ID: 358600
Cookbook: browseurl.jbs
Time: 22:20:15
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright null 2021

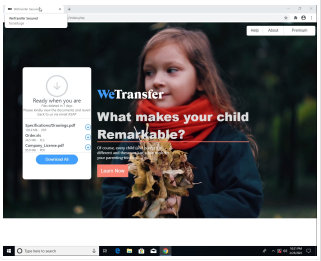
Analysis Report https://bss.edu.ge/transdoc/index.php

Overview

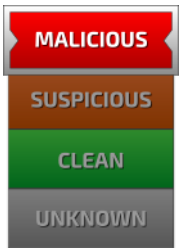
General Information

Sample URL:	http://https://bss.edu.ge/transdoc/index.php
Analysis ID:	358600
Infos:	

Most interesting Screenshot:



Detection

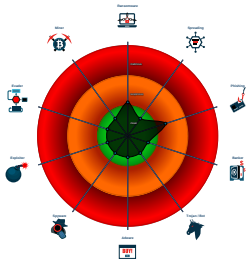


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5708 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://bss.edu.ge/transdoc/index.php' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 400 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1548,12077504496802862364,11838693349827509473,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1720 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6732 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1548,12077504496802862364,11838693349827509473,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=4572 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

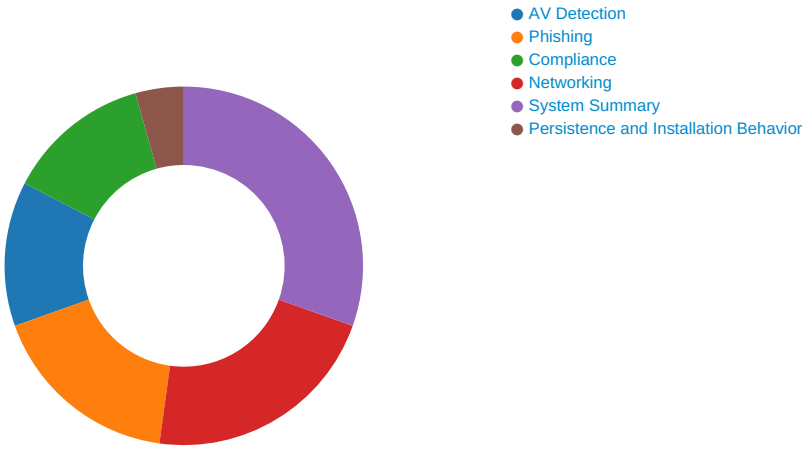
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright null 2021



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Compliance:

Creates a directory in C:\Program Files

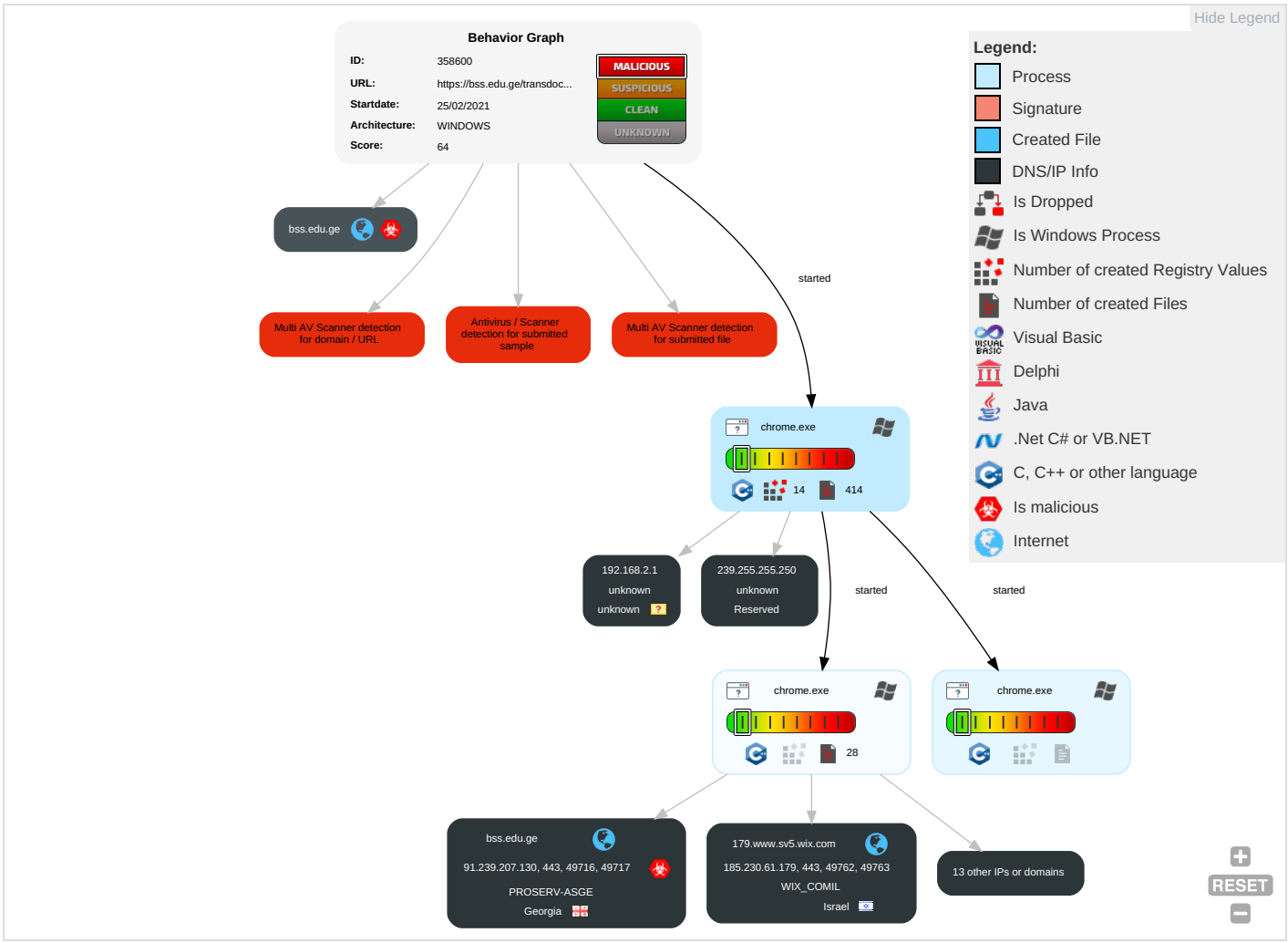
Creates license or readme file

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

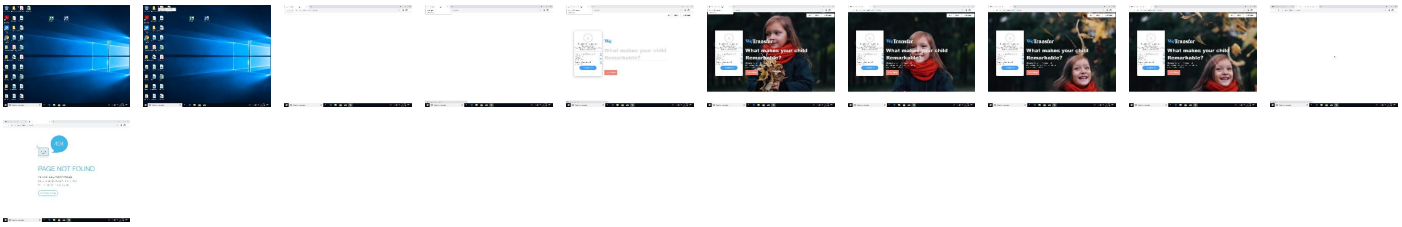
Behavior Graph

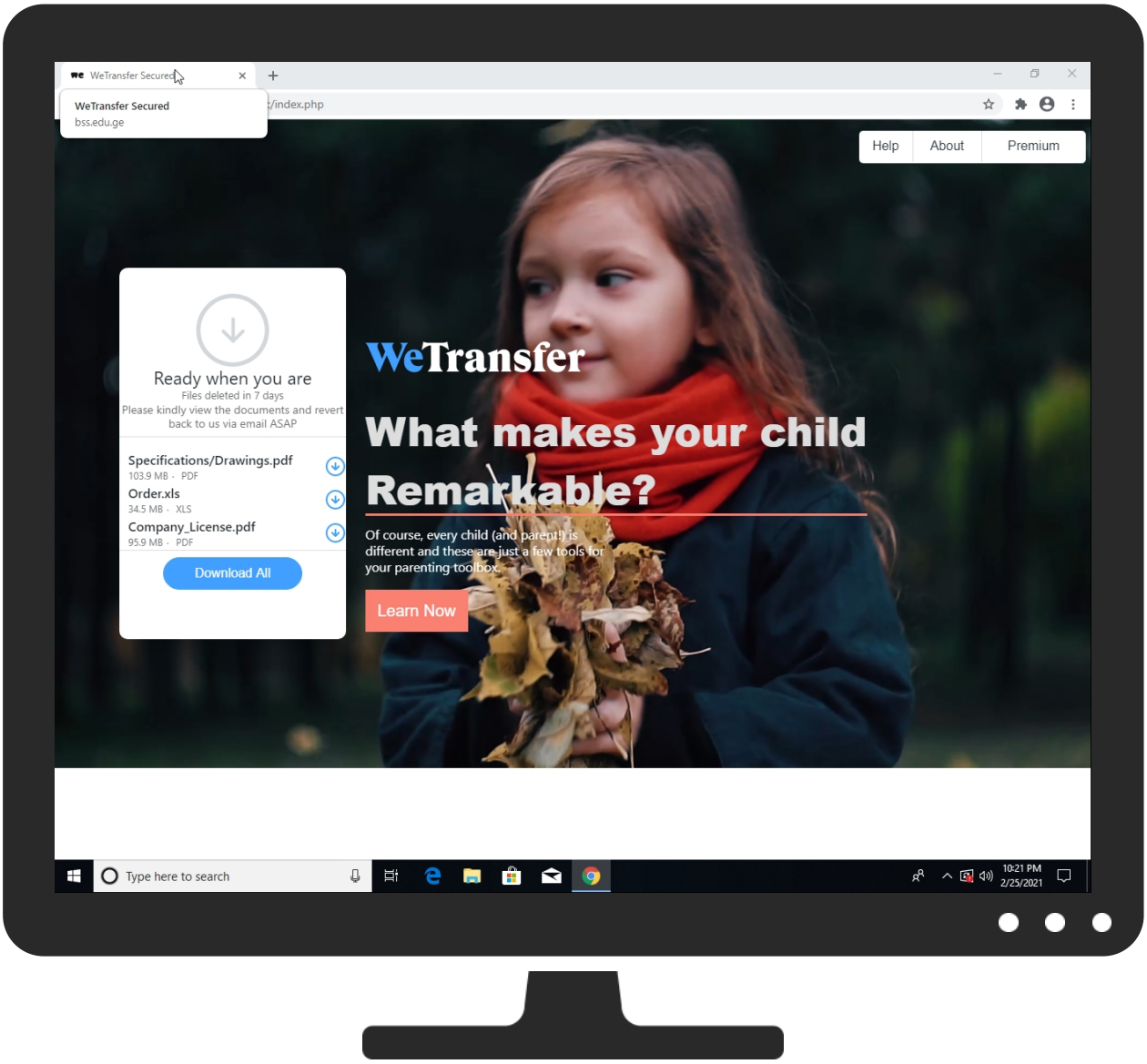


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://bss.edu.ge/transdoc/index.php	17%	Virustotal		Browse
http://https://bss.edu.ge/transdoc/index.php	100%	Avira URL Cloud	phishing	
http://https://bss.edu.ge/transdoc/index.php	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bss.edu.ge	6%	Virustotal		Browse
td-balancer-euw2-6-109.wixdns.net	0%	Virustotal		Browse
www.besproutable.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://besproutable.com/#&	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://bss.edu.ge/transdoc/js/jquery.js	0%	Avira URL Cloud	safe	
http://https://besproutable.com/	0%	Avira URL Cloud	safe	
http://https://www.besproutable.com	0%	Avira URL Cloud	safe	
http://https://bss.edu.ge/	0%	Avira URL Cloud	safe	
http://https://bss.edu.ge/transdoc/index.php2	0%	Avira URL Cloud	safe	
http://https://bss.edu.ge/transdoc/index.phpj	0%	Avira URL Cloud	safe	
http://https://besproutable.com/z	0%	Avira URL Cloud	safe	
http://https://bss.edu.ge/transdoc/index.phpWeTransfer	0%	Avira URL Cloud	safe	
http://https://bss.edu.ge/transdoc/files/icon.ico	0%	Avira URL Cloud	safe	
http://https://bss.edu.ge/transdoc/js/main.js	0%	Avira URL Cloud	safe	
http://https://bss.edu.ge/3Fp	0%	Avira URL Cloud	safe	
http://https://www.besproutable.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
td-static-34-96-106-200.parastorage.com	34.96.106.200	true	false		high
bss.edu.ge	91.239.207.130	true	true	• 6%, Virustotal, Browse	unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false	• 0%, Virustotal, Browse	unknown
179.www.sv5.wix.com	185.230.61.179	true	false		high
googlehosted.l.googleusercontent.com	142.250.184.65	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
www.besproutable.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
static.parastorage.com	unknown	unknown	false		high
www.wix.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bss.edu.ge/transdoc/index.php	true		unknown
http://https://www.besproutable.com/parent	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.wix.com	b95d7805-2ce1-4c24-b76e-637f789cb07b.tmp.1.dr	false		high
http://https://besproutable.com/#&	144cec94ba301c81_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	fb99c5d0-98fb-4f26-995f-fc86ec110386.tmp.1.dr, 8a298803-9696-48aa-a669-7aab15c93704.tmp.1.dr, b95d7805-2ce1-4c24-b76e-637f789cb07b.tmp.1.dr, 8758eb93-0677-4c65-9314-fa0988e0fe7c.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bss.edu.ge/transdoc/js/jquery.js	9673e3d884304536_0.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://bss.edu.ge/transdoc/index.php	Current Session.0.dr, Favicons.0.dr	true		unknown
http://https://static.parastorage.com	b95d7805-2ce1-4c24-b76e-637f789cb07b.tmp.1.dr	false		high
http://https://www.wix.com/	Network Action Predictor.0.dr	false		high
http://https://static.parastorage.com/services/third-party/angular-translate/1.1.1/angular-translate.min.js	2e5a7a718962a8ab_0.0.dr	false		high
http://https://besproutable.com/	2e5a7a718962a8ab_0.0.dr, 41f0a85b681a4673_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.besproutable.com	b95d7805-2ce1-4c24-b76e-637f789cb07b.tmp.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.jsdelivr.net	b95d7805-2ce1-4c24-b76e-637f789cb07b.tmp.1.dr	false		high
http://https://static.parastorage.com/services/wix-public/1.299.0/scripts/error-pages/app.js	144cec94ba301c81_0.0.dr	false		high
http://https://static.parastorage.com/services/third-party/angularjs/1.2.28/angular.min.js	41f0a85b681a4673_0.0.dr	false		high
http://https://bss.edu.ge/	948ef966964219be_0.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://bss.edu.ge/transdoc/index.php2	History Provider Cache.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://static.parastorage.com/services/third-party/jquery/2.0.3/jquery.min.js	4f54a2bfeccad0b1_0.0.dr	false		high
http://https://static.parastorage.com/	Network Action Predictor.0.dr	false		high
http://https://bss.edu.ge/transdoc/index.phpj	Current Session.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	fb99c5d0-98fb-4f26-995f-fc86ec110386.tmp.1.dr, b95d7805-2ce1-4c24-b76e-637f789cb07b.tmp.1.dr	false		high
http://https://besproutable.com/z	f08086ba5cc99bb1_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://bss.edu.ge/transdoc/index.phpWeTransfer	History.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://bss.edu.ge/transdoc/files/icon.ico	Favicons.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://bss.edu.ge/transdoc/js/main.js	948ef966964219be_0.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.besproutable.com/parent	Current Session.0.dr	false		unknown
http://https://bss.edu.ge/3Fp	9673e3d884304536_0.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://www.besproutable.com/	Network Action Predictor.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.184.65	unknown	United States		15169	GOOGLEUS	false
185.230.61.179	unknown	Israel		58182	WIX_COMIL	false
34.96.106.200	unknown	United States		15169	GOOGLEUS	false
91.239.207.130	unknown	Georgia		47810	PROSERV-ASGE	true
239.255.255.250	unknown	Reserved		unknown	unknown	false
35.246.6.109	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:	358600
Start date:	25.02.2021
Start time:	22:20:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://bss.edu.ge/transdoc/index.php
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:	20
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:	mal64.win@34/183@7/8
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.besproutable.com/parent

Copyright null 2021

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): 52.255.188.83, 13.88.21.125, 168.61.161.212, 104.43.193.48, 216.58.208.142, 142.250.180.77, 216.58.205.78, 173.194.187.170, 2.20.142.209, 2.20.142.210, 74.125.173.39, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 142.250.180.163, 216.58.206.42, 142.250.184.42, 142.250.184.106, 216.58.205.74, 142.250.180.74, 142.250.180.106, 142.250.180.138, 216.58.208.170, 216.58.209.42, 51.104.139.180, 23.218.208.56, 20.54.26.129, 216.58.208.131, 74.125.173.28, 216.58.208.163, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, clientservices.googleapis.com, r6.sn-4g5e6nld.gvt1.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, r1---sn-4g5e6nlk.gvt1.com, clients2.google.com, redirector.gvt1.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, dualstack.f3.shared.global.fastly.net, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, r5.sn-4g5e6nz7.gvt1.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, www.googleapis.com, r1.sn-4g5e6nlk.gvt1.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, r6---sn-4g5e6nld.gvt1.com, r5---sn-4g5e6nz7.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:21:05	API Interceptor	1x Sleep call for process: chrome.exe modified

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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0765536003145497
Encrypted:	false
SSDEEP:	6:kKf2bqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:3f3kPlE99SNxAhUeo+aKt
MD5:	2DBB6F6881ED22588007C4AF5361CE70
SHA1:	0C3DC0728B0F6CC635F88A4377178AF9370080CB
SHA-256:	1BC53EFF7F8F5E5D3A77A20BCD36436D063074C750F69E49FC6A013F6CC1648D
SHA-512:	048DC10A032E4DDFA3620F987CC48E27B6EADEC8808837346AB715EC6514D743F1A0304A684DD6CC9EE0D90A9921BF3FFA91FC3A4B7D1947FF7633FE4511044
Malicious:	false
Reputation:	low
Preview:	p..... .....d.....(..... .....&.....h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\38a0add5-2680-4d80-b2f1-faa4abadee6f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7472103415700206
Encrypted:	false
SSDEEP:	384:VrBS/TRi8Z25lVu0jaNLrQvnt3wP1QHJoG8rrWB3DxQVVVEreXmeJCtTnzIOdNHn:3Z+qFVOpksgevLZJkn7qxKXJD19
MD5:	89D43A78BFF46B2561B11A2D098569C0
SHA1:	28002967C1261A4A4B8227B3E982E03B9341A01F
SHA-256:	AB5DB6BED52F9066C46CA326DAB7E5DFBE767519515B2BB52014367907790D5C
SHA-512:	B7D1D36DA2762BA35FB412043B4202448478D3791DAFA524A8C29FF39F29B015355A30099B583B3D782AF48788CAB588D8F7F0D07E36F2D8EB2FF7A78AFCBF6E
Malicious:	false
Reputation:	low
Preview:	.q.....*...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....28.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\4004f49b-b922-4a78-a12e-fbc23226d638.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):	164950
Entropy (8bit):	6.0816814364383225
Encrypted:	false
SSDEEP:	3072:u66smGflW7LtsevCLxZJasImhjp3qm4JaPlrnZFcbXafIB0u1GOJmA3iuRa:f9flkhsXNZswa2b3aqfllUOoSiuRa
MD5:	2E9BD370D2D66CDA028A78567ABB6F3E
SHA1:	16C6D233E977AB0EB0C312FEB7A17D82DE14D03D
SHA-256:	05B1E276AB3B4616C0D2F0D3C82E855B78B9464DCC4534AD6A024DB4CF0A72F0
SHA-512:	3563C77D17B32E5266058BE053985792F7069FCC97F684903B789D3C4E412EEF3CD013678DB7F5A8CDA0FD3D65A96BCFD4A8C1AFFC79BF0BB441D3B729065C2E
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":1.614320464860994e+12,"network":1.614288066e+12,"ticks":95878702.0,"uncertainty":4595785.0}},"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\83d55b35-ec27-48d7-bb1d-0ed1be4ff4ca.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.746268349442211
Encrypted:	false
SSDEEP:	384:jrBS/TRi815+jaNLrQvnt3wP1QHJoG8rrWB3DxQVVVEreXmeJCtTnzIOdNHNi1r8:J6qFVOpksgevLZJkn7qxKXJD1L

C:\Users\user\AppData\Local\Google\Chrome\User Data\83d55b35-ec27-48d7-bb1d-0ed1be4ff4ca.tmp	
MD5:	4BAAD5DE66CB34CD086CAF88ACD7C240
SHA1:	F452136993B4C079EB0DA8ADCE36D892655FFFCF
SHA-256:	453F41673F7DD6271207C42C62416689E48A19D8A6218700021139F9C1F49F0B
SHA-512:	68D969CBCDD1B4CC5BF15B224BDC7AEBBF50730B6D0E175FB649307F3215518F8BBCA2C4B97F282F1FF8FA9ECBE7FE276D77D2417489CAD8220A4C0C377516 3E
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....28.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\92e1f1ce-9e0c-4361-a6b0-d34524fbbc1b.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):	156470
Entropy (8bit):	6.051075868032443
Encrypted:	false
SSDEEP:	3072:bsmGflW7LtsevCLxZJasImhjp3qm4JaPlrnZFcbXafIB0u1GOJmA3iuRa:aflkhsXNZswa2b3aqfIlUOoSiuRa
MD5:	28EFBC4E9FD227AFAE195FFA492586B7
SHA1:	EC4032E31DDE98B8F88B3E6F51D5EA359CEE20E5
SHA-256:	E3ED1A96CB88CCE111A01669FE6D7478BAF0139B79DCD17D9B361265AE67C436
SHA-512:	173E5A8349618FE0D03118242FC084E6A8C191A40FD11381BFFC558D8F10C69319D6AA26D7A7F7C0609B6BB327BAD0C7AA90EF308A6E270C7A306E9D8E015C1
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":1.614320464860994e+12,"network":1.614288066e+12,"ticks":95878702.0,"uncertainty":4595785.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016888701"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\9b2b2967-5934-4a35-9d00-e8e89f5abb34.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):	164950
Entropy (8bit):	6.081681219680164
Encrypted:	false
SSDEEP:	3072:ufIsmGflW7LtsevCLxZJasImhjp3qm4JaPlrnZFcbXafIB0u1GOJmA3iuRa:avflkhsXNZswa2b3aqfIlUOoSiuRa
MD5:	5577CA3D6BB685CF02385A453075CB36
SHA1:	7F583B7848B1DE0EBB949EADAEC9F87D92F89093
SHA-256:	61B5B874CB232D05A6C6F02C926C721BF80D84E0DA473A59F7F4400506B0FBA7
SHA-512:	5A9FB45B4B1226519F7EDA7F40F4CA31258DC69BBFB97F69DB787B1B9B34C89D149735230ED3A28FBBF5E173354081374709FD1C45F144675BD52711950B564E
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":1.614320464860994e+12,"network":1.614288066e+12,"ticks":95878702.0,"uncertainty":4595785.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABmAAAAAQAAIAAAABAL2tyan+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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
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\22655057-8861-4339-aea5-b8d82abb215b.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):	5728
Entropy (8bit):	5.182909336353521
Encrypted:	false
SSDEEP:	96:nr2sn4YxixPoIPcV2ok0JCKL8rkdpYbOTQVuwn:nrD4HxP5c74KEkdM
MD5:	42D9496E28BFDC659B4AAFD8E2FD2CDE
SHA1:	267781F14BB0529E6A0D22A39D590D65BF53721A
SHA-256:	4DFE5644BF9958C4DC0F5DB446E2368E76DA7E619123A3D7C5CEF5430746DEC0
SHA-512:	5D8ADA1A8E47819BC7FBD1240F5D1267E38642D782CB0930CD756AF348ADAB967A1A792FA506C881F7E796078417C3415C1E5D6890DCDB612D915AE6BBC2E5 8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258794062108856","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","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","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3c861450-5cb6-42c7-b3bf-04e8fe251480.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):	5672
Entropy (8bit):	5.173410230996694
Encrypted:	false
SSDEEP:	96:nrj/n4YxixPoIPcV2ok0JCKL8mk/11bOTQVuwn:nrj4HxP5c74KBk/v
MD5:	76A8CB636DF606D3E2EDEB1D3B8C4624
SHA1:	D398E4B09D311853789889ECF9BA63970E7DACF5
SHA-256:	1D57DA5BEB6FC4CDA7B68AC61E15F717A966B9729250B19289D275E80DE2C135
SHA-512:	F9E13F9F2A6F1C1EA37CB5DB4EEC57DBE9C5CE8FED944753A9E9A64F6BBEEC323126DE6A7D395E08AA359888BAB037EEDB5E1FC88C19CF69D540F41712DC9 05E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258794062108856","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","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","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\63d1ad1b-eaa5-408c-be6e-3453acd2bd7a.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):	5.535690850403163
Encrypted:	false
SSDEEP:	384:5UltALl+/XE1kXqKf/pUZNCgVLH2HfDZrUGHGtnT7Ev4LC:zLlwE1kXqKf/pUZNCgVLH2Hf9rUmGtnc
MD5:	6ACD313CC8AF0859C20040C90865EE2C
SHA1:	9E353F16B941B290853B19108752DB77784AA185
SHA-256:	01AC429227B7164CA6A66A2027A6C63EBE9D7BA258B2838BBB1999D8621B7F98
SHA-512:	C9E850181936C02E4B532BAC82D8C74F3DA349DB9C8B5B0D3B8C1C900B048BE43C3749BF0F10AC86FC8238E0518F0368F7FB0E77402EEE11E745CAE25190C90 B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\63d1ad1b-eaa5-408c-be6e-3453acd2bd7a.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":"13258794061883135","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\9ab1cf94-097f-4342-acb9-56078b55ae1e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.109834684373485
Encrypted:	false
SSDEEP:	6:mNfPOq2PWXp+N23iKKdK9RXXTZIFUtpefeqZmwPefFEHvzkwOWXp+N23iKKdK9Rn:Rva5Kk7XT2FUtpvq/PtH75f5Kk7XVJ
MD5:	73C80D0446389E1915C69C5D98432EA6
SHA1:	130D6C48FDD342BB6C4C5FB85637D86C066C0D00
SHA-256:	58CC36F3544326EBC0033A48DF7670C233955D4CF9A05C74E788E34A5EAD9EFF
SHA-512:	431B5785CB9CAAA5E5DFFA7579D6B90535CF72FA842381C5A75AAC4C6969D59E8A858B016958756FAEE454450B315D80737F4381B00A48A23D0D11439D5D3628
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:10.312 1ab0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/02/25-22:21:10.325 1ab0 Recovering log #3.2021/02/25-22:21:10.326 1ab0 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):	5.084112002937577
Encrypted:	false
SSDEEP:	6:mNfKUuAq2PWXp+N23iKKdKyDZIFUtpefbhZmwPefYd1FzkwOWXp+N23iKKdKyJLJ:ZUHva5Kk02FUtpO/PV5f5KkWJ
MD5:	AB8512DFC0B94E8E6E4614EF65E88CD9
SHA1:	0F73EC278FAD463D60131D81C2ED193247FAD26B
SHA-256:	1E15792AFEC16283395B9F2F417262CDF193D0589141B17950F00F640DF60CC5
SHA-512:	577D83FD91839306F38DF4117C35B11344BF9DB7A1B678C74B006D2CD33947A5F7517FDBC01F2A453F8313817E24C70D63BC6A84F0ECA8C1D37261701609FA09
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:10.302 1ab0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/02/25-22:21:10.303 1ab0 Recovering log #3.2021/02/25-22:21:10.304 1ab0 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\144cec94ba301c81_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\144cec94ba301c81_0	
Size (bytes):	248
Entropy (8bit):	5.426255243009931
Encrypted:	false
SSDEEP:	6:mQYk+cGyAGDsiYUGIgHXqH9kaePhxQZK6t:p+hGYiY9OdXeYT
MD5:	63C38F9C313F6C13D7DC09B703841D53
SHA1:	3BA788052DBE74FE9F2EDF9B2B2EEE89CD9C7186
SHA-256:	FB9F214C7F96B1592903CB3DE8764F865738B385A55634DD023815DF9E15BB26
SHA-512:	B33F7644B8CEA14B290A773C87E60264AC86BFFA00B8C509A3EB8DED2930C0264E91E41B622201439CE03EC64497A3DDF7A03EACF10FC848AFDA44D5BE76DE D1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t.....3...._keyhttps://static.parastorage.com/services/wix-public/1.299.0/scripts/error-pages/app.js .https://besproutable.com/#& .../.....1..I.S.#.4g....? yo}.ET}....,h.A..Eo.....r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e5a7a718962a8ab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	263
Entropy (8bit):	5.437620166086777
Encrypted:	false
SSDEEP:	6:mcPYtVYk+cGyAGmvCFKj2FuIahDKtgbVIWDnA2hr/ZK6t:xAD+hGmZjRIE9a8A2Z/T
MD5:	38DD81685E24CB0A9532D677DD67C658
SHA1:	F191E5AA70E7927D0C96193444DE4F0DB25CD74E
SHA-256:	F87E7A62EBA611A14EAC675DC86FFAB31D5A3106D065BB9EA3B9499D251D2CF0
SHA-512:	58794D7DDC5874670FA35E2629CEB72036854EB1B027583E567F1156030A5DA94C7B8187A0DD73020EBF8D1DCB446A60BA13676C238478726522C33CACE312A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....$.a...._keyhttps://static.parastorage.com/services/third-party/angular-translate/1.1.1/angular-translate.min.js .https://besproutable.com/|...../.....$...|.. ....h.%...xi..-....A..Eo.....6./.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\35a19c5fec54e19d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.4747328771557155
Encrypted:	false
SSDEEP:	6:mOxd/PYk+cGyAGmv2KZuBCYqpFgboNT01OCK6t:ZdD+hGmuMu8Yqpn21
MD5:	F65B43B092C9AC15F3660A2B9B8DFD86
SHA1:	CF2E0598C7B43DCB243904B03795ADAAA2D2A548
SHA-256:	5BF299F49DAAB4ED4BA4F30D0288F6F8D1C383F247B09D84D5BF5BDD81CC7A4B
SHA-512:	04C097C91B384F3BD75B40E5667B8612D128F7FEBA5DEC8EF85F40B5F526B0F5C49E093972C7E4D32ED7B43C095FD0B4C3C12B05A3FDDB05319FBB26BB1A0A C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}...cCpR...._keyhttps://static.parastorage.com/services/third-party/angularjs/1.2.28/i18n/angular-locale_en.js .https://besproutable.com/.. .../.....O, }"g....s.....,I.5.H..z.....i.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41f0a85b681a4673_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.491176089975046
Encrypted:	false
SSDEEP:	6:msPYk+cGyAGmv2KbYXqBtgboo27rx4AK6t:x+hGmupqH
MD5:	86D6E23B907F938C84FAFC5705931010
SHA1:	DF8E039A643E772FFD73A126F57AC6D8EF190311
SHA-256:	E01B0FA4D3C0441B6C914CBD1A7202D5B818CB9A0FDDCC94E388ECA6E2C177C9
SHA-512:	D8CF1B1F78CB91055AA45CC9F5B87847E5BC0B2FFBC820AA583CF1DCE0B5C7D80A94880773A51434D7639A70A424EF022EA77743D6645D1351253B28DB3B010
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41f0a85b681a4673_0	
Preview:	0\r..m.....r.....R'...._keyhttps://static.parastorage.com/services/third-party/angularjs/1.2.28/angular.min.js .https://besproutable.com/...../.....9....}.'....Y.....A..Eo.....w.p,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f54a2bfeccad0b1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.474768378951151
Encrypted:	false
SSDEEP:	6:m9qr6EYk+cGyAGmvS8QK1tg4TN34sK6t:KfU+hGmb/31
MD5:	FA4FB25D742D7480162E8FE373110A77
SHA1:	BA87497FC15BB9303D66A1B7B30EEB1772DE312A
SHA-256:	5142F291953E1025E5B49ECBB09E70A650F8C32F7625A5F2580EE3A302BC156A
SHA-512:	A18EE77D6A0F38E5BAF2518D07B720A1116052A4C4204E32C284196325BAC846E263032FF20A23B062BAAE77D006FFC32FCA7C98CE6E230D43E14D324BA57FE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....._keyhttps://static.parastorage.com/services/third-party/jquery/2.0.3/jquery.min.js .https://besproutable.com/...../.....Lm..Mw{.D.P.D.A.<.S.a..<..j...A..Eo.....z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\948ef966964219be_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.3894067419708085
Encrypted:	false
SSDEEP:	3:m+l319Xa8RzYn1CvVIgKvDw1CvofH/lHCyVPNf/tE9kZm0Z/pK5kt:mqY1CzCGgcNf/ty03K6t
MD5:	7A48B451E0C60CF5BBCC7F52A3E9ADB3
SHA1:	AC1AFBA2A1CEDC67822DC9BD5AFB05C7505AC11E
SHA-256:	286C580861269F2A43DEAA55A17B2170F29CF51A805B70B8DF548CC495CC2693
SHA-512:	DC73DF321B2474908E6C5DA3030C69BF5C3B6283EEC629F9E935D111933164E12CDBE919A70EE386C4DD38236FC3C0E3D41507F7132D3A4D99CA341DB26FAF0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?...J....._keyhttps://bss.edu.ge/transdoc/js/main.js .https://bss.edu.ge/..r.../.....jJ.....X....6.q.w..8TI..zpu.H....Y.LMM.A..Eo.....\.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9673e3d884304536_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	197
Entropy (8bit):	5.401672220291833
Encrypted:	false
SSDEEP:	3:m+lrpzA8RzYn1CvVIPjWFVRw1CvWproW/lHCjL/Cbo8Sk162fiVyRmAQhXpK5kt:myp9Y1C+jWFVAC6gX2hX16yArZK6t
MD5:	858374E74036A8C84E306360E1BED7E6
SHA1:	F3EF0C29879A4AE4A8DE3B74EDDB5F3B3C482329
SHA-256:	D2679BB5D4B51EA999F244161242B89CF697AA39D5F136702B9268F5827D888A
SHA-512:	02778FA7572B7D4B3E1EE0DCBCF801B45909879967F5069B1FC2EBE7AD08785BD79B5C5DD77328AD90D8B69DD4EE3865C07C5E661B2FB52FEC99A0E0EF16D68D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A.....6...._keyhttps://bss.edu.ge/transdoc/js/jquery.js .https://bss.edu.ge/3Fp.../.....i|.....w.g..yH.J....+.._..~f..=.SF.C..A..Eo.....5.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f08086ba5cc99bb1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	263
Entropy (8bit):	5.486555178582861
Encrypted:	false
SSDEEP:	6:mcTjYk+cGyAGDsiYbGJtU/Kvtgd6DSvqK6t:xT+hGYiYbG3ZDl
MD5:	A26C7F3E49A86593B6111DFF8B445D36

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f08086ba5cc99bb1_0	
SHA1:	D7D7008D5B97339B27429FA22753AA8EC13A66AF
SHA-256:	56C10C309CBAB0335615F98CCB691534DCAF712115DC8934A079C531B2C59E28
SHA-512:	D2868AE8AE941A05CCDB0C7DE0CF341D024012EEAE118B5D43DBFB0B3A1F6D6F7C06BAFFBC761AA7DD511C4A4D863324C3D67545636D32E7A1E78BAF0FB6D F56
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://static.parastorage.com/services/wix-public/1.299.0/scripts/error-pages/locale/messages_en.js .https://besproutable.com/z...../..... ...=...i.A?...S.....l.C..w.h..A..Eo.....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):	432
Entropy (8bit):	5.052325962561729
Encrypted:	false
SSDEEP:	6:giStxSsZniaSkBlAqo/aS4uUS+RSQDb7u3zHUbzQ3zbn3pHkQ+IRwHp:gDQqlPisX74zHOzyz7V4hp
MD5:	A704DE9822F154DE34A10131F9260869
SHA1:	0AF48F5EFB7C9BEC14BEB5103EA4E2C0DDB529AD
SHA-256:	79C3A8FDA1590ADC5C1F9C508D1EBE6C5C0CA03350EFEDDB61FB4923B9F0B803
SHA-512:	410E3A795252F33F54B2CBBE8C75985693F070B36C8A433414B9848AC646654FBE4B303C24195AB836F8A426732CCE078504A97A5323148BB55A6583AEC56AAD
Malicious:	false
Reputation:	low
Preview:	.....oy retne.....0...L.@...../.....\....@...../.....b.qzZ.@...../.....T._..5@...../.....sF.h[..A@...../.....TO@...../.....B.f....8t.../.....6E0...s..8t... /.....^}.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:	dropped
Size (bytes):	12288
Entropy (8bit):	1.1024936162481092
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwAlBi/gAZOZD/FiuF+:TekLLOpEO5J/Kn7Uv7i/NOZgU+
MD5:	BBDAB2C3EB3EAC30032CD7342AF9C421
SHA1:	9862B675AE75D60864DFCD41822FB746E1705DF2
SHA-256:	77A60E739F6860EC9250BCAC5BF7FFCBAD0B72F798FB8AAE31E5A5B2405E614F
SHA-512:	B38DD4CF8AC3198CF5343D92AD07E01851E2C7BDC3063B9092CE4F158299CD97FDFA8DDF30FA9058CE27FCA3EFA018006FCBD3DA2D731557E21761AF70715A 7
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):	0.9692986106332475
Encrypted:	false
SSDEEP:	24:GcLgAZOZD/pLfqLbJLbXaFpEO5bNmISHn06Uwp+t8:G8NOZpLfq5LLOpEO5J/Kn7U6M8
MD5:	5D386E3D9C3353DC2351581D5003817B
SHA1:	4F2CE85CA4641B67053C4523B1D0ACFBD9A25ABE
SHA-256:	417B86A28A5171CC405F62532939A05D2E7090ABF125A80C9BB55E3799F71D2E
SHA-512:	1CBF0A9BF1CFAD8442F5DD16032ED9B03C8C834319E881CDD36450850A0653795CF6F8EA8F0748571B9B54F60D0F4B52C3F3B0DCA81DBB23AB7A57BF56A5B4 F
Malicious:	false
Reputation:	low
Preview:	.....n..... ....

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):	2108
Entropy (8bit):	3.17458805388203
Encrypted:	false
SSDEEP:	24:34SA/sVlrlA5lqQwl5M7aGLe6YQwEYDGtZmuMVGV22VnyuLeMwuCu2OlL:341sPxihsZZYDduMlVFV9LeMwuCuPL
MD5:	696C546FE60B3C65367D8FA90D9EE8EE
SHA1:	7338012AAC4EA7E7C9C16C826C3C06732631ED1E
SHA-256:	78B1839F6386D0892B843214B2CB1875E22E44D5A9BD93BF670D59D1C68819F9
SHA-512:	D0080F72584419FB9CB5DCFA554033C51F64173FBDDD6B2FA2F2D28A182FF4C886DCDA005574C886F8E5C661ADA1FFE938ED2367454AB401D26BEF2A19098FE2
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...546d5f56_2155_425c_b2aa_331f0ea6bef8.....!.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....%...https://bss.edu.ge/transdoc/index.php.....W.e.T .r.a.n.s.f.e.r. .S.e.c.u.r.e.d.....h.....`.....RD.E7...SD.E7...X.....p.....R...%...h.t.t.p.s.:././.b.s.s.. .e.d.u...g.e./.t.r.a.n.s.d.o.c./.i.n.d.e.x...p.h.p.....8.....0.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e .r.s.i.o.n. .1.0. .....=.&.....N.o. .o.w.n.e.r.....1.....

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.158131579573638
Encrypted:	false
SSDEEP:	6:mNfR/Aq2PWXp+N23iKKdK8aPrqIFUtpefRc1ZZmwPefAkwOWXp+N23iKKdK8amLJ:SAva5KkL3FUtpr/PL5f5KkQJ
MD5:	CC7B911DAC682CA8BDE612286A47B42A
SHA1:	274FF15088FC21682DBA04DF306FF07FBE0C2226
SHA-256:	82CC7DB0C6F5ACA9817E378DE52706B8EE853D030867514B3B87E2D6566E71D1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
SHA-512:	39E0A5217A144C392FE54F0CC81632864B123BEED86E822210872FA775F300C162686156EC93BCCE05A5E4EF80CBC08C33952B64F8B53DAFE1E1FD15F3669505
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:02.148 660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/02/25-22 :21:02.149 660 Recovering log #3.2021/02/25-22:21:02.150 660 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.156293759260025
Encrypted:	false
SSDEEP:	6:mNfQyq2PWXp+N23iKKdK8NIFUtpef6Fz1ZmwPefbpRkwOWXp+N23iKKdK8+eLJ:hyva5KkpFUtpfFZ/PspR5f5KkqJ
MD5:	6E913BCA97A40BA7C08DA9A65AB7BF82
SHA1:	CF7239C6FE0996CF61FF7A79F74D9089BB6D5AAD
SHA-256:	8BA16C1ECF6B896A4086A02515148CE4EB6B85657897A795CF89BF104B53340B
SHA-512:	FB56A3CDE7D8AB9B304AEC71557BB0B8748005F5E3379235ADBD18FBA0970B1EFA6D880C5A7E78BE1C17884D68C36CF6623C8B89D98CFABA4D2607C29C9FD 81
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:04.245 8a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/02/25-22 :21:04.247 8a4 Recovering log #3.2021/02/25-22:21:04.248 8a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003. log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
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):	16384
Entropy (8bit):	1.6946225954934115
Encrypted:	false
SSDEEP:	24:LLwxh0GY/l1rWR1PmCx9fZjsBX+T6Uw0w8FmUarC+CwSpLzNbfBlQtNDWdiIm88S:yBmw6fUX/h9NrzBlQHWdiIX8OHnML6
MD5:	6B0D391CE9610041268BA222A7D75028
SHA1:	52ECA92717FFC1DE5C6566D15527ED5DC8C692F2
SHA-256:	76B428F06C6042A4B483A1D5BB6233073D44180F75165576D4EAB42948EB4423
SHA-512:	F7D2620677D0544AB0CD499951A1451DFEB1D8DFB0F7D5C0CC00EC4C00A0875F489C2DC9EB747509CBA893B768FE14EF0BC1839BC5FDDE7810FE27CD56CCB64
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7763339899653999
Encrypted:	false
SSDEEP:	24:UuyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uw63n:UudBmw6fUp3n
MD5:	9806D05E061426B956F593EF692C8712
SHA1:	D91EEFB5014F4B3A5668E180013CDF4D432C90EC
SHA-256:	BB2A4C17913DC250834C2BBF4259B49124EBDA8B2151AFCDF506D7BF3A2A6452
SHA-512:	932E5F85BF693A27654E4F4F47F8F80EBE7CE8EC5F391FC4DDFE528B31159BB72F7012F4E7562D424E3BDF90C3124F0043E76CF1DAE35CC52FF34FFBAF607C5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Preview:	.....L^.1..... ....

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):	5.193592660655487
Encrypted:	false
SSDEEP:	6:mNfmIq2PWXp+N23iKKdK25+Xqx8chI+IFUtpefHvZmwPefikwOWXp+N23iKKdK2L:kva5KkTXfchI3FUtpMv/Pr5f5KkTXfcF
MD5:	5B46B0E10779BCF390B25B41E1E6432A
SHA1:	788CAED8D725098622570B0095496F5899675A90
SHA-256:	951BC5F729C83F9E1F3886FC8421BE87462E617023E7C46EC3805C304BAA76DA
SHA-512:	0CA1DEFB35F45417543827B5853AFD94C91C5B3BC788D12643BE69F50E773AAC2C4BDC5663BC4B09366055E885C13BCF2DA9DBDE7F2BDE5E1049C31AADB7F2E
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:10.294 1ab0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/02/25-22:21:10.297 1ab0 Recovering log #3.2021/02/25-22:21:10.298 1ab0 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):	5.1179500310443
Encrypted:	false
SSDEEP:	6:mNf2Oq2PWXp+N23iKKdK25+XuoIFUtpefhvZmwPefh9kwOWXp+N23iKKdK25+Xu6:dOva5KkTXYFUtpe/PS5f5KkTXHJ
MD5:	3D1E8E6DC917E93BC7685E5320D1FE7E
SHA1:	E2A5C313E847BB07BE8361E8C1F451B7E80506F3
SHA-256:	C6D37BB01C420590EAED3C196201CA2DA430FFA657FAE323D98ACF7EE8AE966A
SHA-512:	52271141130D29F411BE0F1461F74FBCF6C2C314C3648BA7B029336F28681E4BF642D400AD39DEE4715F5394B5176C5062E0E3FD71DA979FBAB9A470D5A1757D
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:10.290 1ab0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/02/25-22:21:10.291 1ab0 Recovering log #3.2021/02/25-22:21:10.291 1ab0 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):	5.172528754687131

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Encrypted:	false
SSDEEP:	6:mNf2Aq2PWXp+N23iKKdKWT5g1IdqIFUtpefJbZZmwPefJbzkwOWXp+N23iKKdKW4:vAva5Kkg5gSRFUtpU/PU5f5Kkg5gS3SJ
MD5:	DEFF41877FEEFF9E84DC1BAFA3126267
SHA1:	A0F345EBA1AD7ACA51FAC82885259EA18F96DD15
SHA-256:	176C10BB8296C49B6FD8CE0D8CEB2E1C3658A8BF9529A8A91F25B3E16BA02DA9
SHA-512:	50BD1736DFA39DE11FF6B86DE8846791BC552AF8A5D8B56D00B079F27203BF33F09DB2AB3C8EEF1FCB59C401E2E0CA0C830EB06298555DEACDABD03D581EBF4D
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:10.283 1ab0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/02/25-22:21:10.284 1ab0 Recovering log #3.2021/02/25-22:21:10.284 1ab0 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):	0.10345400265980419
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvgli5Mf1CwHF6HOo/lCxthihchCGCxC+/er7yn0CCwHn:TL+A/nSflwl6HNuQXGI/znkwH
MD5:	52C9586EE018EF827173BF6EB319EAC6
SHA1:	0DF7F7588C3D0297A6EB5A74D58EAAEA4DFB1551
SHA-256:	CFECD437AD76D10ACC4876938A75B64A2F5AE9B9B24D47A7857CCD1FC45674C3
SHA-512:	1C230B95D35E26A10D7CF62477387BC285C85DD7225D3CA64A4491038E28A869FF75303BFCC4D285DFFEACEAFA50956A07AE1958AB150C5718DC27585F115FE
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
Size (bytes):	577
Entropy (8bit):	5.114290079460768
Encrypted:	false
SSDEEP:	12:IXlSRjdroK3uBDaTeLBpJ5/e1tlPOfTNKBk778B/xgskZBaDkwdpDbfW3n0:sTpC0BKHOf5lY78BJgskfaDkwfDbe30
MD5:	A38E7CD02E84AAE0713B75C80852F1CB
SHA1:	C6871082E9088EA1ACDB1DDC76671D05D6E92CBA
SHA-256:	CCBDA2BC58DDC3481DCE1509C87F4CC2843B6D7E39D2D9629390EA7093FAC000
SHA-512:	BDE82D71928B92646DDD52F9AC578A371CFC20B24AC2A8615182721BC06D2DAE411F8ED8D3A719205D40439DC87AD2F3FB13BBE38A3CC2BA52F264EB5B7F8E6
Malicious:	false
Reputation:	low
Preview:	....."B....bss..edu..ge..https..index..php..secured..transdoc..wetransfer*f.....bss.....edu.....ge.....https.....index.....php.....secured.....transdoc.....wetransfer..2.... .....a.....b.....c.....d.....e.....f.....g.....h.....i.....n.....o.....p.....r.....s.....t.....u.....w.....x...:S..... .....B_...[..... .....*%https://bss.edu.ge/transdoc/index.php2.WeTransfer Secured:.....J.....""....

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):	42076
Entropy (8bit):	0.11699488681915875
Encrypted:	false
SSDEEP:	6:+vk4mfaaWg9bNFlWCj/leB8/l3lM04/fMt76Y4QZVRtRex99pG/hlaqR4EZY4QZ0:oUaNqLBj/2Y3lZ4nMWQA9LQlhBQZ8fOE
MD5:	78B69E97016BAF066B9787CF62DA84C3
SHA1:	71620D40D1DED78F720651484EC7ED5159D828F0
SHA-256:	C3E01EA451E8AE5593523D873A232255466EAB4D9C2BAFD5E51746B6F0DDBD4A
SHA-512:	4F87B9A322622D69736AF820FF055B5D254C35A36961270F46132D1FDEEEEB47A2AA097B9890FC6226E00BD71EA4BD482DF035F955B1E1F8B1051ABC772294BF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Preview:	.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.439289846469471
Encrypted:	false
SSDEEP:	48:cZKnGf/gNaa79aMhd8dbpYRnBnpL3bQSefgGYNrS0U9RdiN9O:cI6INaa79aMh2dbpYRnBnpjbQ5fgGgrs
MD5:	ABA81C590568C1482A685582D4F108D7
SHA1:	B24A1CE71D1019161DBD52D374B39F157B797D88
SHA-256:	1C00D7C37004337CA096CAFB878DC59667738B710955E3881E1D7A6C8ED33012
SHA-512:	2CAC3C8318A1CD80289CF4A78C7BCA5996784EC0A144D8DCD575EFEE354D41517099952A5076761181F8AF8518D1D131B209C86DB5EA005D0AB3C232613FD6
Malicious:	false
Reputation:	low
Preview:	s9.....*.....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..516504000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-02-25 22:21:11.48][INFO][mr.Init] MR instance ID: b2d2c7f4-65ef-43e2-ace7-a931c208e0ca\n","[2021-02-25 22:21:11.48][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-02-25 22:21:11.48][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-02-25 22:21:11.48][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-02-25 22:21:11.48][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-02-25 22:21:11.48][INFO][mr.CastProvider] Query enabled: true\n","[2021-02-25 22:21:11.48][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):	329
Entropy (8bit):	5.1256956117978305
Encrypted:	false
SSDEEP:	6:mNfb+q2PWXp+N23iKKdK8a2jMGIFUtpefb7ZmwPefbcTnkwOWXp+N23iKKdK8a23:Pva5Kk8EFUtpG/Pvn5f5Kk8bJ
MD5:	96D35AEC8D0E764516A393E2AC90014F
SHA1:	221B8F198248DDB96B3C805D5CDC6F68D729032D
SHA-256:	A0180887A7F49AFAAF49A7341A55E4764FDDA2F8C9292EB88F3FEC0E5A2B1458
SHA-512:	B23CEB7623F34C61377F5E022031AAC47C48EEF1BC49E83F9558391822C3BC24C074443200306809F27311EE49AEB4E36D80CA5D064545B1B1CBF4B6D8B74165
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:01.925 660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/02/25-22:21:01.929 660 Recovering log #3.2021/02/25-22:21:01.931 660 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:	dropped
Size (bytes):	24576
Entropy (8bit):	1.1609457005653654
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOe6POqAuhjspnWOoQq9aIdQ/7:HUcLz
MD5:	FE82DC4A89EF5815FDBFC71B7018F146
SHA1:	B6B4A4D2F3187BE4FAF8E833FC4BE95959759239
SHA-256:	57E1D72D17D22E4D3CC9C90E04E45395DDC1BB453D91F691E5F85A93E5143613
SHA-512:	6AD009BDA99AEF8A0C9ADAC587FA4A65082D187F7111C42CE07B97277F5F0EBB3575AAEF6C50B07E5418ADC9F80579116B9C7E891C5146E624258E168D89F98
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.0192346008395856
Encrypted:	false
SSDEEP:	48:44q7w/qALihje9kqL42WOT/ulqrw/qALihje9kqL42WOT/c8:44UOqAuhjspnWOSkOqAuhjspnWOL
MD5:	9B1D6EF1835548A52E908871938137AC
SHA1:	AE394753BAD019F854468237EA60E041FE95A935
SHA-256:	1AC24FEEA291A24722F5065ECA00A4228610EB2055252E3C11E66256B4D90F1B
SHA-512:	98F4B602E5A390FB24FA12F7D4E50379E303066D54C24EDE221402E70ADA055C0E0A308519256868FF0B0B8F7AB96CD738D502E0DFA012EF13BE751A1CF487CI
Malicious:	false
Reputation:	low
Preview:	.....ve..... ....

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):	331
Entropy (8bit):	5.163710760482548
Encrypted:	false
SSDEEP:	6:mNfdU+q2PWXp+N23iKKdKgXz4rRIFUtpefdWHZmwPefdjzkwOWXp+N23iKKdKgXS:mva5KkgXiuFUtpdH/POz5f5KkgX2J
MD5:	708D96326CAF70F43D376B56BF3D2831
SHA1:	8633DBDC32403659DAD4DF2EC14D0DC6ABFD1415
SHA-256:	13956CA5830D0A963A6ABCF9C020D520B0159C14001BEF9F7135BC5F9C278ED1
SHA-512:	AF2F0F7A629F86E004CE949022700FEDC632F6FEE03D5DC4436425579A82FFB72FD85C1F86F9B34AECAF4FB81E3E4FFFDCB01D694884027BA2FBA0A517F5119
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:02.181 660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/02/25-22:21:02.183 660 Recovering log #3.2021/02/25-22:21:02.184 660 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:5ljljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.136348203096811
Encrypted:	false
SSDEEP:	6:mNfmkF3cM+q2PWXp+N23iKKdKrQMxIFUtpefmzJZmwPefmiNcMVkwOWXp+N23iKN:u3cM+va5KkCFUtpDJ/PSNcMV5f5KktJ
MD5:	51AE2007E3B8147AB656E5757A3817A5
SHA1:	8A4D856E11CE5A000182E10630D2297C1A3A0251
SHA-256:	B76C95CD0BB8C499D1EE87005D2CB1A87C499F1665FC20183BFCBE2AF1B50864
SHA-512:	73F85D4D3B76BEF074786614224F2D83B5C11E9316F9F6656025EBFD9A30C51C1A4BE5227C9EF127904A91C277A19545900EB5D464477BF6CDDE52764176ADAD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:02.072 168c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/02/25-22:21:02.073 168c Recovering log #3.2021/02/25-22:21:02.074 168c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.117184164882692
Encrypted:	false
SSDEEP:	6:mNfbdi+L+q2PWXp+N23iKKdK7Uh2ghZIFUtpefbdjMJKWZmwPefbdBnlLVkwOWXw:wNL+va5KkIhHh2FUtpAjMEW/PATLV5fI
MD5:	00C592F9A2AA387233EB2916F44674FD
SHA1:	72EFF7FEF3A87C5329C15CAF8284434C683CFFE0
SHA-256:	4F3BFFF3431A60FFE4938CDC285E6AB4ADB184353C388E488F67F0C17D147F06
SHA-512:	3017EE07E4559D69A1A651768908F8FA5F060CA1ADA3C6F74559BD685BBB0EA6D2D4009C1DBFB857A75F542850B3EB51AA6B34AB80DAA204748A576C960ED4F8
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:01.867 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/02/25-22:21:01.868 10ec Recovering log #3.2021/02/25-22:21:01.869 10ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\8a298803-9696-48aa-a669-7aab15c93704.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.200179425948358
Encrypted:	false
SSDEEP:	12:AQNcM+va5KkFFUtpQZJ/PQZcMV5f5KkOJ:Akcda5KkfgOZqZc2f5KkK
MD5:	ED2EBEEB15F73A1EDDB56E0B3576D824
SHA1:	DC8E37EC9D2CFF6859536DAA213CA2965A24BD36
SHA-256:	50AB9DD6A3D3F27EE2B4E9D305AC5640925BEE5FD8269FF917AC34810AF93B05
SHA-512:	C1B95D3EEF326A822FCC7EEF170B2C25435F72E17A169D6C0735DA44A96199687E5FE3B04A8B5F27D076C12FEF8B17C2F486A0D8532CA9283E33030BB45A1EEC
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:02.125 168c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/02/25-22:21:02.126 168c Recovering log #3.2021/02/25-22:21:02.126 168c 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):	429
Entropy (8bit):	5.221138378062197
Encrypted:	false
SSDEEP:	6:mNfdUGN1WM+q2PWXp+N23iKKdKusNpqz4rRIFUtpefb1ZmwPefdvB1WMVkwOWXpx:FE1L+va5KkmiuFUtps/Pa3LV5f5Kkm2J
MD5:	194CA8F9F4575BDE92CF1B4E210EA213
SHA1:	407FA2100A5FB14059CF9D2322B0D1D603F503B5
SHA-256:	A1EBC84A2016E5F2321A6ED23A855120BC13CCF443C0B91F9A8B2784B51ECA47
SHA-512:	9A47F0BA96D9C5033C2D8CFD83DBD5343C78A93EA7B4F739538711C898F2E63F36163ADD99A212F893569127819E3ABB538811A0EDDE281981D4C51AC79FCA4
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:02.175 f1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/02/25-22:21:02.179 f1c Recovering log #3.2021/02/25-22:21:02.180 f1c 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):	415
Entropy (8bit):	5.244676369574411
Encrypted:	false
SSDEEP:	6:mNfndllyq2PWXp+N23iKKdKusNpZQMxIFUtpefSKj1ZmwPefB+RkwOWXp+N23iKX:I0yva5KkMFUtpKJ/Py+R5f5KkTJ
MD5:	DCA4A780855A192653972257CD3C1F7E
SHA1:	8E2D1DA6A8FA8061C00D373BCBA619BE99A8F967
SHA-256:	587FCA1D46874DA9DD03177A22A8A36E798B87406390471E3E38E6C846B7BB5D
SHA-512:	25C21E90E478725B861638DDB5ACA62779161310363D19245240682CDF0F73E7E7AA1024329ADAF139E0435AC3993E9F637BA7D19410CC28A91DF0E442187CD6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Preview:	2021/02/25-22:21:18.433 8a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/02/25-22:21:18.434 8a4 Recovering log #3.2021/02/25-22:21:18.435 8a4 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\8758eb93-0677-4c65-9314-fa0988e0fe7c.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
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):	5.202352000347405
Encrypted:	false
SSDEEP:	12:KcM+va5KkkGHArBFUtpuJ/PJcMV5f5KkkGHAryJ:Kcda5KkkGgPgo/c2f5KkkGga
MD5:	2BCEDE3F081A6C3E0BDD7B7C345C8A2A
SHA1:	B5BFBD7A9F6CD7E100D2360A673D35B3438894F5
SHA-256:	06382A36D595D8F5334465AEF50CDA79A56C0BDB76750420BCEB8837A7264C75
SHA-512:	E529E5F9312BBE4682C7C3E247AB31496D40B4CC0091B5677E279B1182E0C7205FC6FDA8E460DE32CD4AD5987A523592832C2225E22ACCB87583C72E51F8AD7
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:09.954 168c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/02/25-22:21:09.958 168c Recovering log #3.2021/02/25-22:21:09.959 168c 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):	429
Entropy (8bit):	5.1940788190884435

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Encrypted:	false
SSDEEP:	12:OL+va5KkkGHArqiuFUtpd/PWB1LV5f5KkkGHArq2J:OYa5KkkGgCgG3Df5KkkGg7
MD5:	A0FD5D64B96371DDC72C1552546208CB
SHA1:	5D5EE824159F7CDB65DF7E92980F54BFB5CBB4CF
SHA-256:	14F8DA04672D30361E4C7D9D0C5DC8450A676FC96D5ED3906C3EB4A07D7B93D9
SHA-512:	6F01959A2072C1E4057D2BCEA25093C766C9BE0A2ACBEC30BEABED374DE264F0F338B9D8DE1C71B048EB09AF3C6A9AEBB56EBF81AAC6EF88288D58528FB80106
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:09.963 f1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/02/25-22:21:09.964 f1c Recovering log #3.2021/02/25-22:21:09.965 f1c 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):	415
Entropy (8bit):	5.127450745299304
Encrypted:	false
SSDEEP:	12:8Nyva5KkkGHArAFUtpMQJ/PMQ1R5f5KkkGHArfJ:6Ya5KkkGgkgZF1Df5KkkGgV
MD5:	BE7C6C344B01DAAE090A7E72A9C29B14
SHA1:	DBC720D283360CB17A90D5919C577BB118D8C8C7
SHA-256:	0C1842EEFA8DD9D8203ACDA50F1EE9977B3DBD4A84BFF14ED4B26BDCF6A6065D
SHA-512:	08928B2F641642CDADEE4F5706C1B700489CA9CC2CB9D21DD266A1E5E967916D27F99826DF8BB7A07E2941B75BA16ADD35960413F643B938F1E555E0EE6AB58C
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:25.223 8a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/02/25-22:21:25.224 8a4 Recovering log #3.2021/02/25-22:21:25.224 8a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
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):	5.164285309428378
Encrypted:	false
SSDEEP:	6:mNfbdMlL+q2PWXp+N23iKKdKpIFUtpefbdTKWZmwPefbdaLVkwOWXp+N23iKKdK7:wMlL+va5KkmFUtpAGW/PAaLV5f5KkaUJ
MD5:	64DDE2BFFFC2BD8CA7736B4716E86D41
SHA1:	A05B8E209D1D3143269BDB03265CD896B8C21430
SHA-256:	B8B50377B92E4C47834A60CF18CB3128DC045501513DE27463CDFFC60B203A2E
SHA-512:	40743EDCFE5FF20BA8EEAAE5317A3C16F02184AC6E666BD4397C7032A6CCA7CB260B690080CC879D21E8739CAB4C9A0B3ADBB4A7549A18CC5D839D57817E883
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:01.886 10ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/02/25-22:21:01.892 10ec Recovering log #3.2021/02/25-22:21:01.893 10ec 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):	399
Entropy (8bit):	5.306298964404627
Encrypted:	false
SSDEEP:	6:mNf3L0yq2PWXp+N23iKKdKks8Y5JKKhdIFUtpef3h1ZmwPef3FEj31RkwOWXp+NA:Byva5KkkOrsFUtpW/PMlIR5f5KkkOrzJ
MD5:	2CF0A263290BC74E44E925201D196A5B
SHA1:	BE532632AF00EB927D3983F8BA40D4A9923CF0B5
SHA-256:	6A5246E5298D4BA3F50E1D0B6DD619F1CB5E09BD8E4865DF40648E72BA98BB96
SHA-512:	55D57018A74D75E355E2B73EAFF2BB4D22C7F4B4F5FF7A897DEEB2B24285A4FB11A3F94EB2691E4E69797DA962F9E3011859A7DD9E6922309F2700CBFD81AF0
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:11.517 8a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/02/25-22:21:11.518 8a4 Recovering log #3.2021/02/25-22:21:11.519 8a4 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):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:CSSSNn:4+
MD5:	3F10DA8ACC60D8818629048A9B11A365
SHA1:	33FB064A2811DBE31FADF22FA55759047BA60349
SHA-256:	5BF9B09C4C2CAD39EAAD15ED3280D0CE1BE5FDA5E2E1806847E4B05FDD4767FF
SHA-512:	BACBBE4259E36FFDBBF81759500D66120DBC97C08431864C7FE240B088FEFD4D17553305089440DCEE41FE74318B4FC7C62BEA669F4753B08B61F0EA24B3A8DB
Malicious:	false
Reputation:	low
Preview:	.....}...(..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b95d7805-2ce1-4c24-b76e-637f789cb07b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2732
Entropy (8bit):	4.892903409748109
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b95d7805-2ce1-4c24-b76e-637f789cb07b.tmp	
SSDEEP:	48:Y2TntwCXGDHz5s1RLsUTsaTRt46bsLkzs1fyKsa3q38VsQMHssYMHMvYhbD:JTnOCXGDHz6nPQ6q3f/a38vGcGMAhH
MD5:	F6EDE1C490BBF4EF5137A67D4587EC25
SHA1:	38B6A104065B06901AE7C138E03F0F45A722CB24
SHA-256:	A475EEDF0835AFB63B5CCCE253BF4656EBB8DA92ABB3B03F0F77CEDCDBBE8CB7
SHA-512:	AF4913D04903E43DEA78099EEEE9360A7959035FF605B0821A29BE697CEC9BBCF73BDA41B340FF21E1075ECBF2C57D55D79EC34E1C0F557FE9809BF83179AD6 F
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13261386064764261","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13261386064765409","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c09db41c-ec7a-4fc4-8bef-af0686cd6bbf.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):	1540
Entropy (8bit):	5.58838606434058
Encrypted:	false
SSDEEP:	48:YI6UUhVseKUedUYAU7qPeUer2UefI4wUIwUxUenw:GUUX3KUoUhUuPeU9UEIdUNUxUD
MD5:	63F6EC0D8D92EEBE9E770418CF1D2304
SHA1:	2DD0B4106E8F23B0967508461509D79F9709EE12
SHA-256:	B7F9A4B368CB8411D639915D6563FCA7B91458AD93F442B55082932A4D073F41
SHA-512:	520E3A8A9301975D1E833C1529D98D71BF22C989735CDCC0563A280E7CA582A9FA82E49B31D3E52E63DC7D3E36208916240790557B6B52EFA0129DEF228682EE
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1645856465.963989,"host":"qaDeFdT1UTirY0OQe+c5LKw+zjx6vF/+3vFh7CgrAOY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614320465.963996},{"expiry":1645856478.068027,"host":"tt3zguFPm5QK7v0HiIayCngI9aYzI+xnvz4fXkVqhaQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614320478.068031},{"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\ca295e52-b2f9-46e8-a82e-d3099d7213d7.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):	5702
Entropy (8bit):	5.181743937605227
Encrypted:	false
SSDEEP:	96:nr2/n4YxixPoIPcV2ok0JCKL8Bk5nybOTQVuwn:nrS4HxP5c74Kek5I
MD5:	6F92D15DDA7E8CB9BBDAFEEE16F56E66
SHA1:	4B07B41932710CC23BCB8B7BF6AC93BB1BB4019D
SHA-256:	1F04B3FF41D0E7D132304F59A1A937F3D8E98003140DDD65ACA96B4D3E42035C
SHA-512:	28ABA67D804C7F375CB642F1ACCDEB673538ADFA01F884ACC8EB2475A3D6C0E39808D07B2E8C01B8AC623BBE70913F0978E5B702ACEA65165E639EB3C204E6 94
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258794062108856","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","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","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cb017fbb-900c-4cab-a903-240e66d614fe.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):	5.535795708520935
Encrypted:	false
SSDEEP:	384:5Ult1Ll+/XE1kXqKf/pUZNCgVLH2HfDZrUGHG+nTIMv4Ln:gLlwE1kXqKf/pUZNCgVLH2Hf9rUmG+nk

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cb017fbb-900c-4cab-a903-240e66d614fe.tmp	
MD5:	08B3ACA4DF35826ACB22E70279D01179
SHA1:	5A9F91DFD20FCDB0AA2452772A371C5B9BACBC4D
SHA-256:	AEE8644DA6DC7B2BA7A78FA476FBF3A995D37F6FEC2F02D283EEBB582E71F06E
SHA-512:	1D530E276D3AB3048635A638040B7997D3B93E4B69C3441F3F9C4088629439FC5F921EACBF8D69FD195E00738C42D524E5CD04FCC938FEFEB52F03C8FA30269
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":"13258794061883135","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\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.345265256053261
Encrypted:	false
SSDEEP:	3:tUKotfjL9hZmwv3atfj9FFeJ01V8satfj9FFeJ01WGv:mNfjLHZmwPefjnFW0VvefjnFW0tv
MD5:	6C3D9580AA425C70D569F4AC9970B1C2
SHA1:	53270883582AE0F1157BE154F833475F8B1CD700
SHA-256:	9A5095B58912D7D6E80823FED0EE051347A3262110FECD61E097DC9C32FAA0C6
SHA-512:	B5E93C1C055594CABCB1034A2E7985275BE4A20C886E1107CF2DBF72713DDA9A539113D25DF4ED99FFBA027E37D1DED9AFD565514C8D8CCEDD7CD337A26666F
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:09.170 1ab0 Recovering log #3.2021/02/25-22:21:09.228 1ab0 Delete type=0 #3.2021/02/25-22:21:09.228 1ab0 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\df037bab-defd-4f1a-acc3-c0537e81a54e.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):	1205
Entropy (8bit):	5.58065538723771
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUedUlkq/HeUeXby2qUeXvIG7wUURUenHQ:YI6UUhVseKUedU+qPeUer2UefI4wUYUD
MD5:	D69D11576E1CFA7E5AC3C66F8416127B
SHA1:	AF1B1A33BE4845C739A35E42BD647AC66B5CDEC9
SHA-256:	24CD5D38D365BF1797EFCDB76B1E3B7B790313FA7312FF708CB4AB2DFADEBE06
SHA-512:	FEF252C3458F6BD6DE4DD09703D2503D915AF9393E32F29FACC72FCD853611D40373A6B1E18B0B84F10319297B2393A78A5D6D7998626FEBCE3F83BBC833A0C
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1645856465.963989,"host":"qaDeFdT1UTirY0OQe+c5LKw+zjx6vF/+3vFh7CgrAOY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614320465.963996},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1645856464.764317,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fb99c5d0-98fb-4f26-995f-fc86ec110386.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\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.17227832254867
Encrypted:	false
SSDEEP:	6:mNfL1WM+q2PWXp+N23iKKdKfrzAdIFUtpef/fNj1ZmwPef/fN1WMVkwOWXp+N23m:a1L+va5Kk9FUtp+NJ/P+N1LV5f5Kk2J
MD5:	67317659232A4821663D70D5DC147189
SHA1:	D23B5D4BC3961AABF47B32F8BF7A08679936CE26
SHA-256:	529B02AA443FEB1CEFB75960DB75707822F6F4F1D540D390D8FD52309A9DFA92
SHA-512:	823C39BE37384343278F71A602075366D64AC0DE487A31F1F7B3CCCB545474A77C9905A21E3F74B80596DF6D0F0DBC8624E84437DF6A9267DC6780F175947A29
Malicious:	false
Reputation:	low
Preview:	2021/02/25-22:21:10.435 f1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/02/25-22:21:10.437 f1c Recovering log #3.2021/02/25-22:21:10.437 f1c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.19.0\Indexing in Progress	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir5708_2140087493\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	223592
Entropy (8bit):	4.9638585725691575
Encrypted:	false
SSDEEP:	3072:SRztNSIhnVr91m7Y+VFwPmqSqm2+Sc4Q2PRbKbG5uu5hrExzu6KyGbx+9Omzpj:ShNZDE7nxPC5cVr6xE
MD5:	FCCFC2303ACCE4945A4E5B17FEB074D6
SHA1:	314086BBE1D350CB8850C76D89C00EC6D4E7B0BE
SHA-256:	6139961F1E07AE33628E913D3551469AFB1AD57A29F0520B2281879A44CBC92F
SHA-512:	7F8E9D7919C5A4896113EBFDACC5B9728DC9F56138B163FD92E9CC82B393890B125FADE7586B3A4373B9930311035E5581B14705167070A28FDB5D42D69EA14E
Malicious:	false
Reputation:	low
Preview:	.....d.....5..... .....`...D.....|.....t...p.....h...d...`.....t...L...T...8...@...<...8...4.....,...(.....uocca.....&.....ozama.....3..0.....0iupb.....@_..H.....g.bat.....`.....onwod.....x.....ennab.....d.....nozam.....(v.....geips.....rekoj.....lgoog.....`.....uotpo.....lreko.....o.....x7.....x.....tf.....H...,.....P...L.....@...<...t...4...0...P...(...0... .....h.....H.....(.....l.....H.....(.....t.....l...h...d...`.....T...P...L...H...X...@...<...8...4...0.....(...$... .....d.....@..... .....p.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\bb688642-0249-44c8-8fed-3fa039a29a30.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):	164950
Entropy (8bit):	6.081682913439702
Encrypted:	false
SSDEEP:	3072:VfIsmGfIW7LtsevCLxZJasImhjp3qm4JaPlrnZFcbXafIB0u1GOJmA3iuRa:FvflkhsXNZswa2b3aqfIlUOoSiuRa
MD5:	AAB774FF6E0A84D1B1D5A04B52366D76
SHA1:	7E90DE111F01181F8FDFE337D3793AF15BCA4A84
SHA-256:	0E0E33E719B6575463FF09F2AC80A4A07035BB8F81FB29B6923D431ABFC93D0E
SHA-512:	1BBAA6CD561EE3EBDCCC49C3EA727FA273F983B5031AA8C987530BCB99E40A69C0E112A0E48B3C82B3D1D1AE1FCA057B336DFB124DDDFEE241FBC5CA9356 93DE
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":1.614320464860994e+12,"network":1.614288066e+12,"ticks":95878702.0,"uncertainty":4595785.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016888701"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\c4a8bb56-76bb-4166-96f1-a83ab8506349.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.74688231875869
Encrypted:	false
SSDEEP:	384:FrBS/TRi8Z25lVu0jaNLrQvnt3wP1QHJoG8rrWB3DxQVVVEreXmeKYCtTnzIOdNM:nZ+qFVOpgsgevLZJkn7qxKXJD16
MD5:	A19D1EC9E964DC4F24D241C674C18AB6
SHA1:	38877A2E1D2C6D69740A1692EFFFF84AD21A8B7F
SHA-256:	440B88844BFFB6417797663647E343A1855786E1459A7D52E5A9674A7078665C
SHA-512:	43680A0C8A1969295A3CB46DDBF9C15830C2328EB2B7CBE5B1AFC1B239113307CE5FC5A4931F9444A07C2BFC8B79DB758B410B6B428AF83D03F21C172058DF2
Malicious:	false
Reputation:	low
Preview:	.t.....*...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....28.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\5708_463549847\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9477608398895883
Encrypted:	false
SSDEEP:	3:SdUoLS6MTYUAZdXtbJXBVGHIVWfE:S/7MTYUATPv8c
MD5:	AFFD907C7BB49B4A7449E67EE49D99C7
SHA1:	3DAEC57822D8C39E0BDE14BCD19B906CED0F55ED
SHA-256:	D5CDD87B76D7E6C3DC16374D41B8350519BE46B978EAC80AB70E6386F6E702FB
SHA-512:	488D45EA5C58C2F27360E86CC50F487AE81F6E5C8D58D82C0155346297AAA542018BBCCAD138972D173E3E822F06D62A95EFDE2426D8823AC1C987214D67D01
Malicious:	false
Reputation:	low
Preview:	1.869f6197c3fdd474910319ff37ee13b73f8fb8ceeaaa62517e2d056b6a03ff54

C:\Users\user\AppData\Local\Temp\71ac5287-60b8-4d0a-aea3-f84e87e14c8f.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

C:\Users\user\AppData\Local\Temp\71ac5287-60b8-4d0a-aea3-f84e87e14c8f.tmp	
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\7719cf8e-4948-4365-a3a0-d079d3926fe6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\7d5b9742-2769-48b3-9e64-0493a208f40b.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\d3f95c49-20fd-406d-a6fd-6233e34822d2.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

C:\Users\user\AppData\Local\Temp\d3f95c49-20fd-406d-a6fd-6233e34822d2.tmp	
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;..._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q...:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni..`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\7719cf8e-4948-4365-a3a0-d079d3926fe6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...'].....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\bg\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):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "....., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "....., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\ca\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):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\cs\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):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\da\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):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C53E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\de\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):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\el\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):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\el\messages.json	
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\es\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):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\es\messages.json	
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\es_419\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):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5708_225109263\CRX_INSTALL_locales\et\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):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

Static File Info

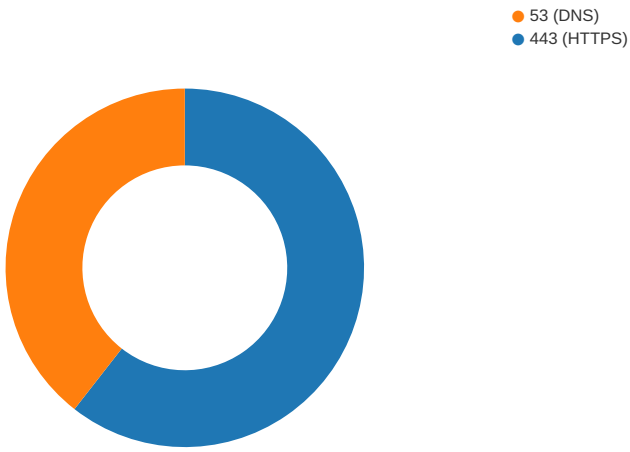
No static file info

Network Behavior

Network Port Distribution

Total Packets: 109

Copyright null 2021



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:21:04.516606092 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:04.517407894 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:04.619231939 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.619396925 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:04.619891882 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:04.627185106 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.627393961 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:04.627985001 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:04.722295046 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.723618031 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.723635912 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.723650932 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.723661900 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.723733902 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:04.727231979 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.727243900 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.727320910 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:04.736135006 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.737413883 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.737436056 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.737454891 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.737469912 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.737591982 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:04.737643957 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:04.742784977 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.742808104 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:04.742965937 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.498737097 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.499552965 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.499749899 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.604085922 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.604208946 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.604275942 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.610353947 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.610575914 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.610691071 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.644010067 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.651654959 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.651696920 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.651738882 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.651776075 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.651801109 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.651830912 CET	49716	443	192.168.2.3	91.239.207.130

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:21:05.651858091 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.651896000 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.651921034 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.651947021 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.657943010 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.658025980 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.706892967 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.706960917 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.707003117 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.707031965 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.707077026 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.707129955 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.754476070 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.783977032 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.794233084 CET	49726	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.795327902 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.795984983 CET	49727	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.893332958 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.893376112 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.893439054 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.893475056 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.893516064 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.893517017 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.893553972 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.893563032 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.893590927 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.893619061 CET	443	49717	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.893657923 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.893708944 CET	49717	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.897850990 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.898694992 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.898739100 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.898777008 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.898821115 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.898847103 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.898885012 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.898920059 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.898942947 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.898983955 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899004936 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.899048090 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899089098 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899115086 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.899158955 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899207115 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899230957 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.899275064 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899316072 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899343014 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.899374962 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899411917 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899449110 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899466038 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.899508953 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899521112 CET	49716	443	192.168.2.3	91.239.207.130
Feb 25, 2021 22:21:05.899558067 CET	443	49716	91.239.207.130	192.168.2.3
Feb 25, 2021 22:21:05.899595976 CET	443	49716	91.239.207.130	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:20:52.788985968 CET	49199	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:20:52.838741064 CET	53	49199	8.8.8.8	192.168.2.3
Feb 25, 2021 22:20:53.616549015 CET	50620	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:20:53.668128014 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 22:20:54.400816917 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:20:54.450643063 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 22:20:55.185250998 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:20:55.238305092 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 22:20:56.946861029 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:20:56.995989084 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 22:20:58.307264090 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:20:58.356110096 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:01.078259945 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:01.135535955 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:02.689960957 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:02.743784904 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:03.840950012 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:03.892433882 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:04.446443081 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:04.448508024 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:04.449536085 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:04.451658010 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:04.504353046 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:04.505496025 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:04.509100914 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:04.509804010 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:04.947078943 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:04.986952066 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:05.004235029 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:05.040757895 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:05.065226078 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:05.108227968 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:05.116554022 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:05.174771070 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:05.793093920 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:05.841770887 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:06.232239008 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:06.282788038 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:06.302726984 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:06.370626926 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:06.581285000 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:06.646888018 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:07.429898024 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:07.480328083 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:08.514051914 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:08.562906981 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:09.520611048 CET	56579	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:09.586908102 CET	53	56579	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:09.711905956 CET	60633	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:09.829623938 CET	53	60633	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:10.496500969 CET	61292	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:10.545139074 CET	53	61292	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:11.405280113 CET	63619	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:11.462596893 CET	53	63619	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:13.968828917 CET	64910	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:14.055022001 CET	53	64910	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:17.110569954 CET	56130	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:17.159712076 CET	53	56130	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:17.462133884 CET	56338	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:17.534708023 CET	53	56338	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:17.739054918 CET	59420	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:17.790723085 CET	53	59420	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:18.366925001 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.409570932 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.410324097 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.452315092 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.452370882 CET	443	59422	34.96.106.200	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:21:18.452419043 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.452476978 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.452640057 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.453948021 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.454174995 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.504112959 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.505168915 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.505333900 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.505491972 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.505548000 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.505597115 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.505647898 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.505697966 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.505747080 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.505794048 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.505841970 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.505891085 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.506400108 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.506875038 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.506925106 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.506931067 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.506936073 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.506978035 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.507662058 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.508951902 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.508970976 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.510556936 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.510612965 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.510776997 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.513514996 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.513575077 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.514452934 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.515219927 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.515278101 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.515448093 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.517505884 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.517559052 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.517703056 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.519999981 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.520051956 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.520236969 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.522918940 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.522980928 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.523140907 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.524996042 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.525053024 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.525226116 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.527105093 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.527460098 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.528383970 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.528512001 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.529473066 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.530692101 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.532315016 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.532378912 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.532495022 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.534224033 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.534538984 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.535526037 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.536762953 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.536982059 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.538229942 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.538271904 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.538485050 CET	59422	443	192.168.2.3	34.96.106.200

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:21:18.541192055 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.546245098 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.546478987 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.547900915 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.549462080 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.549479008 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:18.549693108 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.576437950 CET	59422	443	192.168.2.3	34.96.106.200
Feb 25, 2021 22:21:18.604996920 CET	443	59422	34.96.106.200	192.168.2.3
Feb 25, 2021 22:21:20.497664928 CET	58784	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:20.547858953 CET	53	58784	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:21.675159931 CET	63978	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:21.729198933 CET	53	63978	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:24.613512039 CET	62938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:24.666445017 CET	53	62938	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:34.589693069 CET	55708	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:34.650808096 CET	53	55708	8.8.8.8	192.168.2.3
Feb 25, 2021 22:21:47.053936958 CET	56803	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:21:47.115098000 CET	53	56803	8.8.8.8	192.168.2.3
Feb 25, 2021 22:22:00.016099930 CET	57145	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:22:00.073334932 CET	53	57145	8.8.8.8	192.168.2.3
Feb 25, 2021 22:22:02.371202946 CET	55359	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:22:02.436384916 CET	53	55359	8.8.8.8	192.168.2.3
Feb 25, 2021 22:22:02.931535006 CET	64124	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:22:02.994631052 CET	53	64124	8.8.8.8	192.168.2.3
Feb 25, 2021 22:22:03.159104109 CET	49361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:22:03.237355947 CET	53	49361	8.8.8.8	192.168.2.3
Feb 25, 2021 22:22:03.314393044 CET	63150	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:22:03.384252071 CET	53	63150	8.8.8.8	192.168.2.3
Feb 25, 2021 22:22:03.404839039 CET	53279	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:22:03.469728947 CET	53	53279	8.8.8.8	192.168.2.3
Feb 25, 2021 22:22:05.884162903 CET	56881	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:22:05.938848972 CET	53	56881	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 22:21:04.451658010 CET	192.168.2.3	8.8.8.8	0xd2a6	Standard query (0)	bss.edu.ge	A (IP address)	IN (0x0001)
Feb 25, 2021 22:21:05.793093920 CET	192.168.2.3	8.8.8.8	0x5ba4	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Feb 25, 2021 22:21:09.520611048 CET	192.168.2.3	8.8.8.8	0xbf4d	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:21:09.711905956 CET	192.168.2.3	8.8.8.8	0xa2f	Standard query (0)	bss.edu.ge	A (IP address)	IN (0x0001)
Feb 25, 2021 22:21:13.968828917 CET	192.168.2.3	8.8.8.8	0x3a8d	Standard query (0)	www.bespro utable.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:21:17.110569954 CET	192.168.2.3	8.8.8.8	0xff2f	Standard query (0)	static.par astorage.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:21:17.462133884 CET	192.168.2.3	8.8.8.8	0xbe25	Standard query (0)	www.wix.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 22:21:04.509100914 CET	8.8.8.8	192.168.2.3	0xd2a6	No error (0)	bss.edu.ge		91.239.207.130	A (IP address)	IN (0x0001)
Feb 25, 2021 22:21:05.841770887 CET	8.8.8.8	192.168.2.3	0x5ba4	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:21:09.586908102 CET	8.8.8.8	192.168.2.3	0xbf4d	No error (0)	clients2.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:21:09.586908102 CET	8.8.8.8	192.168.2.3	0xbf4d	No error (0)	googlehosted.l.google usercontent.com		142.250.184.65	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 22:21:09.829623938 CET	8.8.8.8	192.168.2.3	0xa2f	No error (0)	bss.edu.ge		91.239.207.130	A (IP address)	IN (0x0001)
Feb 25, 2021 22:21:14.055022001 CET	8.8.8.8	192.168.2.3	0x3a8d	No error (0)	www.besproutable.com	www101.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:21:14.055022001 CET	8.8.8.8	192.168.2.3	0x3a8d	No error (0)	www101.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:21:14.055022001 CET	8.8.8.8	192.168.2.3	0x3a8d	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:21:14.055022001 CET	8.8.8.8	192.168.2.3	0x3a8d	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:21:14.055022001 CET	8.8.8.8	192.168.2.3	0x3a8d	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Feb 25, 2021 22:21:17.159712076 CET	8.8.8.8	192.168.2.3	0xff2f	No error (0)	static.parastorage.com	td-static-34-96-106-200.parastorage.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:21:17.159712076 CET	8.8.8.8	192.168.2.3	0xff2f	No error (0)	td-static-34-96-106-200.parastorage.com		34.96.106.200	A (IP address)	IN (0x0001)
Feb 25, 2021 22:21:17.534708023 CET	8.8.8.8	192.168.2.3	0xbe25	No error (0)	www.wix.com	wwworigin.wix.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:21:17.534708023 CET	8.8.8.8	192.168.2.3	0xbe25	No error (0)	wwworigin.wix.com	179.www.sv5.wix.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:21:17.534708023 CET	8.8.8.8	192.168.2.3	0xbe25	No error (0)	179.www.sv5.wix.com		185.230.61.179	A (IP address)	IN (0x0001)

HTTPS Packets

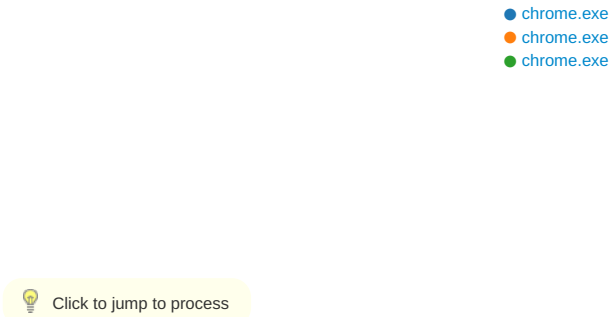
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 22:21:10.097187996 CET	91.239.207.130	443	192.168.2.3	49744	CN=bss.edu.ge CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 14 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Apr 15 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 22:21:10.234390974 CET	91.239.207.130	443	192.168.2.3	49745	CN=bss.edu.ge CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 14 01:00:00 CET 2021	Thu Apr 15 01:59:59 CEST 2021	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5708 Parent PID: 4088

General

Start time:	22:21:00

Start date:	25/02/2021
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://bss.edu.ge/transdoc/index.php'
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: 400 Parent PID: 5708

General

Start time:	22:21:02
Start date:	25/02/2021
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=1548,12077504496802862364,11838693349827509473,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1720 /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

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 6732 Parent PID: 5708

General

Start time:	22:21:07
Start date:	25/02/2021
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=audio.mojom.AudioService --field-trial-handle=1548,12077504496802862364,11838693349827509473,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=4572 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Copyright null 2021