.cloud/	Network Action Predictor.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://32273976467384105930.eu-gb.cf.appdomain.cloud/#covid19	Current Session.0.dr, History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud	Current Session.0.dr	false	• Avira URL Cloud: phishing	unknown
http://https://appdomain.cloud/	0eab880a7eb32e9b_0.0.dr, a21476c205fe2897_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud=5https://32273976467384105930.eu-gb.cf.appdoma	Current Session.0.dr	false	• Avira URL Cloud: safe	low
http://https://clients2.googleusercontent.com	b835b65e-20f3-4464-8424-2379eda66ff8.tmp.1.dr	false		high
http://https://47410795723635106367.eu-gb.cf.appdomain.cloud/css/dest5.html	Current Session.0.dr	false		unknown
http://https://32273976467384105930.eu-gb.cf.appdomain.cloud/perl/token/reactjs/?92a6281f-d6ba-4907-aeb5-a6	Current Session.0.dr, History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://appdomain.cloud/(	3de03e4ace9be524_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
158.176.79.200	unknown	United States		36351	SOFTLAYERUS	false
141.125.73.152	unknown	United States		36351	SOFTLAYERUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.23.33	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	350539
Start date:	09.02.2021
Start time:	15:03:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://894f2824690f4f688cb014399e893234.svc.dynamics.com/t/r/vb3XY_VLx7l-xHga3YHy8JRbFYUbDDzXt6qsDcUtzO0#covid19@rztienen.be
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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.win@29/165@5/6
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 172.217.23.78, 172.217.22.205, 216.58.207.174, 52.183.87.159, 74.125.173.135, 74.125.110.104, 13.64.90.137, 216.58.207.131, 104.42.151.234, 172.217.22.202, 172.217.22.234, 172.217.20.234, 172.217.23.42, 172.217.23.74, 92.122.145.53, 40.88.32.150, 51.11.168.160, 184.30.20.56, 205.185.216.10, 205.185.216.42, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): mktsvcp102wu001.westus2.cloudapp.azure.com, arc.msn.com.nsatc.net, r2.sn-4g5ednsy.gvt1.com, e13678.dscb.akamaiedge.net, clientservices.googleapis.com, r3.sn-4g5ednsr.gvt1.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, skypedataprdcoleus15.cloudapp.net, www.microsoft.com-c-3.edgekey.net, clients2.google.com, redirector.gvt1.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, www.googleapis.com, skypedataprdcolcus15.cloudapp.net, r3---sn-4g5ednsr.gvt1.com, blobcollector.events.data.trafficmanager.net, r2---sn-4g5ednsy.gvt1.com, clients.l.google.com, skypedataprdcolwus16.cloudapp.net, www.microsoft.com • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\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 GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\1440d5b4-4c78-4e80-b45c-c838631a38b6.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):	163958
Entropy (8bit):	6.081906797437628
Encrypted:	false
SSDEEP:	3072:a/4xSXQbWW6AI6tgG70tjhFYnt09bKbrfEx314FcbXafIB0u1GOJmA3iuR/:2QS2NI6rActEObraqfIlUOoSiuR/
MD5:	534910561F22EAC7B70D3B993328CEB2
SHA1:	75989CC8A1CD11722A2135349022F64A5760F1C2
SHA-256:	15430099E554319384918FDA2E26FB062B9EC83EE963587CAAB4FBA45F83213D
SHA-512:	A8BC5B7605D38F4C9AC9CC745F4A41D0DF41F0438145DB6D11336942DE8A360EDCCC671AB1E60EDF7A476C2FBBB85887FE24D0C3CD906BFE45DA2259B11413F
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":1.612911865199613e+12,"network":1.612879467e+12,"ticks":99192307.0,"uncertainty":4513447.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510166079 96"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\84c90b8e-30aa-40d2-ada7-5b5d8107d0e5.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):	163958

C:\Users\user\AppData\Local\Google\Chrome\User Data\84c90b8e-30aa-40d2-ada7-5b5d8107d0e5.tmp	
Entropy (8bit):	6.081906797437628
Encrypted:	false
SSDEEP:	3072:a/4xSXQbWW6AI6tgG70tjhFYnt09bKbrfEx314FcbXafIB0u1GOJmA3iuR/:2QS2NI6rActEObraqfIlUOoSiuR/
MD5:	534910561F22EAC7B70D3B993328CEB2
SHA1:	75989CC8A1CD11722A2135349022F64A5760F1C2
SHA-256:	15430099E554319384918FDA2E26FB062B9EC83EE963587CAAB4FBA45F83213D
SHA-512:	A8BC5B7605D38F4C9AC9CC745F4A41D0DF41F0438145DB6D11336942DE8A360EDCCC671AB1E60EDF7A476C2FBBB85887FE24D0C3CD906BFE45DA2259B11413F
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":1.612911865199613e+12,"network":1.612879467e+12,"ticks":99192307.0,"uncertainty":4513447.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftIE1G1mkftIE1G1mkftIE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC....................s}.....M..2.!..%sdPC....................s}.....M..2.!..%sdPC....................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0d35db51-bea6-4f7e-9913-e08fdc4f0cab.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):	5875
Entropy (8bit):	5.203659084457981
Encrypted:	false
SSDEEP:	96:nFKFPF546L2cVlok0JCZGRWL8Rskc1JbOTQVuwn:nFKD54C2cG4ZGYSskcr
MD5:	6813599659DA790FAD538A4C9F5BB4EC
SHA1:	E45B3CCDC2047E4082C532E8F88516C3F4138163
SHA-256:	0D6047CBA202BBBC5F4F1950DEEBE32C82E20551F3BBED835413F00947F096DE
SHA-512:	C430C30B5655A7EDA2A69D8530DAD13EFB0DD840E04E4BAF0CC8913E545FF30E2368FD240F93ADECDDF31B42C4F178355027826AF78EA9C7A979C334F633C19
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13257385462364275","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","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","0","0","7355378"],"daily_received_length":["0","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\46d57de0-36c3-42a5-b88e-0b208529028e.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\46d57de0-36c3-42a5-b88e-0b208529028e.tmp	
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\730aebb4-3175-47eb-8228-184b1de90565.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):	5923
Entropy (8bit):	5.201945489959421
Encrypted:	false
SSDEEP:	96:nFKF/F546L2cVHok0JCZGRWL8Rskc1JbOTQVuwn:nFK354C2cU4ZGYSskcr
MD5:	ACE8A11E1F5E1BE3EDA2147D7A228498
SHA1:	5ABFD1AC2ACD85EA3DB5AC9E354165564A07EA2C
SHA-256:	13F88A671C22A8E6DB0CFF1A9BED589995E6BC0F279C49DADB36BD6ACA5FBC00
SHA-512:	73E1C38E2B9888569ECFB67B5BAA3746EBF003939913FC50122A002F846FCE67724B2B234A745C356B9325BF2A7D2B00A338C3B621023767D1D8F77675C415AA
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13257385462364275","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","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","7355378"],"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\99577afc-55ca-45cc-8f67-c1becc9333fb.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):	22614
Entropy (8bit):	5.535777554696796
Encrypted:	false
SSDEEP:	384:MFrtMLlwiX831kXqKf/pUZNCgVLH2HfDhrUgHGAnTapGRs42:ZLlxW1kXqKf/pUZNCgVLH2Hf9rUkGAno
MD5:	EF18DF1542C8963A7003AABE357EFC3A
SHA1:	4EDB7945DB6AE85E4D79BC756B1C95C58BE1A175
SHA-256:	ED229E306C275E0E26994EB6A56E37658AF01FE6E99B8E65AE99D0030885A0F5
SHA-512:	0FFAE6F236E9372BFCA55B65361ADE1479472C423BA87DF3824140B403CD511B8660C3D36589988FCFF9BB84503A9513C3E00513E7B259755A7C1535DDE028AC
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":"13257385462049491","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\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.246718639441381
Encrypted:	false
SSDEEP:	6:muy+q2PWXp+N23iKKdK9RXXTZIFUtpP/ZmwPPmNVkwOWXp+N23iKKdK9RXX5LJ:bva5Kk7XT2FUtpH/PW5f5Kk7XVJ
MD5:	4CCBC46ABCA0E1313E04C458811B5677
SHA1:	858A063CB08B3D7E06FA3899548704CECAE273F3
SHA-256:	B374A87CE36603C402DCF9013BF23DEDDF809BAB15DF94AB8E6CC2A0C1AD2214
SHA-512:	A291A5C64144D3A31A5729342B92EF991D2B11A9B8F6D2D607A26C3C1C8E2F87483889F2EF1589B5F5CE186B2DC0A6A621826FD8B71FF02EFD7857EDF4C2B1E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2021/02/09-15:04:27.818 1928 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/02/09-15:04:27.831 1928 Recovering log #3.2021/02/09-15:04:27.832 1928 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.2283102493573
Encrypted:	false
SSDEEP:	6:muD+q2PWXp+N23iKKdKyDZIFUtpPfU+ZZmwPPFtdFNVkwOWXp+N23iKKdKyJLJ:Cva5Kk02FUtpP/PttdF5f5KkWJ
MD5:	276C8744A451FDF668EC4389F9309049
SHA1:	6472E26649EAB2E3DA08933FCBB9AA2F23F07ABC
SHA-256:	CD616F7779F1BA1766652909129B429C88915EA34BBB0E67A4E9ADAA13FF2185
SHA-512:	2857869E20A5EC77999F1C56EF6BA4EDBAFD28ACD3FC95CB08C57A84AA36F23EE716202268B5B3A43EBA83D15BD835D2B0CED0D55155D983C085F5D714A411CD
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:27.439 1928 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/02/09-15:04:27.440 1928 Recovering log #3.2021/02/09-15:04:27.442 1928 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\Code Cache\js\0eab880a7eb32e9b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	380
Entropy (8bit):	5.710956445612739
Encrypted:	false
SSDEEP:	6:mmYGLTDQyKfZ+O2uTBXWFRzhoHIQFYiDIyTydzXSx7jRR1FPbh/+hZK6t:3DQL2UhWFhhoH3FLTyRixFRt+
MD5:	EE1A7F857A271E7CDA0D3B73DE822CAE
SHA1:	E21EFCB48ED85688DEF716B659711D0EF31DF14F
SHA-256:	F5ADED9F1D034AFF853684840531058DECCFE16A6FFC866F1988C783A678B6DC
SHA-512:	27F8DC810E64EF2C9BFAB0E70CC4600C281A6A49D691D0D7EE9C277F9B3C62C922E357424404C6354114101E000AAC6874B1CFB94BA54DEC5851FC515FFAE01
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/microsoft-365/_scrf/js/themes=default/9e-6ade99/ff-dc7b13/2b-b6ab60/8a-91655a/28-8f59e1/71-4da314/58-f3fc85/e6-9d6ac7/cd-8ce651/f5-7e27a5/a1-c53a14?ver=2.0 .https://appdomain.cloud/`P.../.....[..h.....lB.&C../.}q.*...k./P..A..Eo.....~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3de03e4ace9be524_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	290
Entropy (8bit):	5.632799389459213
Encrypted:	false
SSDEEP:	6:mUXYGLTDQyKfZ+O2uTBXWFRzhGP4BOfzXS/1nK2YuTBxh+cmzprUbK6t:xzDQL2UhWFhh8i/VKqTBzQc
MD5:	06F71609A3065649587C89EE6FC5DCC7
SHA1:	43AFB9505C95892AC6B922FEC10ECED10419B49B
SHA-256:	BD5B402503B47D4CB5404225C2969AB3FDE6C7FC8F5424B9390F4B6EDC0CBB81
SHA-512:	42A325031F680016C80254EE1E8D5FFED39697888E4B8860E17F2A0403FC9D919272C3DA06C83A27783F53378EF54E467975AE311CFE5DD4474346F5F48F29C2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....hd....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/microsoft-365/_scrf/js/themes=default/9e-bcc229/94-3cd1e0?ver=2.0 .https://appdomain.cloud/(..../.....s..oZ._...x...9C..K.!(..P.A..Eo.....u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a21476c205fe2897_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	560

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a21476c205fe2897_0	
Entropy (8bit):	5.494559950435052
Encrypted:	false
SSDEEP:	12:fzDQL2UhWFhhBoKRtCOXXc8HNC1Ngw9jMuwLmzli1UpYzN:rjUYhHhtCOXXc8tCrMu0mz42pYzN
MD5:	6247A7C19BAD4BDF4329B1E83B769C43
SHA1:	E052CB3BBA6F4511BA1E28AD3AE8D1F2F046A246
SHA-256:	38B07CB63DDE01A5B180417FDF832A50D3AF836F1F90577DA1B167D94312144E
SHA-512:	A2A371D57A384EF47A240D1CF438BC6D6B6BE522A9BBD87D43962D058D7352A0021C51882BFAE8E7E60CDBBC41FC9EE9323A485C9B1F61F5AE76A024E99F7EC0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....*....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-neu-prod/microsoft-365/_scrf/js/themes=default/2f-63ce8f/2d-7a9063/dc-7e9864/4f-5115f8/7d-266f10/4a-abd94b/6d-c07ea1/29-1ec5a9/23-c64e70/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/f8-73a5f2/79-499886/7e-cda2d3/b2-7087f0/e5-08f1c0/91-97a04f/1f-100dea/33-abe4df/50-f1e180/e3-082b89?ver=2.0 .https://appdomain.cloud/.h.../.....4y2...O. q &i.....s..nQV..A..Eo.....g%.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	312
Entropy (8bit):	4.825769356326691
Encrypted:	false
SSDEEP:	6:aHXKXwTAOTxFvlmUZqyf/CzQ3zbn3pHkQ+IRwHcl:a3GwvljJfazyz7V4hcl
MD5:	6B2C5A255FFA3149B8DA8889905D3A01
SHA1:	934048B9200C6036DBA27C3755DB8ABFE8184DA6
SHA-256:	133A384EB1A88F555E3F7E28ABACD18A95DF95289FA5D7F2DE8E87D36AA48439
SHA-512:	578DF212451A8CC333A031494E0A2C22AD764A0032018340A3DB76DE33DC7769F7445EE312288971F320C819D96BD8F20BAA3290481988AFAAE696B3A11B1FB1
Malicious:	false
Reputation:	low
Preview:	0...#eBroy retne.....~....@..../.....(...v..@..../.....$..J>.=@..../.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<..\.O $.KPu../.....p..(....KPu../.....q....._.KPu../.....+<P|...X.KPu../.....[..../.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	12288
Entropy (8bit):	1.4761052998252646
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7U15w/DcpLBBiUINOZ3DFKS:dNwMgLBBLIO3ZKS
MD5:	91A07E756B0C97B8F445640006D78EC4
SHA1:	E11D4F9F6BD2FE91843441205610C8B53BF5FE28
SHA-256:	8BDBA60148DE1AA624BD39E9FA184CFB8AF9352F3501F9107F7B5EF04D58C471
SHA-512:	BD5849E733BBE50F7A95CC8294D9380A4130F4C5ED90EA133EA132501AF2CC7613467C13D1C61DFF1E1E4E5BB9E52EBD1E57EF502C36901F9A72E8C4725995(
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9667476275231096
Encrypted:	false
SSDEEP:	24:VcLgAZOZD/oqLbJLbXaFpEO5bNmISHn06Uw48:V8NOZoq5LLOpEO5J/Kn7Ub8
MD5:	51BF016C5F6CC8C8427298189B46C837
SHA1:	B5346F42DB9A6BEB097789EC72FEFE5C7490C509
SHA-256:	58A8C209F1CC2CC6D89DD8D07358F5D820585F95357625657F1F056F2AEFC8BC
SHA-512:	EAFD878BD2E39CF40DE52A541DE411FC0E8645F347ACED259F9AAA8448C9DE099FD867EBBCD0CC97D865325B8F3E08A57C7417AE51CAFB48F4A877794D4E0FC
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Reputation:	low
Preview:	.....s..... ....

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):	11064
Entropy (8bit):	4.2235081330235715
Encrypted:	false
SSDEEP:	192:3yjBvSJR4bfCp1ngSYsp5WkwpLTbfQbfkpWJKApwp699OTbfQbfkq/:qUpp1pRwpU9pwpc
MD5:	9342446A0371F1BA911985F9B6E66528
SHA1:	0CDE29F8B9AFE93F381A7053215A5CE646BC570B
SHA-256:	CEF31A145847577381F910431FBE8AD5204EB0F13C6B10777581A1E46CAD47CA
SHA-512:	615CCD3032646B6EB91F4A137B46A511DFCBCFFA633B78921B2BB5943BC720013F8913E3F9DCEDA463E19F168E3C1E33D7DA4D51E23BD0343F9493505F1799D
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...0832186c_05ed_4452_8608_3b7216add259.....fP..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....J...https://32273976467384105930.eu-gb.cf.a ppdomain.cloud/#covid19@rztienen.be.....h.....`.....N.....N...@.....X.....J...h.t.t.p.s.:././ .3.2.2.7.3.9.7.6.4.6.7.3.8.4.1.0.5.9.3.0...e.u.-.g.b...c.f...a.p.p.d.o.m.a.i.n...c.l.o.u.d./.#.c.o.v.i.d.1.9.@.r.z.t.i.e.n.e.n...b.e.....8.....0.....8..... ....}...https://894f2824690f4f688cb014399e893234.

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Entropy (8bit):	5.2239107797013355
Encrypted:	false
SSDEEP:	6:mQ1q2PWXp+N23iKKdK8aPrqIFUtpvIMZmwPvDkwOWXp+N23iKKdK8amLJ:f1va5KkL3FUtpvIM/PvD5f5KkQJ
MD5:	E84D868C8929032253CFDB30E1FD4021
SHA1:	C5C74E32642B00C869C1910B06B7D5A119AF6510
SHA-256:	D8E652DE7E72AEF321AD9B1FA69C31A153DAA90867C9723299F0E5C2780E347C
SHA-512:	A8D7749A167CE28E8270577AA62E3850410F9EA971048377B65B29D2D2FDC7AC8F67C2186AFF37B8241860A94D0B1F8ABB3DAEDEB4E4CF38B3CDFED9B5D019 A
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:22.370 1650 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/02/09-15:04:22.375 1650 Recovering log #3.2021/02/09-15:04:22.377 1650 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5..................f.5................f.5................f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.240267899472867
Encrypted:	false
SSDEEP:	6:mduVq2PWXp+N23iKKdK8NIFUtpwhVXZmwPxkwOWXp+N23iKKdK8+eLJ:iqva5KkpFUtpqh/Px5f5KkqJ
MD5:	A9DD916C8EB71CA26729DF52AF8C4591
SHA1:	DC1188405BC8F3632592BC4C9EBECC196D243DD2
SHA-256:	D8D0B37636DE0CAEAAFE99F87757CC350F71E5162CE8326EC7352333C0E739FC
SHA-512:	08CF9263F8FE93315E00D11F79FC1C85D44A23577B12A45B30AE9F30B2162820D1E1AD4BA9AE323C24A1DAEB84E070753E1C7742DCE1A1A9F1C4030A2B14C2D F
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:24.585 1650 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/02/09-15:04:24.587 1650 Recovering log #3.2021/02/09-15:04:24.588 1650 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","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):	372
Entropy (8bit):	5.288143214850104
Encrypted:	false
SSDEEP:	6:mu9+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpPWQ6ZZmwPPWQcVkwOWXp+N23iKKdP:Qva5KkTXfchI3FUtpf6Z/Pfc5f5KkTXc
MD5:	E2BB80C015A1276715D17215DED799BF
SHA1:	44C2A5CB457FF6EC4EAAC44542FC290A2963D41D
SHA-256:	0BB7FABC217734EE3833511F6764745A3C973A5A0AD746D3256DCC38BD4766C7
SHA-512:	E4AABC8EAB143A97BB72BE7CD8E300BAB16B525FB0CC7AD9B4FBB646A5665B6B834BBA4CC24236B298E47DA30A883FE98CA53032FDFC7DCD7EB72A758751B22A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/02/09-15:04:27.231 1928 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/02/09-15:04:27.357 1928 Recovering log #3.2021/02/09-15:04:27.359 1928 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.232446430665004
Encrypted:	false
SSDEEP:	6:muUcU+q2PWXp+N23iKKdK25+XuoIFUtpPUcqZmwPPUcB9VkwOWXp+N23iKKdK25y:cOva5KkTXYFUtpsV/PsaD5f5KkTXHJ
MD5:	2D6AF84191E9DCB4D428E3127D171E11
SHA1:	1B5214BCFCA6AC1CBED9EB240151D250314CCF51
SHA-256:	215087549675795EC75B317865FC8850E8EEF6C0ECD3ADF4CF1A44ABA4C47AA5
SHA-512:	161917C6E0147F23703E55FC09AC4E20B6A1A3C6AB2D905CCE2B123C8CFC32AEC8E2B922F9CC16324D4CD8045C3497AE4454ED52BF27C42C6054EC7C0FF305 2
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:27.191 1928 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/02/09-15:04:27.193 1928 Recovering log #3.2021/02/09-15:04:27.194 1928 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.257250062173096
Encrypted:	false
SSDEEP:	6:muN3+q2PWXp+N23iKKdKWT5g1IdqIFUtpPYFvFZZmwPPJ9VkwOWXp+N23iKKdKW4:gva5Kkg5gSRFUtpQvX/Px5f5Kkg5gS3e
MD5:	BAFFBFC5877597A3D20176AEED01194C
SHA1:	FB1EBAC0F64104991A904383BFAF463C7DFD20CA
SHA-256:	B46E4A3E4AA096228A6140E31197AFDB8E526A3C2149D6B0376C08C801B7AEE5
SHA-512:	69E61F82D11CD6DE944671D8D0F6A71F33B48E8537BA6A8859A7B70C4AE212F45C98A4E1470401821C818B351D8B90200048AEA32B693A17D845C9CA454C5CF3
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:27.068 1928 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/02/09-15:04:27.070 1928 Recovering log #3.2021/02/09-15:04:27.071 1928 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.7041420151743756
Encrypted:	false
SSDEEP:	48:T+GBqQdmFQ71GQxIrIDv2TRYGBqQ0mFQ71GQoFrIDu:yWbmFWfxIkL2TeWymFWfoFki
MD5:	91C5B6AFBF98CFF1B95831D4BD92BE7D
SHA1:	BDBA6A055C8E6BA632F009FCF3DC3DD7397883FE
SHA-256:	41D84432701363DC7F5E5DEAB99FE141A9E8C4076157C82D3EB2CEA77B66457F
SHA-512:	0E7DAF10D6D008B7EA28FEE72EB6296DC67F96E213E8A7FA6517BFC53F7053907572A77C21772922CD7D8B49AB47149856E332EE4D1B5331DDB05C1FA5E280E B
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Size (bytes):	1364
Entropy (8bit):	5.817005149643441
Encrypted:	false
SSDEEP:	24:S9rmI2Nr0D3IP8GQsN6qWslEeWqWH8SSgESZO5kAr8enyBDOxoaByr6tD2BtY7Eu:S9rmFJ8NebWfhnEpOArrByrIDsYR5
MD5:	6012AFE44BAE1691DEE7038851A75F6C
SHA1:	EE7A3F31CD8B4127E9A742975D0857D9B9761534
SHA-256:	426304F5FB3F433E009BD57D9BD10FB51F496A97BF8041FAB9DDDEC4E2B5CAB5
SHA-512:	F248FBB41BB90E0626A2E0DA8FAF2AA5079CBFE7B61ED963B8C2BB88668B68285CD4DE1E8A2C862B69F3FCF4FA1F403387FF0F26F3A5C91DC6D757ABC16812BC
Malicious:	false
Reputation:	low
Preview:	....."..... 894f2824690f4f688cb014399e893234..be..com..covid19..dynamics..https..r..rztienen..svc..t..vb3xy..vlx7l..xhga3yhy8jrbfyubddzxt6qsdcutzo0..322739 76467384105930..appdomain..cf..cloud..eu..gb*.....3227397646738410593O...$. 894f2824690f4f688cb014399e893234.....appdomain.....be.....cf.....cloud.....com.....covid19.....dynamics.....eu.....gb.....https.....r.....rztienen.....svc.....t.....vb3xy.....vlx7l...#..xhga3yhy8jrbfyubddzxt6qsdcutzo0..2..."....0.....1.....2.....3.....4. .....5.....6.....7.....8.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....l.....m.....n.....o.....p.....q.....r..... ..s.....t.....u.....v.....x.....y.....z...:

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33356
Entropy (8bit):	0.047616568017833996
Encrypted:	false
SSDEEP:	3:vd93llu/fllPv/NllP4tfllPC/NllPLltFllPktfllPxltFllP6QMRgSWbNFl/lu:PptqVGZ6vg9bNFlWCj/lI12El3n
MD5:	5F2E29B4F892060607110526C40FD1A3
SHA1:	AF00EFC0465B7C0481E917E86603A4412D3C2C2A
SHA-256:	969722A829653AEEB6F18DD8B39F109ECA223C9F813B16E69C1ACDCC4B5C05D7
SHA-512:	46BA32545F73BD006ABBF5B52568BC6AE1FD601E0F1899931FBB157663FCB4733C3FBEBFE03E61C2220935544FD6D62EBA5F64CD0B72B6C82BB9FDC5AC696F1
Malicious:	false
Reputation:	low
Preview:	.....%.DA..... ....

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:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.4760466022325405
Encrypted:	false
SSDEEP:	48:OZ8fKbGXBVfKTXfKOfKma7yfKmMufKr+8dbGfKrVefK4OfK4GfDbQSefgGbNrS0z:OqffVfwfFfVa7yfVMufsdbGfSefPOfPP
MD5:	98B5F388CE9730256E984744E1EEF852
SHA1:	C344B64D3425BA11BC2BD438EF7C5B40F713189C
SHA-256:	B96C02EA7F0D776039A4785D3B33E97065CD8FC9388CD2B3982806FD76167143
SHA-512:	B6B4E22BBB4D68A256428B82DA55E44A494A410EC899B9A3C5806ADF16184C795E41CCB4F8332AE16C5B03600D421DAE67152DE294DD5CEEA4AEA1C664BE8870
Malicious:	false
Reputation:	low
Preview:	.x.h...*.....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..780678000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-02-09 15:04:29.95][INFO][mr.Init] MR instance ID: a67c4374-1aa2-42cf-8bd6-b715a6c1937e\n","[2021-02-09 15:04:29.95][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-02-09 15:04:29.95][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-02-09 15:04:29.95][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-02-09 15:04:29.95][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-02-09 15:04:29.96][INFO][mr.CastProvider] Query enabled: true\n","[2021-02-09 15:04:29.96][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.140297048472326
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SSDEEP:	6:meenVq2PWXp+N23iKKdK8a2jMGIFUtp0YgZmwPVVSIkwOWXp+N23iKKdK8a2jMmd:jkva5Kk8EFUtp0h/PVVF5f5Kk8bJ
MD5:	E9CF0595A6BF1156BDD55F3EA20E4CEF
SHA1:	DBB006C70DD5EBF0DA0D4467F2E01F6772F0B2F7
SHA-256:	0C111FB517B94FAC3312C30D38A180B5762D3FFC048579B70AED64A1D01E69CD
SHA-512:	33151DCDD20810374BD458859BBB8792FB98C8E1C0DA6837A047035A5376D82057FE3578F349E27075AC6BD4DE392171555630DF8DF26E78D4383AF8595AF7DC
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:22.076 1090 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/02/09-15:04:22.080 1090 Recovering log #3.2021/02/09-15:04:22.081 1090 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
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):	49152
Entropy (8bit):	1.3063254171129688
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOQFh3fOqAuhjspnWOi8+XHFhylPOqAuhjspnWORVFoIa/OqAuhjsD:HZFh3XH8+XHFhylnwVFoP3X+A8Fo6ln
MD5:	CEE09EDE076878764B9AA12ED5D1B732
SHA1:	2C735AE88B3561550F2CFBBAD5C0CA4048937AAC
SHA-256:	18B9E0874B192A5E9295619976124981B4B8E15F8D1AF377875144ED695E22AD
SHA-512:	8753EE214D5A7F6372E3EE5251A03F81F5C5085A04CCB744D256E48F377821E22593B12502CC4B39A6B5A1CAD08F265ADD051E0FE0412930981FBCC676F804EE
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>...,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	51344
Entropy (8bit):	1.118593035370662
Encrypted:	false
SSDEEP:	96:xIUOqAuhjspnWOZmXFhfkOqAuhjspnWOL80OqAuhjspnWO1TVFoIrEOqAuhjspnu:iyfXFhfi5SqTVFosC1
MD5:	28F4F4D73D59E550CCFB62E664F2FE0F
SHA1:	544421634B78D7CD154F02FD14EB9E299D4DF108
SHA-256:	696703A3FEF4C0D854492236303990AD7937309672A6FF28DAA97FA9F67347BC
SHA-512:	B6247477207C5809615554F4E3922B2846ED1460C0C020C54E72D0FF653340D3BEF63F2756B8FE0A0E2088BBBC4A482C5243A0BC0FFD6FE6541902EF6C04D24C
Malicious:	false
Reputation:	low
Preview:	.....Y..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.235489548460162
Encrypted:	false
SSDEEP:	6:mQbi+q2PWXp+N23iKKdKgXz4rRIFUtpvLZmwPvKVkwOWXp+N23iKKdKgXz4q8LJ:fbi+va5KkgXiuFUtpvL/PvKV5f5KkgXS
MD5:	74C2F533AA49E2D87A7BE42513C91CB7
SHA1:	C186F2CED0A350E4DF004F9C98CCAAF52652F97F
SHA-256:	07E99BE4D543E1EFF6681B08C4F6EF025D02D42536C338CF848ABC75B62B9D3C
SHA-512:	075BB991B47F4C67E4AB8508B64F3E3F942A3ECB60A9C8E9BEF56A8A8F453B74FACB28CF85F6E0520B10837684CD7C7824577F3B96D639C4A0FC4990ABE941A2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Preview:	2021/02/09-15:04:22.394 159c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/02/09-15:04:22.397 159c Recovering log #3.2021/02/09-15:04:22.398 159c 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:	3:5ljljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.206803148777483
Encrypted:	false
SSDEEP:	6:m0Xot+q2PWXp+N23iKKdKrQMxIFUtpdBZmwPdRA3VkwOWXp+N23iKKdKrQMFLJ:FRva5KkCFUtpX/PQ5f5KktJ
MD5:	CA18242F05A7968E656CA31B0BCA3937
SHA1:	F7D9AF23FEAABEEE31F86F9BECCA70DC083478CF
SHA-256:	967CE8420533F169A8919BE23AA251C6D1E81A952A91433CF6A88DDD20CAEAEF
SHA-512:	608C5A649333973CF3A01B2A6BF53D84AAE6D2A3D2967B0FDEA7AAF43D059EB6E3097CEFAA813C8C322E75EB73A5F767021147B4D5C35424EEB9010671FA8696
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:22.272 568 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/02/09-15:04:22.273 568 Recovering log #3.2021/02/09-15:04:22.274 568 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\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.3665859992483425
Encrypted:	false
SSDEEP:	3:Q5QlePrEGBjuR+dqERaPq:QKeczE9
MD5:	C007317E66F9775B86FDABD3D1ED8495
SHA1:	093417FE07C28D42D1BFF4004C4FFD9771FE757F
SHA-256:	7DB8CB3BB32D74D45009D5C8C214ED88C38A842F3B0DC7C3ADB2CE19EF895860
SHA-512:	4C54B48B89ABFB488B18143192C565A16533A0ABD11FDD9E79558C51B0766E012ED40033118C7A491A290CCFC6718C4671677DEF15BCC81233F81C9C4473ABF
Malicious:	false
Reputation:	low
Preview:	..5..... 4acdab501b72f77a84af0ec82cc9a447.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.153988180675294
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SSDEEP:	6:maG+q2PWXp+N23iKKdK7Uh2ghZIFUtpbmZmwP/W3VkwOWXp+N23iKKdK7Uh2gnLJ:nG+va5KklhHh2FUtpbm/Pu3V5f5Kklh9
MD5:	A713734D87E750D32299BCEA3386929D
SHA1:	C27D6924385B7A3A9FBD7F6FC35EFC4380CD476B
SHA-256:	6C9437DB0BE876926359AE37DEC48C89B496C7D740AD9C1EBFFEED7D1D4E5D60
SHA-512:	9D8B2DE3A4AB1DEEA19866BEDC1944D2DE5737DC2EDC111550BD8D867D2D6891C62931BCE19E29ECBC457D74E6D989752223CE5917C1B6AAF2CE00BFFA64 6AD
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:22.039 72c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/02/09-15:04:22.044 72c Recovering log #3.2021/02/09-15:04:22.048 72c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Char acteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\806b53b5-432d-474e-8896-c81c2150adad.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\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):	427
Entropy (8bit):	5.275926505490745
Encrypted:	false
SSDEEP:	6:mQgeN+q2PWXp+N23iKKdKusNpV/2jMGIFUtpvG6ZmwPvctVkwOWXp+N23iKKdKux:fgeIva5KkFFUtpvd/Pvg5f5KkOJ
MD5:	565790841D5ADC3F90F089CC64B90E61
SHA1:	686077B451D0688D313FF4C50BB1D3098D0860E3
SHA-256:	BFB49CF62522C8B18EB53B6F3EC17146CFDC7C14484B3CA6B4567DA23F3D240A
SHA-512:	F0AC1A0729F8A546849D831379E4315C5453D4ED374A5D1F54924038410C6979020843C53125969B48BF9D806FFE65265744D8CF8D3BD5D4E08281B8E6624DF9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Preview:	2021/02/09-15:04:22.350 568 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/02/09-15:04:22.352 568 Recovering log #3.2021/02/09-15:04:22.353 568 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):	432
Entropy (8bit):	5.291118311453458
Encrypted:	false
SSDEEP:	6:mQIRq2PWXp+N23iKKdKusNpqz4rRIFUtpvdZmwPp5kwOWXp+N23iKKdKusNpqz4n:fOva5KkmiuFUtpvd/PL5f5Kkm2J
MD5:	0A7D3B89DA52B196CB9D072BC6B44732
SHA1:	55DBEBFCB29E5118FFD169AADAE3FD4C1DE29883
SHA-256:	D727CFCD1D58421746E0C80B7601A38DA552367302A6FEC3DC0465AA00DEE1FE
SHA-512:	55CEF288936971429600D8B145288360F6889431B6EAFAF9230BC1BA108E944E442A217D2985235C9D321E50713CFE958802BA58AE67BC5234DA0A19183BBDA0
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:22.397 1650 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/02/09-15:04:22.399 1650 Recovering log #3.2021/02/09-15:04:22.401 1650 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.276839913474813
Encrypted:	false
SSDEEP:	6:m1BaVSQyq2PWXp+N23iKKdKusNpZQMxIFUtp4TuRG1ZmwP4dQRkwOWXp+N23iKK+:oBaYVva5KkMFUtp40G1/P4dl5f5KkTJ
MD5:	9B4FE4066689ECDF7D6BB1B58AB47594
SHA1:	D4ADC346FE5ADDD9D89BBDB86CD6CC0D5BE6B6C4
SHA-256:	A88AE021073BCE22FBA657E07C7F3881542D6E9ED045D84BAED2F41F7B506F34
SHA-512:	B2EC98C07ED66AB85195921CAED55AB8BEC9E9314266220323CEE6DEBABA199D19FA0364B3FB58DB37D61094411FC61153933FEC4951B6C744057AC85695732
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:39.045 1630 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/02/09-15:04:39.046 1630 Recovering log #3.2021/02/09-15:04:39.047 1630 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\54c0d32b-b64d-4ac6-8909-bd7dffab1345.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\54c0d32b-b64d-4ac6-8909-bd7dffab1345.tmp	
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\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):	430
Entropy (8bit):	5.198594831102855
Encrypted:	false
SSDEEP:	12:US+va5KkkGHArBFUtpki/PkwV5f5KkkGHAryJ:Aa5KkkGgPgTf5KkkGga
MD5:	1C64A38B668DCCDB857ABAC653F2501D
SHA1:	B1C96419EE4F989A267575AC735C6F2A6394687F
SHA-256:	456561976FF47DB144731F5431C8B1106A36089618BEFF4D632BC94CB029B410
SHA-512:	D674545CB68808D449CD16EA83B7688271F557317BF4E73E84895E061F5E2447B6E4AFDE882E66029F8322F77A8B2866A0F5DD79BF53971647FA794B05A642E4
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:27.921 159c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/02/09-15:04:27.925 159c Recovering log #3.2021/02/09-15:04:27.927 159c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.257843730489965
Encrypted:	false
SSDEEP:	12:USbva5KkkGHArqiuFUtpkSR/PkSs5f5KkkGHArq2J:3a5KkkGgCgSf5KkkGg7
MD5:	2BE51F00F71EC5312043D6609230E8F2
SHA1:	1AD70D26DDE9E4B54405FB385BF7E1438B9DEF91
SHA-256:	6E09EF4C6CD6EF8F2D83F90E2E4A69CB7B24E60E3D52489D588F28E230DE20A0
SHA-512:	E1C4CD81B653E593D7254CAAACA17524C75D881BBD82452AE8A6EFB55B89B5FE24F670A2B5842A0F85FE8FDFBC90650F48E23572F84CA9C5935C03A2C6053F8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Preview:	2021/02/09-15:04:27.974 1644 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/02/09-15:04:27.975 1644 Recovering log #3.2021/02/09-15:04:27.976 1644 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.218236931906078
Encrypted:	false
SSDEEP:	12:ZVva5KkkGHArAFUtpqVG1/PdI5f5KkkGHArfJ:Da5KkkGgkgHOf5KkkGgV
MD5:	A4AE1768A6FDA1380CCB268BFCEC79CA
SHA1:	49EB9DD598144136AB563E572549DA1C50548836
SHA-256:	A8C53BC62CA6434E5753E54B5B5746EEF73465828C03BEA773CF0DD3D360CAA9
SHA-512:	B0B58E099C65451E2C89E10EBBD69DA743D121628B7D4F9E834C62F4B22FAD959236044F366E7C43784B41ADE7FC6E9DCA60D8361396BA92738FDA1C6C98E07
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:44.154 1630 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/02/09-15:04:44.157 1630 Recovering log #3.2021/02/09-15:04:44.158 1630 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:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.212966836875089
Encrypted:	false
SSDEEP:	6:mcF39+q2PWXp+N23iKKdKpIFUtpxCbJZmwPx1N9VkwOWXp+N23iKKdKa/WLJ:Qva5KkmFUtpe/PF5f5KkaUJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
MD5:	7DD3AFB0BBFB9912F09894777090221D
SHA1:	59BC61127C3831BC891545F4A6C7F1AFF5EA560F
SHA-256:	40C5C31898A718C435203FB0D19883E8A76AE39603B5832722DE8AA195EBFE43
SHA-512:	728A83B5A1547A1F54438E0EE7AE8E5D45CC5D04B97301D234502453ADD7EB50C408E9BB18E3C10ED654FAC43E583926AC1280B4F128CB689910C673CC01B47
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:22.052 1148 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/02/09-15:04:22.053 1148 Recovering log #3.2021/02/09-15:04:22.054 1148 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.346480078930533
Encrypted:	false
SSDEEP:	12:x+YVva5KkkOrsFUtpBhRG1/PBxYI5f5KkkOrzJ:x+ya5Kk+g727Df5Kkn
MD5:	12FEA9C261D6E4E55542F1AF5E3A6EA6
SHA1:	E0AFF7DD73A664A4F5B51A7206E378EFDA6FB16F
SHA-256:	1C62D466AA56BB06127F432156DFEF723D4204C5FF2B20571EBA30B3D77B3836
SHA-512:	63F577A4464AC907DDB21A6796CB12C9FCB6270518AF043886E42ABF5607AC4995E40D3BEB5E635D0FEAE2BCFA048ACFEE8F6A64384AFFB7E60AA57A33E65685
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:29.964 1630 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/02/09-15:04:29.966 1630 Recovering log #3.2021/02/09-15:04:29.967 1630 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\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.688721875540868
Encrypted:	false
SSDEEP:	3:VDanduF1X0AMAOg:VDsduF10qOg
MD5:	16C102032E2BF0456EFB6E87E5356027
SHA1:	C276B8B29B1D9A44EE5E5BB740D65699E872DB29
SHA-256:	7BB0A9036ABE24970B546A04229803DD7C3107486B8F6AB781F676798D5AB978
SHA-512:	8E9E33383A61578DF392E3D8EDD871C834D0CD2B3AF01B0C090BFED1D5DCC093B8DB2A153A3FD2052CD71E58FE1BA3637B7D6590C12519244636257D3314CB3
Malicious:	false
Reputation:	low
Preview:	....q..@.....rG.....vl.....ND3kSb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b09a5045-8a95-40de-8ceb-32b319b4289c.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):	22612
Entropy (8bit):	5.535750954133064
Encrypted:	false
SSDEEP:	384:MFrtZLlwiX831kXqKf/pUZNCgVLH2HfDhrUgHGjnTat8s4D:6LlxW1kXqKf/pUZNCgVLH2Hf9rUkGjnJ
MD5:	3FE5C6C36D07027F43098E7306A16304
SHA1:	0C4DC21E27DD398FF1A301E80A87772F24D8E4E5
SHA-256:	BC9EC5B56F67DD9000CBE450268C4FF2D9A94B9657EDDC2A9D205BBB63177D7B
SHA-512:	FCC792C8170C9A92D5B8F8A0C1401C2D0CA4E51C9A1AF8C053B769FAAD32CCDD1E233974A8BC5638E06B3118EBAC08E572E0EECCC06EA2AD38D42C8D789AC58
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b09a5045-8a95-40de-8ceb-32b319b4289c.tmp	
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":"13257385462049491","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b835b65e-20f3-4464-8424-2379eda66ff8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c96f8aed-5a5f-4066-8092-f14b18ceded0.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):	1374
Entropy (8bit):	5.582061435384344
Encrypted:	false
SSDEEP:	24:YytHUI6H0UhVsTG1KUeVO4y6B3UaDkq/HeUeXby2qUeXv77wUTHRUenHQ:YyZUI6UUhVseKUePUa4qPeUer2UefXwF
MD5:	213236B3374B7881769D745297E65AB8
SHA1:	0030DF4BC8C38A85F7F6F307495F34D3E4199211
SHA-256:	4CF6360BDDE92EAAE8E199BCB997A58B8DB921A92E8F7235902B8F442EB97AB5
SHA-512:	9D9118E60E69C0A35165BDAFF7CF0A9FD73323DE3BFBEE67161ACACAB9EF92CC3CBBC589588F518D181E3D45E0A21622BF034C9E189AF2FB09370103D190AA65
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1644447873.006809,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1612911873.006814},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1644447865.697998,"host":"xve7bFjiCcMHp3qspIgPuRL1YOnSznK/sMOCT6Xqjq4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612911865.698004},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obse

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
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):	4.512434109331244
Encrypted:	false
SSDEEP:	3:tUKoRkd11Zmwv3aRsXNkSV8saRs2UcXWSWGv:mOXZmwP/XNhVv/z+jtv
MD5:	94127B3A35A08EA623E45DE99F5B24CD
SHA1:	F0D1FD4B9ED157AEAAEAA68255A5478C578E0AB3
SHA-256:	C47B76EFD60CFA1F58F4756680A8DFDD90E5898F4D0EC45274AF804C445F40EB
SHA-512:	AC1E6C4E82C74B12444ECE55CAB4BB675919A734A164568292E6655599E1DE8866EE60BF16B90C4E23DBC7AAA50E98F32B153408A1507E006FA3ABB8F6BD5230
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:26.456 1928 Recovering log #3.2021/02/09-15:04:26.506 1928 Delete type=0 #3.2021/02/09-15:04:26.507 1928 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/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.206031644423989
Encrypted:	false
SSDEEP:	6:mkvq2PWXp+N23iKKdKfrzAdIFUtpBQZmwPBYkwOWXp+N23iKKdKfrzILJ:xvva5Kk9FUtpBQ/PBY5f5Kk2J
MD5:	29A565AA444BA6CC279F211195ED95F9
SHA1:	B7ECAFD9CE4A9D2D0E7A33511B7AB14C297C67C3
SHA-256:	485ADF87C229024E7307B1A3C57EC0E54157B89EB054572FA2A21DCDDCBEA852
SHA-512:	629F60666733F45458AB150B62BEFA282C19653A1F64B51D4219A40D7697615960B5DD20516C301F12212063E0650BC0C068B27A188500BD018A9478418A3C8A
Malicious:	false
Reputation:	low
Preview:	2021/02/09-15:04:29.031 1644 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/02/09-15:04:29.033 1644 Recovering log #3.2021/02/09-15:04:29.033 1644 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\c0c6180b-b34b-4560-a1a9-42bd758beb95.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7441322566521777
Encrypted:	false
SSDEEP:	384:rLYXn9aENlKb2Njrov/l3IXdEHNkGkTrOJTfx4p59YrSvmKtKVrbLUOxZDNG1jCR:Qa1VShk0ceL/RBQXfONKPFrZj
MD5:	8968C8FA00F0CDB20F50C38266E092F6
SHA1:	C459B0BA46B1A5F00581506F596737D18C85BC83
SHA-256:	5273418E99671A4D0DB7A0A47043CB508A20A368CC42E5B77D6389D52C92EA3F
SHA-512:	0C5089DF47B30DBDFCFB146C59E1824C883EACA8861D73DE9EB40363426306B2D9A572D76A39C17F1D13DB4C6583890C7F5C43F98B245DBBD46514D956592C
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.../18.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\Temp\8c825e67-be3d-4c50-b6e6-e9fd5310c7c4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59(
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./ ?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o..,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\9504e688-7584-419a-b709-0f96d2a78997.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\a48800a1-00ef-4cc9-8dda-04a634949a3f.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\c8db6bd9-836d-4cb1-86a7-19eadf8d4161.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L]....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..I.6r[yU...%..f.....N..V.....<+.....I..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\8c825e67-be3d-4c50-b6e6-e9fd5310c7c4.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

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\8c825e67-be3d-4c50-b6e6-e9fd5310c7c4.tmp	
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L\....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "14284488690781267 31": {.. "message": ".... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "....".. },.. "16366867476874943 76": {.. "message": "... ...".. },.. "18027627465894571 77": {.. "message": "...".. },.. "18503975003120203 88": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\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:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": ".. .. ..".. },.. "12827687646031907 5": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "...".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": "..... .....".. },.. "18503975003120203 88": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\bg\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "155090464710828958": {.. "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_dir5152_1022280208\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:lPswlWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4 C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ... .".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE 1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522 140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\cs\messages.json	
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_dir5152_1022280208\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\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

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\el\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": "....... .. }.. "12139579827238759 20": {.. "message": ".... ... .;".. }.. "1282768 76460319075": {.. "message": "..... .... }.. "14284488690781267 31": {.. "message": "..... ....." .. }.. "15221406833188603 51": {.. "message": "..... ...." .. }.. "15509040647108289 58": {.. "message": "....." .. }.. "16366867476874943 76": {.. "message": "..... ...." .. }.. "18503975003120203 88": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Freezes".. }.. "12139579827238759 20": {.. "message": "Which of the following best describes your network?".. }.. "12827687646031907 5": {.. "message": "Device Discovery".. }.. "14284488690781267 31": {.. "message": "Video Smoothness".. }.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. }.. "15509040647108289 58": {.. "message": "Smooth".. }.. "16366867476874943 76": {.. "message": "Perfect".. }.. "18027627465894571 77": {.. "message": "Volume".. }.. "18503975003120203 88": {.. "message": "Are you able to see your Chrom ecast 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_dir5152_1022280208\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:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71E EEE
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205 17": {.. "message": "Congelaci.n de im.genes".. }.. "12139579827238759 20": {.. "message": ".Cu.l de las siguientes respuestas descr ibe mejor tu red?".. }.. "12827687646031907 5": {.. "message": "Detecci.n de dispositivo".. }.. "14284488690781267 31": {.. "message": "Fluidez del v.deo".. }.. "15221406833188603 51": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. }.. "15509040647108289 58": {.. "message": "V.deo fluido".. }.. "16366867476874943 76": {.. "message": "Perfecta".. }.. "18027627465894571 77": {.. "message": "Volumen".. }.. "18503975003120203 88": {.. "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_dir5152_1022280208\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:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB1120272356 6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\et\messages.json	
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_dir5152_1022280208\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "1282768764603190 75": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... .... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\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?".. },.. "1282768764603190 75": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "1522140683318860351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\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

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\fil\messages.json	
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_dir5152_1022280208\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
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".. },.. "1636686747687494376": {.. "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_dir5152_1022280208\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": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\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": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\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".. },.. "1636686747687494376": {.. "message": "Savr.ena".. },.. "1802762746589457177": {.. "message": "Glasno.a".. },.. "1850397500312020388": {.. "message": "Vidite li svoj Chromecast u $START_LINK$aplikaciji Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\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_dir5152_1022280208\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_dir5152_1022280208\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

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\it\messages.json	
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_dir5152_1022280208\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16519
Entropy (8bit):	5.675556017051063
Encrypted:	false
SSDEEP:	192:nkprPhQdxkRWrZe1wYpMR5wnAV6c8TEKdl:YrLRWri65wAV6uml
MD5:	6F2CC1A6B258DF45F519BA24149FABDC
SHA1:	8A58C7880C6D22765DCBB6BCE22A192C1B109AE1
SHA-256:	42ECFEE727CFC4F2845FEFDACE5EDC2E0A40AFAD69973A3B950CE653A7633342
SHA-512:	F7454F0E14301C59CC54361ACC0A1C6D072EF9BDF5DEA60646FB90B1CE47612785938C784A4CF1DE3E62648A14420374933B5F5DA43907BC00D3799FF163A3D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "...".. },.. "1213957982723875920": {.. "message": "..... ".. },.. "128276876460319075": {.. "message": "..... ".. },.. "1428448869078126731": {.. "message": "..... ".. },.. "1522140683318860351": {.. "message": "..... ".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..".. },.. "1850397500312020388": {.. "message": "$START_LINK$Google Home ...END_LINK. Chromecast .....$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\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:	DF8BC9E577D3ECB0E6C303E1D2C9E9A4A8317CAE810A9DFC88D91B373A4B665722C5A9AB5A589BB947FDA4C7CD9A6DF39DDD13EA47FE9EFF7E0AC43E49FF3479
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..... .....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... $

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\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

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\ko\messages.json	
MD5:	E303CD63AD00EB3154431DED78E871C4
SHA1:	3B1E5B8E2CF5EBDF5D33656EF80A46563F751783
SHA-256:	FDE602BFDB1AFD282682DA5338C4F91D8A2F6CB5411DB8F62F4583D629CE67A6
SHA-512:	18BA1D5A25FBC1829AD957A531B0CC490AFCBD20AC22181021363AA3CFB916270B8732E824463C9B0897220E8AE86EB1BE561D6540E6C625F08F228F61DDFFA
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "...".. },.. "1213957982723875920": {.. "message": ".. . .. .?".. },.. "128276876460319075": {.. "message": ".. ..".. },.. "142844869078126731": {.. "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_dir5152_1022280208\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15802
Entropy (8bit):	5.354550839818046
Encrypted:	false
SSDEEP:	192:lGxSprfkiRR+2zJckS1khrnPI85+80p3DWReV6c8TEKdl:lG4rlq0OkSmhrwbpIeV6uml
MD5:	93BBBE82F024FBCB7FB18E203F253429
SHA1:	83F4D80F64FA2ADCE6C515C5F663BD38A76C51DB
SHA-256:	E7A8570922CCC4F2CA3721C4E61F426158C4E7BC90274FBC8BE4040FF8B6CA9B
SHA-512:	B7E7878106B466CE95069141DF1DE387E847348B62E9C4D548006452F3E164B3AD842E9673A56DC011A5ECC3346B5863E2034EE477A9D1F3E0ABD76B2D0F640A
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Stringa".. },.. "1213957982723875920": {.. "message": "Kuris i. toliau pateikt. teigini. geriausiai apib.dina j.s. tinkl. ?".. },.. "128276876460319075": {.. "message": ".renginio suradimas".. },.. "142844869078126731": {.. "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_dir5152_1022280208\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".. },.. "142844869078126731": {.. "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_dir5152_1022280208\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

C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\ml\messages.json	
SHA-512:	DD1711B017DC65E1272972A1BEBD7A1B1769E1F22B37B20582573392CD432725D19DCE134145B3C031428BC0B5948B02A9AA93C8A651BEAA189B686B7BC2AD4
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ....".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message"

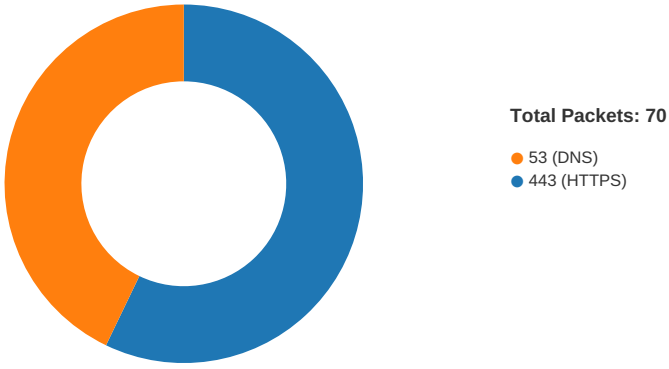
C:\Users\user\AppData\Local\Temp\scoped_dir5152_1022280208\CRX_INSTALL_locales\mr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19628
Entropy (8bit):	5.311054092888986
Encrypted:	false
SSDEEP:	192:PbrpprGy+RmIosTmidpzlF1Akk03LQYOkQrjNjP8hZYiEQ5z+excV6c8TEKdl:PbfrGUIos7dpzxbP7KrjNjaBEYuV6uml
MD5:	659F5B4ACA112D3ECBB6EC1613DDE824
SHA1:	5DEE35FCD260554999F8DDEC489FBA9F81FA8EEE
SHA-256:	C8B765E7A07578BC078A952E151E3B866506959E15E79E9E5E1DBB98F9C4008F
SHA-512:	F74B36C1B6160E444F4969D13788A9C60637BDC11DC5065B2518B668E8D638384E00557ACDC88B3EA225D9231B6BED4B227BFB2E12C92773073B256F62ADDE6
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".... ....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "..... $START_LINK$ Goo

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 15:04:26.428302050 CET	49729	443	192.168.2.3	141.125.73.152
Feb 9, 2021 15:04:26.480618000 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:26.480715036 CET	49729	443	192.168.2.3	141.125.73.152

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 15:04:26.481297016 CET	49729	443	192.168.2.3	141.125.73.152
Feb 9, 2021 15:04:26.533524990 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:26.542013884 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:26.542038918 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:26.542056084 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:26.542123079 CET	49729	443	192.168.2.3	141.125.73.152
Feb 9, 2021 15:04:26.578691959 CET	49729	443	192.168.2.3	141.125.73.152
Feb 9, 2021 15:04:26.631396055 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:26.632379055 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:26.632901907 CET	49729	443	192.168.2.3	141.125.73.152
Feb 9, 2021 15:04:26.721596956 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:26.721620083 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:26.721628904 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:26.721750021 CET	49729	443	192.168.2.3	141.125.73.152
Feb 9, 2021 15:04:26.896795988 CET	49729	443	192.168.2.3	141.125.73.152
Feb 9, 2021 15:04:26.990612030 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:27.001468897 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:27.001497030 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:27.001507998 CET	443	49729	141.125.73.152	192.168.2.3
Feb 9, 2021 15:04:27.001590967 CET	49729	443	192.168.2.3	141.125.73.152
Feb 9, 2021 15:04:27.041624069 CET	49729	443	192.168.2.3	141.125.73.152
Feb 9, 2021 15:04:27.642232895 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.687566996 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.687813044 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.688122034 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.733354092 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.747503996 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.747548103 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.747570038 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.747591972 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.747704029 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.747750044 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.773427010 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.773688078 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.773874998 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.817933083 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.818186045 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.818291903 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.818361998 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.820061922 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.820087910 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.820111990 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.820146084 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.820173025 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.820204973 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.823352098 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.823375940 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.823482990 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.826694012 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.826785088 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.826864004 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.826970100 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.829041004 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.829066992 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.829195023 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.832268000 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.832298994 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.832362890 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.832396984 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.861738920 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.861766100 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.861924887 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.863248110 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.863279104 CET	443	49738	172.217.23.33	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 15:04:27.863388062 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.866501093 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.866537094 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.866647959 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.869673014 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.869707108 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.869810104 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.872850895 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.872955084 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.873011112 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.876096964 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.876126051 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.876245975 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.879307032 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.879338980 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.879465103 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.882580042 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.882611990 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.882744074 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.885742903 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.885775089 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.885871887 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.888649940 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.888684034 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.888875961 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.891614914 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.891650915 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.891761065 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.894620895 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.894648075 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.894731998 CET	49738	443	192.168.2.3	172.217.23.33
Feb 9, 2021 15:04:27.897548914 CET	443	49738	172.217.23.33	192.168.2.3
Feb 9, 2021 15:04:27.897578001 CET	443	49738	172.217.23.33	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 15:04:17.824954987 CET	50141	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:17.885339022 CET	53	50141	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:18.805680037 CET	53023	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:18.854317904 CET	53	53023	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:19.995827913 CET	49563	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:20.047398090 CET	53	49563	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:23.440064907 CET	51352	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:23.492533922 CET	53	51352	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:25.264909983 CET	58823	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:25.311798096 CET	57568	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:25.313445091 CET	53	58823	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:25.315025091 CET	50540	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:25.325314999 CET	54366	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:25.329272985 CET	53034	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:25.378259897 CET	53	57568	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:25.387149096 CET	53	54366	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:25.396290064 CET	53	53034	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:25.403817892 CET	53	50540	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:25.835272074 CET	57762	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:25.896285057 CET	53	57762	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:25.998034954 CET	55435	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:26.046838999 CET	53	55435	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:26.355093002 CET	56132	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:26.424168110 CET	53	56132	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:26.613208055 CET	58987	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:26.664593935 CET	53	58987	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:27.144319057 CET	56579	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 15:04:27.214484930 CET	53	56579	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:27.563344002 CET	60633	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:27.623440981 CET	53	60633	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:28.043884039 CET	61292	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:28.100975037 CET	53	61292	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:30.314728975 CET	64910	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:30.384463072 CET	53	64910	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:31.600347996 CET	52123	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:31.650805950 CET	53	52123	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:32.084345102 CET	56130	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:32.150090933 CET	53	56130	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:32.914441109 CET	56338	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:32.974226952 CET	53	56338	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:34.351305008 CET	63978	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:34.419290066 CET	53	63978	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:40.745537996 CET	55708	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:40.808464050 CET	53	55708	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:43.643877983 CET	56803	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:43.692543030 CET	53	56803	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:44.560827971 CET	57145	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:44.620872021 CET	53	57145	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:49.754759073 CET	55359	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:49.814285040 CET	53	55359	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:50.363092899 CET	58306	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:50.414685011 CET	53	58306	8.8.8.8	192.168.2.3
Feb 9, 2021 15:04:51.319590092 CET	64124	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:04:51.378037930 CET	53	64124	8.8.8.8	192.168.2.3
Feb 9, 2021 15:05:06.698889017 CET	49361	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:05:06.752331018 CET	53	49361	8.8.8.8	192.168.2.3
Feb 9, 2021 15:05:06.858405113 CET	63150	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:05:06.906999111 CET	53	63150	8.8.8.8	192.168.2.3
Feb 9, 2021 15:05:10.687519073 CET	53279	53	192.168.2.3	8.8.8.8
Feb 9, 2021 15:05:10.751154900 CET	53	53279	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 9, 2021 15:04:25.315025091 CET	192.168.2.3	8.8.8.8	0x8f8	Standard query (0)	894f2824690f4f688cb014399e893234.svc.dynamics.com	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:26.355093002 CET	192.168.2.3	8.8.8.8	0xee75	Standard query (0)	32273976467384105930.eu-gb.cf.appdomain.cloud	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:27.563344002 CET	192.168.2.3	8.8.8.8	0xd89a	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:32.084345102 CET	192.168.2.3	8.8.8.8	0x2835	Standard query (0)	47410795723635106367.eu-gb.cf.appdomain.cloud	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:40.745537996 CET	192.168.2.3	8.8.8.8	0x6022	Standard query (0)	47410795723635106367.eu-gb.cf.appdomain.cloud	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 9, 2021 15:04:25.403817892 CET	8.8.8.8	192.168.2.3	0x8f8	No error (0)	894f2824690f4f688cb014399e893234.svc.dynamics.com	mktsvcp102wu001.svc.dynamics.com		CNAME (Canonical name)	IN (0x0001)
Feb 9, 2021 15:04:25.403817892 CET	8.8.8.8	192.168.2.3	0x8f8	No error (0)	mktsvcp102wu001.svc.dynamics.com	mktsvcp102wu001.westus2.cloudapp.azure.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 9, 2021 15:04:26.424168110 CET	8.8.8.8	192.168.2.3	0xee75	No error (0)	3227397646 7384105930.eu-gb.cf. appdomain. cloud		141.125.73.152	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:26.424168110 CET	8.8.8.8	192.168.2.3	0xee75	No error (0)	3227397646 7384105930.eu-gb.cf. appdomain. cloud		158.176.79.200	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:26.424168110 CET	8.8.8.8	192.168.2.3	0xee75	No error (0)	3227397646 7384105930.eu-gb.cf. appdomain. cloud		158.175.115.200	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:27.623440981 CET	8.8.8.8	192.168.2.3	0xd89a	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.googleuserc ontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 9, 2021 15:04:27.623440981 CET	8.8.8.8	192.168.2.3	0xd89a	No error (0)	googlehost ed.l.googl euserconte nt.com		172.217.23.33	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:32.150090933 CET	8.8.8.8	192.168.2.3	0x2835	No error (0)	4741079572 3635106367.eu-gb.cf. appdomain. cloud		158.176.79.200	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:32.150090933 CET	8.8.8.8	192.168.2.3	0x2835	No error (0)	4741079572 3635106367.eu-gb.cf. appdomain. cloud		141.125.73.152	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:32.150090933 CET	8.8.8.8	192.168.2.3	0x2835	No error (0)	4741079572 3635106367.eu-gb.cf. appdomain. cloud		158.175.115.200	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:40.808464050 CET	8.8.8.8	192.168.2.3	0x6022	No error (0)	4741079572 3635106367.eu-gb.cf. appdomain. cloud		141.125.73.152	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:40.808464050 CET	8.8.8.8	192.168.2.3	0x6022	No error (0)	4741079572 3635106367.eu-gb.cf. appdomain. cloud		158.176.79.200	A (IP address)	IN (0x0001)
Feb 9, 2021 15:04:40.808464050 CET	8.8.8.8	192.168.2.3	0x6022	No error (0)	4741079572 3635106367.eu-gb.cf. appdomain. cloud		158.175.115.200	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 9, 2021 15:04:26.542056084 CET	141.125.73.152	443	192.168.2.3	49729	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 9, 2021 15:04:32.266958952 CET	158.176.79.200	443	192.168.2.3	49751	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:32.267683983 CET	158.176.79.200	443	192.168.2.3	49752	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:32.640950918 CET	158.176.79.200	443	192.168.2.3	49754	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:32.641457081 CET	158.176.79.200	443	192.168.2.3	49755	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:41.195385933 CET	141.125.73.152	443	192.168.2.3	49773	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 9, 2021 15:04:41.195502043 CET	141.125.73.152	443	192.168.2.3	49774	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:41.661623955 CET	141.125.73.152	443	192.168.2.3	49776	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:41.661688089 CET	141.125.73.152	443	192.168.2.3	49775	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:41.999908924 CET	141.125.73.152	443	192.168.2.3	49779	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:42.364615917 CET	141.125.73.152	443	192.168.2.3	49784	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 9, 2021 15:04:42.557046890 CET	141.125.73.152	443	192.168.2.3	49787	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:42.798389912 CET	141.125.73.152	443	192.168.2.3	49788	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:43.011092901 CET	141.125.73.152	443	192.168.2.3	49789	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:43.039760113 CET	141.125.73.152	443	192.168.2.3	49790	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 9, 2021 15:04:43.273785114 CET	141.125.73.152	443	192.168.2.3	49792	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 9, 2021 15:04:43.455915928 CET	141.125.73.152	443	192.168.2.3	49793	CN=*.eu-gb.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5152 Parent PID: 2128

General

Start time:	15:04:21
Start date:	09/02/2021
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://894f2824690f4f688cb014399e893234.svc.dynamics.com/t/r/vb3XY_VLx7l-xHga3YHy8JRbFYUbDDzXt6qsDcUtzO0#covid19@rztienen.be'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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: 1364 Parent PID: 5152

General

Start time:	15:04:22
Start date:	09/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,17904341760629683302,5698386004384518543,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1684 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly