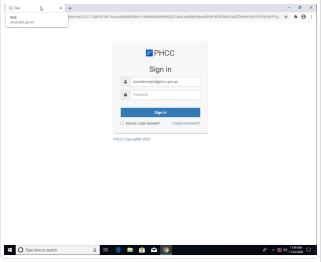
ID: 321463
Cookbook: browseurl.jbs
Time: 11:49:03
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

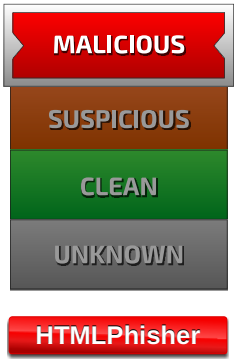
Analysis Report https://wtseticket.gb.net/jnhbtrvr4r/?He…

Overview

General Information

Sample URL:	http://https://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat@phcc.gov.qa
Analysis ID:	321463
Most interesting Screenshot:	

Detection

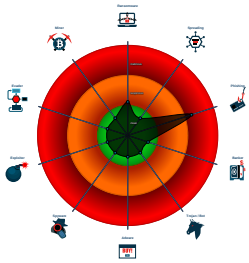


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Yara detected HtmlPhish_10
- HTML body contains low number of …
- No HTML title found
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5984 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat@phcc.gov.qa' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1708 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1516,10236018493698859480,3773363086378492193,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1872 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

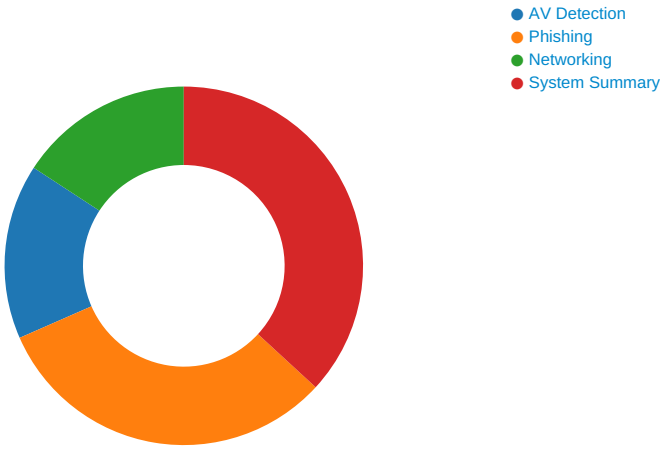
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

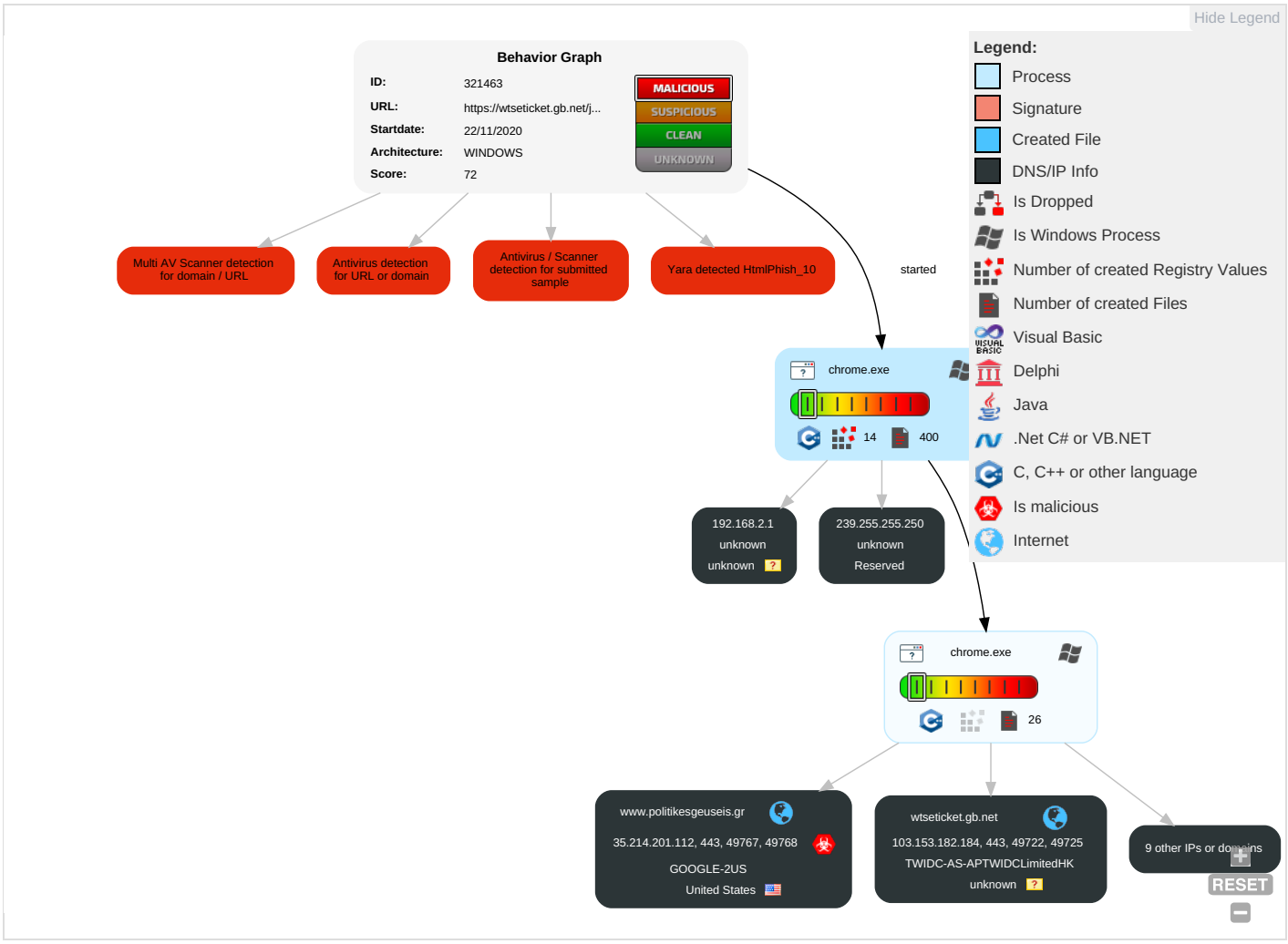
Phishing:

Yara detected HtmlPhish_10

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

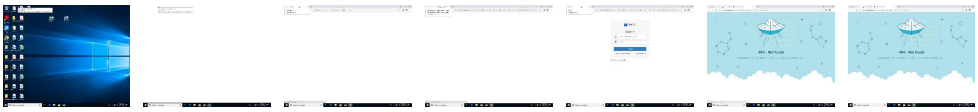
Behavior Graph

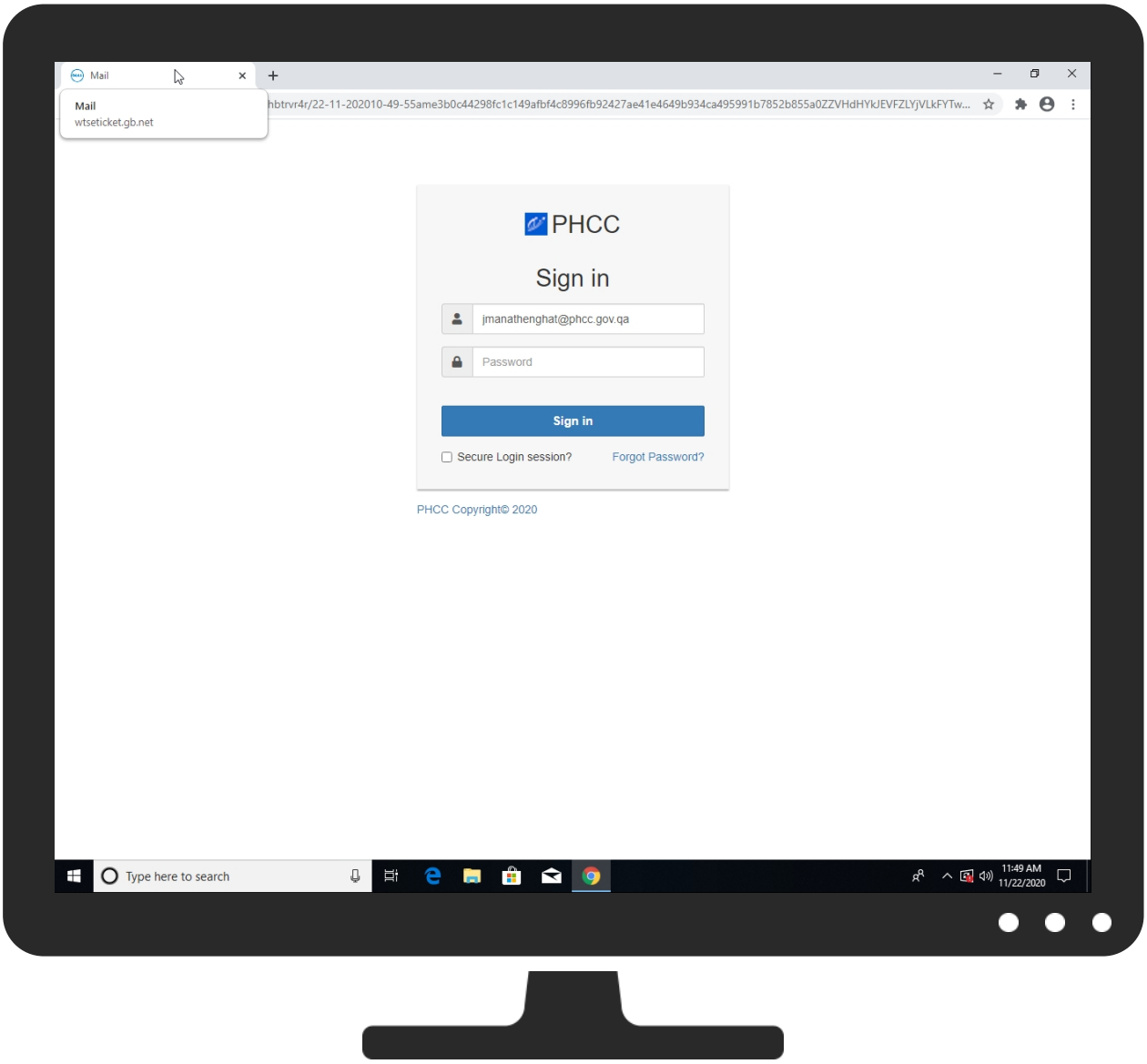


Screenshots

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://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat@phcc.gov.qa	1%	Virustotal		Browse
http://https://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat@phcc.gov.qa	0%	Avira URL Cloud	safe	
http://https://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat@phcc.gov.qa	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat@phcc.gov.qa	100%	UrlScan	phishing brand: generic generic email	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.politikesgeuseis.gr	8%	Virustotal		Browse
wtseticket.gb.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://wtseticket.gb.net/jnhbtrvr4r/22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0ZZVHdHYkJEVFZLYjVLkFYTwGbBDTVKb5K/?Key=22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0ZZVHdHYkJEVFZLYjVLkFYTwGbBDTVKb5K&rand=13InboxLightaspxn_22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0ZZVHdHYkJEVFZLYjVLkFYTwGbBDTVKb5K_a0ZZVHdHYkJEVFZLYjVL-&baf44faa1aca4678dda1777f816dc02ec58281cb8f0417fdc8f6d408390804e2#jmanathenghat@phcc.gov.qa	100%	UrlScan	phishing brand: generic generic email	Browse
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://dns.google	0%	URL Reputation	safe	
http://https://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat	1%	Virustotal		Browse
http://https://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat	0%	Avira URL Cloud	safe	
http://https://wtseticket.gb.net	0%	Virustotal		Browse
http://https://wtseticket.gb.net	0%	Avira URL Cloud	safe	
http://https://www.politikesgeuseis.gr	0%	Avira URL Cloud	safe	
http://https://wtseticket.gb.net/n	0%	Avira URL Cloud	safe	
http://https://www.politikesgeuseis.gr/cricl/oauth/site/service/demp.php?email=info	0%	Avira URL Cloud	safe	
http://https://wtseticket.gb.net/jnhbtrvr4r/22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649	0%	Avira URL Cloud	safe	
http://https://wtseticket.gb.net/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.politikesgeuseis.gr	35.214.201.112	true	true	• 8%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
wtseticket.gb.net	103.153.182.184	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.16.193	true	false		high
stackpath.bootstrapcdn.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high

Contacted URLs

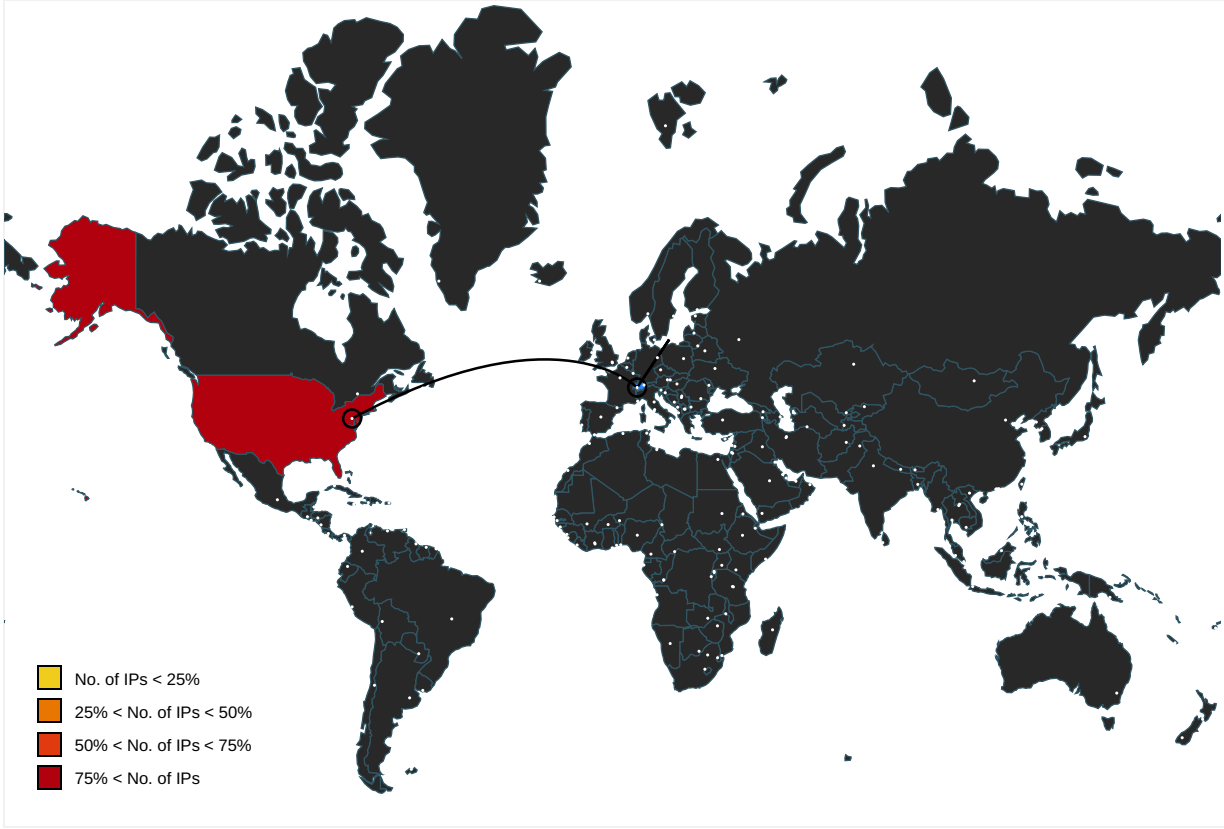
Name	Malicious	Antivirus Detection	Reputation
http://https://wtseticket.gb.net/jnhbtrvr4r/22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0ZZVHdHYkJEVFZLYjVLkFYTwGbBDTVKb5K/?Key=22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0ZZVHdHYkJEVFZLYjVLkFYTwGbBDTVKb5K&rand=13InboxLightaspxn_22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0ZZVHdHYkJEVFZLYjVLkFYTwGbBDTVKb5K_a0ZZVHdHYkJEVFZLYjVL-&baf44faa1aca4678dda1777f816dc02ec58281cb8f0417fdc8f6d408390804e2#jmanathenghat@phcc.gov.qa	true	• 100%, UrlScan, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	eee21476-17e8-42b7-90c0-2f0a91af8bbd.tmp.1.dr, cc5a7900-931d-49f1-a8f7-e43f714d350a.tmp.1.dr, 435e2e3c-1f69-46b7-b5d9-e6261d0e39f4.tmp.1.dr, 6f40c4ef-a496-4944-9447-fe47f0482ae6.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://a.nel.cloudflare.com/report?s=MyBXcp0KgAenI0KA0d3ypM8TQvkhxOO%2F26deAQyh%2F58ANKLihmeexCZpxm	Reporting and NEL.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ka-f.fontawesome.com	6f40c4ef-a496-4944-9447-fe47f0482ae6.tmp.1.dr	false		high
http://https://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat	History.0.dr	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	timesbi.ttf.0.dr	false		high
http://https://wtseticket.gb.net	Current Session.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://code.jquery.com/jquery-3.1.1.min.js	2a9e04a7d6429d53_0.0.dr	false		high
http://https://www.politikesgeuseis.gr	6f40c4ef-a496-4944-9447-fe47f0482ae6.tmp.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com	6f40c4ef-a496-4944-9447-fe47f0482ae6.tmp.1.dr	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	f424d79f54aceb83_0.0.dr	false		high
http://https://wtseticket.gb.net/n	f424d79f54aceb83_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com	6f40c4ef-a496-4944-9447-fe47f0482ae6.tmp.1.dr	false		high
http://https://kit.fontawesome.com	6f40c4ef-a496-4944-9447-fe47f0482ae6.tmp.1.dr	false		high
http://https://www.politikesgeuseis.gr/cricl/oauth/site/service/demp.php?email=info	Current Session.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	6dfc5527c5800d4a_0.0.dr	false		high
http://https://maxcdn.bootstrapcdn.com	6f40c4ef-a496-4944-9447-fe47f0482ae6.tmp.1.dr	false		high
http://https://wtseticket.gb.net/jnhbtrvr4r/22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com	6f40c4ef-a496-4944-9447-fe47f0482ae6.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	435e2e3c-1f69-46b7-b5d9-e6261d0e39f4.tmp.1.dr, 6f40c4ef-a496-4944-9447-fe47f0482ae6.tmp.1.dr	false		high
http://https://wtseticket.gb.net/N	6dfc5527c5800d4a_0.0.dr	false		unknown
http://https://kit.fontawesome.com/585b051251.js	6bc3c417e8323bac_0.0.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	e722df1969b866c0_0.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=awNAGJ0PD7Uypw7DW808mwRXrJ1Vtz77aYNqvy8IOHVR%2BvxdcrHAgZ9VOgRJ	Reporting and NEL.1.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://wtseticket.gb.net/	3c79335a95946c3c_0.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.214.201.112	unknown	United States		19527	GOOGLE-2US	true
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
103.153.182.184	unknown	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	false
172.217.16.193	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321463
Start date:	22.11.2020
Start time:	11:49:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat@phcc.gov.qa
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:	14
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:	mal72.phis.win@31/179@9/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.politikesg euseis.gr/cricl/oauth/site/service/demp.php? email=info@dell.com#
Warnings:	Show All • Exclude process from analysis (whitelisted): 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): 52.147.198.201, 172.217.18.13, 172.217.16.142, 216.58.206.14, 173.194.187.8, 173.194.182.74, 209.197.3.24, 104.18.22.52, 104.18.23.52, 172.217.16.202, 172.217.18.106, 172.217.22.10, 209.197.3.15, 142.250.74.195, 2.20.142.209, 2.20.142.210, 216.58.212.163, 172.64.203.28, 172.64.202.28, 216.58.208.36, 216.58.205.234, 172.217.18.10, 172.217.18.170, 216.58.207.42, 216.58.207.74, 216.58.206.10, 172.217.16.170, 216.58.208.42, 172.217.23.106, 216.58.212.138, 172.217.22.42, 172.217.16.138, 172.217.22.106, 216.58.212.170, 142.250.74.202, 172.217.23.170, 51.104.139.180, 92.122.144.200, 20.54.26.129, 51.103.5.186, 51.11.168.160, 92.122.213.247, 92.122.213.194, 172.217.16.131, 173.194.182.233, 172.217.18.99 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, au.download.windowsupdate.com.edgesuite.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, r3---sn-4g5e6ns6.gvt1.com, ka-f.fontawesome.com.cdn.cloudflare.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, par02p.wns.notify.windows.com.akadns.net, clients2.google.com, redirector.gvt1.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, update.googleapis.com, r4.sn-4g5e6nsz.gvt1.com, www.google.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, firebasestorage.googleapis.com, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, client.wns.windows.com, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, ajax.googleapis.com, fonts.gstatic.com, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, www.googleapis.com, r5.sn-4g5e6ns7.gvt1.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, r4---sn-4g5e6nsz.gvt1.com, blobcollector.events.data.trafficmanager.net, cds.j3z9t3p6.hwcdn.net, clients.l.google.com, r5---sn-4g5e6ns7.gvt1.com, r3.sn-4g5e6ns6.gvt1.com • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:49:55	API Interceptor	4x 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 GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Size (bytes):	235744
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	3072:UcMqZVCp8pwcMqZVCp8pwcMqZVCp8pwcMqZVCp8pj:UPxauPxauPxauPxap
MD5:	E828503A02D13EE56F6F882EC40A3841
SHA1:	C9854C8D019EC8EDCACD970882DF4AD1DC60FBD2
SHA-256:	0606ED099C353DA4B453616F9CC6CB2B1938401CEF5105A409948924639EE8E1
SHA-512:	9DAB1E8F7F935B78F9293E0683B0866108B37D7DE92F42FE824A5C93447039641C361AE7DE8DF0F23A59E43ABF0E7C36880CE625DB22AF14C5881C1B5D6CE41
Malicious:	false
Reputation:	low
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	3.1418912272327546
Encrypted:	false
SSDEEP:	24:8kPcUQU76akPcUQU76SzWkPcUQU76RkPcUQU762:v1EV1EA51Eo1E2
MD5:	3D296B69D9FC30BA5B631A0BFB069C11
SHA1:	7F177A92336DF3BCAC99513B3588A4CF1DEC971D
SHA-256:	6DFE052D718316AE08FC6CB6728F36A886E96A04A1ADAE038D4B9C1CE180961D
SHA-512:	73E9FD30088D062BB72C0E1A85E2597486FC136066CB4A66E786CBF4CB801327B5655C72DEF270CA4BA450EC564E8DC9DC282C5AA4FD360B78177BEA38DCEE D4
Malicious:	false
Reputation:	low
Preview:	p..... ....._j.....(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s. t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...p..... .....(..... .....Y.....$.....8...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..."..0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...p ....(..... .....Y.....$.....8...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..."..0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...p..... .....Q.*...

C:\Users\user\AppData\Local\Google\Chrome\User Data\592dd87b-b532-4766-bed9-f49af3d7b360.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	95428
Entropy (8bit):	3.751724600373279
Encrypted:	false
SSDEEP:	384:t7U7jB+A1KRdVKAHCNHrkvzZ30zxgH5QGonryNXzxktNpsr2Lm2i8O5HH/gOt1v0:NeKl9q9cI0eLbN9InnupKLZ3Re
MD5:	36C549EE3D10D732BC80AECE4FC776F0
SHA1:	230AC2FD8D3F2DCBE479C50E3EE44F571C38412D
SHA-256:	742C639202E0D1AD500967228A3D05FED5F40F871DF4E0B226DEB772177239ED
SHA-512:	A5943762198CD2F1795FB47D51302CC3EB870A48ABBA19A176DEF5921ED9C6384DC71E8A9EABF5AA0BE1789A73B9C97919E0CA5510AC355066A9F43EA23C79 B
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....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\778f627f-8e73-492d-82f2-c06c8ea28815.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):	162691
Entropy (8bit):	6.083116448814815
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\778f627f-8e73-492d-82f2-c06c8ea28815.tmp	
SSDEEP:	3072:lAA2NNCxQM9b0q+szv+tnMIGFcbXafIB0u1GOJmA3iuRR:irExQM9b7fD+ZMHaqfIlUOoSiuRR
MD5:	8C5321E328ED26544FE728F305C54C0E
SHA1:	E0A1BE50008876345AB478B8D89B7149664D3CD3
SHA-256:	3D83E66BABFE08DF6443B255985F267CDA6637BAEC95071AB6C2A9C708B941F9
SHA-512:	BDEF14160D2BBF7E52F1D01F130BACAC44302AABFAA3B1F058F11E30FF85D8C0D048CDE808D1809EF697930194AEB136D395D126E14EF639D9F01D159E56FC0
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":1.606074594850637e+12,"network":1.606042197e+12,"ticks":97852424.0,"uncertainty":4881188.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016631053"},"plugins":{"metadata":{"adobe-flash-player":{"displ

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0fc790de-6164-4b6b-bfd4-4f473c565544.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):	5047
Entropy (8bit):	4.979827620628181
Encrypted:	false
SSDEEP:	48:YcPUkPklwHjhcnqA8RqTlYqlQuoTw01H3CH3G/s8C1Nfct/9BhUJo3KhmeSnpBkv:ntYqX4pcVVok0JCKL8Bk818bOTQVuwn
MD5:	1220FDC5B664488CE9BE88ACF8F6C6F6
SHA1:	39601918A0D072F89478E5BF9EABCE090EAB5AFF
SHA-256:	FFF93F1EC814FD4F2BAC62CCF18E005D5A9989BE2E1D0D19B55DF5295512EF84
SHA-512:	5C4EBAD52CBAFA0F2CD8B7ADB0D2881CA888469816BC4667FF99837AF8BB5F1499D70B5254E28EB293A294A132A56270E0BE7BF9DA47D551678CA8D30E9856B8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250548191876782","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",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1c33f07f-c79a-4a4e-a631-86b132a81d7f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22613
Entropy (8bit):	5.535599653837409
Encrypted:	false
SSDEEP:	384:TjUtFLlXGXO1kXqKf/pUZNCgVLH2HfDRrUvHGRnTUjOr44:kLlcO1kXqKf/pUZNCgVLH2HfVrUfGRnR
MD5:	382E8E993E69F2D72D62C5C0630E3003
SHA1:	C8512F573096DAB40B9AF2E3D64268B5951AF22D
SHA-256:	AA6DF132853A8A9D80527B682183BB3B0A4EB0E1A8C3F6FD0AD479D8EDEAA466
SHA-512:	FC788F016F168ABCACA19737F96C9646EECAF8E6381C76E2B56447B8685FACE875845EF9A41BCC1D196AD52372A31802A2797257DCEFFA23133A30CA7F13002

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1c33f07f-c79a-4a4e-a631-86b132a81d7f.tmp	
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":"13250548191642391","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\2013f5d8-61c4-464d-a9ce-e22fcc632158.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\435e2e3c-1f69-46b7-b5d9-e6261d0e39f4.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\6f40c4ef-a496-4944-9447-fe47f0482ae6.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):	3733
Entropy (8bit):	4.884253482541677
Encrypted:	false
SSDEEP:	96:JTOXGDHzpJt/0QYr6ut566GImzCHzmnGTG5GRhH:JTOXGDHzpJGQYr6ut566GIKCTmncQo
MD5:	1DED81BB42810933EE91A63C1F7CB0E4
SHA1:	D4D1EE63515CD5EC11FD5F75BEA6C08720A22838
SHA-256:	BF2FD97D8D661A8588002B560D79082AFC544D966D88E177835DC270F4C7A652
SHA-512:	15C6DE0C3707C745D83C07701B02F86D14AAC164432B5A12DA51BF2718E5DF3B09BA6A9CB4F74EB0A63E3664CAD991F240DAB0EC5AF01C9026164B4EB7EAB881
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6f40c4ef-a496-4944-9447-fe47f0482ae6.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.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":"13253140194471000","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253140194487906","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253140194642619","port":443,"protocol_str":"quic"},{"advertised

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\96827182-3a3c-4502-b172-5a8014d02298.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):	5.535591566242275
Encrypted:	false
SSDEEP:	384:TjUtFLlXGXO1kXqKf/pUZNCgVLH2HfDRrUvHGcnTUj1r4UV:kLlcO1kXqKf/pUZNCgVLH2HfVrUfGcny
MD5:	0127A4190C84FD2AC47C4136827681DE
SHA1:	77907A05D65F5A6FE9807E11A6C795CA09FC1ECC
SHA-256:	4BC1F4016FB933147628A5DE47B13876CAA49DCF835A2CC500ABDB6DF01F5136
SHA-512:	F6906361C3EA2D048FB87BBF648393C9E76126927E1B965FD85E0171FB28DCD09DF9B67F42211342E8987AE892DA2BF951A8CE96DE6D6F20048CE0ED7112227E
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":"13250548191642391","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9dbcc575-90f4-4388-a971-1eef8f7f1054.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):	2127
Entropy (8bit):	5.573990187625183
Encrypted:	false
SSDEEP:	48:Y1CejSZ+V/t6ZkHS2VwUC6UUhjeUCKU+qPeUer2Uefh9wUkUenw:/2HV/LiUHUUQUCKUVPeU9UEAUkUD
MD5:	8DF8BE6A0923623E3D62A8E63E1B9717
SHA1:	8CBF1D3D81EF0D8C8675265F99E7DF03AEC0C683
SHA-256:	8B2D6BAAD317FADEF661689508CF78DADA29967AEA0F8AF035015388E576FF8B
SHA-512:	CC6E5FBE5A815FBF88CAE3A61C0DCD1067FA50DB36E473EB162560BCB3CA612B75FF77A700C28A94390FD88ED76F38BD6F56BD972B8E2392036A6BBF102CCE56
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606679397.098973,"expect_ct_observed":1606074597.098973,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"Dj/8vXyAvSHjPvTdlUWhkVV3qt7EF4IIBub25XWm+/4=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606679395.792094,"expect_ct_observed":1606074595.792094,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606679395.690491,"expect_ct_observed":1606074595.690491,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"PmHKo9+NfFu9AjQSxw3MoTtfuXlu9G3fM8KGQt4xie4=","nik":[]}],"sts":[{"expiry":1621854595.792086,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606074595.792089},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o

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):	5.218254474645968
Encrypted:	false
SSDEEP:	6:vhAVq2PWXp+N23iKKdK9RXXTZIFUtwgDuAgZmwygDuAIkwOWXp+N23iKKdK9RXXH:vhAVva5Kk7XT2FUtwgDuAg/ygDuAI5fv
MD5:	91C0EF95CD0EF76EB3295E523AB5507E
SHA1:	76BECF68F3B28A9EBC2C82DAA938F5BAD0BABC07
SHA-256:	ADE4C06FF7D1399864385D0C51BFC8777956D099AF35D3EBB0D27CA74885B086
SHA-512:	1FEAA7BC54A690D0A01D4C1D3906084DD132CF5D26301F3CC7678858B6D6BA29F577879A008E0A641EDC0EA29D3016F53DF9C7C99D9243B9848D1B01168354C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2020/11/22-11:50:03.587 1bb4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2020/11/22-11:50:03.591 1bb4 Recovering log #3.2020/11/22-11:50:03.591 1bb4 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):	5.205189094959463
Encrypted:	false
SSDEEP:	6:vhAVq2PWXp+N23iKKdKyDZlFUtwg44AgZmwyg44AIkwOWXp+N23iKKdKyJLJ:vhAVva5Kk02FUtwg44Ag/yg44AI5f5K1
MD5:	19090F450A9910398713DF931AF5C533
SHA1:	385E236C97C4B6D75F2F250B2248500F616A5DA2
SHA-256:	068AA451BD04493148BCD33606393540EA3B1B7BEEDB767661F7BAEA6165D93C
SHA-512:	62E00AB1C820D4DDF33E7AADFF83FBF57B801C46BED34DFE6E49A24CBA8C3BA1F5C62288A4262D8BCC1C1102E96F366DCACF329880DA49BF0D76C7CF7EB0423
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:50:03.569 1bb4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2020/11/22-11:50:03.572 1bb4 Recovering log #3.2020/11/22-11:50:03.572 1bb4 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\2a9e04a7d6429d53_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.415234133994706
Encrypted:	false
SSDEEP:	3:m+ljFgl/lA8RzYP2FycyG8ZFvDLWPAtELoz6ll/lHCtl/hN9hodkRmbxlXpK5kt:mugPYeMjMdWOlgX/hN9hofbtK6t
MD5:	BDFD4EDA7CAC8075186D78DEBD4EF9B2
SHA1:	EE225ADF9A07565654DA510517CF8FEC3428A4E4
SHA-256:	677788A3D42EB675C3E85185D5DF86157D196439BC7FC21EF8BAE26CF7746D94
SHA-512:	360C874C158E57F98A510425628C912202F237C16634991F1058396E938F4F23CA3A17242C7F5CCCC0F58C81D99CBA2F3D918C4464D1CB2FA7CED41E3C20C7E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K...O....._keyhttps://code.jquery.com/jquery-3.1.1.min.js .https://wtseticket.gb.net/..V.M./.....V.....BS....s.<..!.A.....3:h...Mt..A..Eo.....u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3c79335a95946c3c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.9293873190856035
Encrypted:	false
SSDEEP:	6:m8eVYSHT8NWQAlKPUQyrMdilg3PmFMwb4dK6tZWs5gb2IUNnczFMwb4W:Sz8NWQCUUNMUlEmFMUEawgbmNnczFMU
MD5:	6CE7D88092AA6237860D705AD33147BE
SHA1:	4B64D31D07505BBDC3477589EDC470E42F20F163
SHA-256:	F8EF280E224AF475E8455D9CEF08D66C248774580EE9A11DCBC1FDDA3D7A3A25
SHA-512:	AE23E13CD361483FE40913846EACFE11FA91B76DA92584625276A820217F11734A4C20E40EE5FB2CB06A2D202D583D54B545CEFD0B7598E5862987D190CA58C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`....:.Y...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://wtseticket.gb.net/..H.M./.....S....j*..12..,..z7@..@.~/.|..-..A..Eo.....A..Eo.....H.M./.Po..4FE867182085280414740B1C797D1623D56660CDE0C0FCD091E64D974E3AA0D2S....j*..12..,..z7@..@.~/.|..-..A..Eo.....g.(L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6bc3c417e8323bac_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.44254412691679
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6bc3c417e8323bac_0	
SSDEEP:	6:meWPqEYlNYpSVkBMddjalgiXl0gVNhAGYF/ZK6t:vIq0pSVYMTmlbRNg
MD5:	F409859AB535F413C50161340D55DE9D
SHA1:	A0C46861A285BD9161F0C9F5938921BCD59CEFEB
SHA-256:	558678F21D04F4CBC1330728D09EDD264A259F4CA39411E92148404299183713
SHA-512:	AA327D7EACD4CAD65532B1B286F32B9AF04EC2AFDD6A55E80A565376EE385CCC16BA9AC4582C6770AC60D0DF2C4DB9DD01FB14828A6D8B7F74E1D5316C782D93
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....4.j...._keyhttps://kit.fontawesome.com/585b051251.js .https://wtseticket.gb.net/.yH.M./.....Y.....`.s..}....r.A.....ci..5{...A..Eo.....`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6dfc5527c5800d4a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.477088033356978
Encrypted:	false
SSDEEP:	6:mfYET08NaYWbVOqZoMd3lgrwCHA6A/LihK6t:Wg8NaY8ZoMVlwwCg6gi
MD5:	40C4AC8EA7BDC15301B2981409DF3D69
SHA1:	E506FC48E74153D0CB1AE1B96B0165327B610B85
SHA-256:	9BB824E1800CFEC64EF1F932777AB5F4D05451E7022606B8E134EEF4F01ADA27
SHA-512:	85E6CA1D6F931B06E67E35A0528B8B1B3AF9C235FBDF82DD14416A10940A2204AE86C2321E2D485328792CA6CFDCE2D504B93D3F5616A32D12FFF69E35DAAFBE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://wtseticket.gb.net/N.J.M./.....r!....'.v[.!..D...wg&...6./mO..A..Eo.....O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e722df1969b866c0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.430239925126851
Encrypted:	false
SSDEEP:	6:mDnY68E9xEEUgLEroMd0tlgmEtfWQVgl+hK6t:yYgnMitluR
MD5:	5BBB1DD6C31B78592807EC01599BCB60
SHA1:	252E8C2991B5A59C44AFC03971046F34B84F47C4
SHA-256:	113BB658C1EE70771E3E0E39FD61A125D3F1A733F93D6C1058BB433C221ACA52
SHA-512:	54428AE1E90CE5BC6DE9644F4E439D3F8DFEB6A219F424057A42140CE5B00CCB64B2496E1FB80E0E4564FE26B708A86D9B7C0AA17208F64495F5AB32357B7EAF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....v.]...._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://wtseticket.gb.net/..S.M./.....8P4.g+J.8...."..u.9.K.8.y....A..Eo.....`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f424d79f54aceb83_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.36479007038885
Encrypted:	false
SSDEEP:	6:mkYkb8E9xEvAEroMdAslgwEt/FYWXGYkthK6t:1v4aMSslTsqWXGT7
MD5:	B0E46C1FC511A54173C9CD16F0A3B298
SHA1:	E459B097379F4527A2CC093BB1EBBB7740F7CEFC
SHA-256:	DA3F294EC4B2294A9A0720454BB68894DDAED2241537B2B060BE40F6CE5B8570
SHA-512:	5DFC08965426997E53E1FDE0A5C149C43AF0159C5FA9A9372A9A33DE0A297242DEE6D6A0C20E20A7EC00D12B8AC2BE0AA211C8D0EC20FE2EEEF66D96196596B2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....7?f...._keyhttps://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js .https://wtseticket.gb.net/n.T.M./.....D.....LYo.=...kl.....].IN.IA..A..Eo..... k.+.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f56ae8e23c0de173_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94200
Entropy (8bit):	5.772046703318957
Encrypted:	false
SSDEEP:	1536:nt+r+pclQ7k51jvaz1SjW4kUmismiWuxu2vNQZrJLj39G1qvSPY:K+OFDE0kTisuWu2lQZpk1qP
MD5:	9002D41373576AA0D8E60C992B944601
SHA1:	188EDB39E6D940E8F602E8F380CAB86E48050515
SHA-256:	A4CE67D114F475E2C8ED19E582FFB45902515462B9D362516AAEF5A200530DF3
SHA-512:	69890894178F62B3776B20EA4734B760EEB60EDC2D499EAF0757DF831C7C3879F6485A56CC81FAB13F3376C777F2F1B525CD28935C3D6DDCFEB9D40455DB348
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....6....4FE867182085280414740B1C797D1623D56660CDE0C0FCD091E64D974E3AA0D2.....'.JN....O ....n../.....!..... .....(S.H..`L....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@.....module....Q.@.H$.....exports...Qc...]....docume nt.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.jsa..... ...D`....D`....D`.....`z...&...&..!.&....&.(S....!..`.C.....q.L`.....Rc@.....M.....Qb.....d.....Qb"..B....e.....Qb>-.....f.....Qb.....h.....S...Qb.AC.....j.....Qb.f.....k.....Q b.g.....l.....Qb.....n.....Qb6H.....o.....Qb>.#.....p.....Qb.l. ....q.....QbZ..7....r.....Qbz..I....s.....R....Qb...J....v.....Qb&.V....w.....QbJJ.....x.....Qb:.....y....

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):	4.914820485491842
Encrypted:	false
SSDEEP:	6:EtrltxGltk5lOMZKlCtrKlRlmoQtlp0PfelkazQ3zbn3pHkQ+IRwHyR6:cltgM5cl4ov85/0PGDzyz7V4h06
MD5:	083533DAE805EF9900EC43F27F9E13C4
SHA1:	747D1DE7729DF11ADF2888415C7767F480E74100
SHA-256:	32E36ADB61D0A6CB40730B57FBA341352BF00A8EA4742BF72F1013962CDCCC33
SHA-512:	B7A31932055DFAD431D36AD14F647E32802AE4B31441FE5B5B13076EBA2C6F9DB06A8ED8A234033510B886EEDE4BB82EE13302751BD1452F9F7553E7D91B15D E
Malicious:	false
Reputation:	low
Preview:	.....@.oy retne.....T..$..AM.M./.....s..<..j..AM.M./..q.....f.i.."..AM.M./.....J...'U.m.AM.M./.....V.Af.v..AM.M./.....;2....k.AM.M./.....S.B...*.AM.M./..... <l..Z3y<..=.M./.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q....._.KPu../.....+<P|...X.KPu../ .....M.\.M./.

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):	1.125285961468879
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwPEvP19VHlcvIgAZOZD/FyXTP:TekLLOpEO5J/Kn7U/vZFrNOZaP
MD5:	7665606349D8C8FE0697A2301196BCF9
SHA1:	CBFD04AC245A97DAC16EB8A63EFD4FE020F43918
SHA-256:	9C098EE4D453B61F19288F570A1E5221988AC8F0127D4230BD4EB5A83C737402
SHA-512:	93379AC98A49B85B2A447301FBF4042F7CA9CB08CD0FDF9DC7F2AED7340E3DAAD8AC538EA5B6BC1E2E07B646C4A7ECE295881043B7592D0E9F17674EDB306(A5
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):	0.9689618480906617
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
SSDEEP:	24:BcLgAZOZD/JvxvqLbJLbXaFpEO5bNmISHn06UwE8:B8NOZJvxvq5LLOpEO5J/Kn7UH8
MD5:	5AEC9ABA2938199329119C28B6010585
SHA1:	03A9FA45A05F0518F551038DF1EBB53ED9003A02
SHA-256:	4FCA28866C915521C2B3066D3968FE8BA038F408F2CFC58B5C0E699FF327ECEE
SHA-512:	8E266A8C8F5A3A30C8768CFB59B65A91D42A706F31F96ABC6AAF4F875A517DF35C365E9B80A29F0A4F3B918492DBEBB70B070FE9E6944FCC5C9CBF83F8449CE8
Malicious:	false
Reputation:	low
Preview:	.....q*.!..... ....

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):	7211
Entropy (8bit):	4.177943907304816
Encrypted:	false
SSDEEP:	96:344TshhWJ61NgXNPM6/7shh/01NgXNPMH1NRE//VEDiqed:3ZTshhfwE6/7shhswEHm//ow
MD5:	10D2721687A3B8E387B622BF87E036A4
SHA1:	924670803A8140EF4D672EEB1BED024F131D9A82
SHA-256:	AFAAD11158DF00DA725E51F5F409A9FEF044BF3D15DC854FA1E618DDF7D8CDC2
SHA-512:	0EE07E4ABE9002EEBB37BF175ADA82A591E006E8624A17EF8310B20B857B272D29DFD766E7C5B0D6A2BDF38191E1687E3D24CC9BB94159D67F3FB4F635826F08
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...18d86b53_fb7f_4a1d_a5a4_b43cd6b3b319..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....https://wtseticket.gb.net/jnhbtrvr4r/22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0ZZVHdHYkJEVFZLYjVLkFYTwGbBDTVKb5K/?Key=22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0ZZVHdHYkJEVFZLYjVLkFYTwGbBDTVKb5K&rand=13InboxLightaspxn_22-11-202010-49-55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0ZZVHdHYkJEVFZLYjVLkFYTwGbBDTVKb5K_a0ZZVHdHYkJEVFZLYjVL-&baf44faa1aca4678dda1777f816dc02ec58281cb8f0417fdc8f6d408390804e2#jmanathenghat@phcc.gov.qa.....t...p.....h.....h.....`.....h.....p.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.223025008724659
Encrypted:	false
SSDEEP:	6:C9+q2PWXp+N23iKKdK8aPrqIFUtwkJZmwyk9VkwOWXp+N23iKKdK8amLJ:hva5KkL3FUtwG/y65f5KkQJ
MD5:	C0831CDE715E3186C6E323437B065E92
SHA1:	28D10C59A0D43AB1009BA39F03B2309392A0179B
SHA-256:	1B738F06FAA3FF1A109D839D9E64EEB582A20457BC3EF7E82546F3ABD75D71AF
SHA-512:	E783806586E131D922136DE65611C557DF6613616B3943F16A69F115DF82AEB2E8FF9AC3550E02B4B1F81161DB4742508CAD831A8735188B3150DE1D1003F13A
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:49:51.923 1488 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2020/11/22-11:49:51.924 1488 Recovering log #3.2020/11/22-11:49:51.924 1488 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT: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.....f.5.. .....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.190400247930555
Encrypted:	false
SSDEEP:	6:RGN9+q2PWXp+N23iKKdK8NIFUtwo7JZmwyoq9VkwOWXp+N23iKKdK8+eLJ:Rzva5KkpFUtwot/yoU5f5KkqJ
MD5:	FA6590B411F42A825D6DFC1FF607FCF8
SHA1:	C1E16DAF99B285BFE5D438F1E9A6257BC32D0E8A
SHA-256:	0D2D2720EF0E1C5A033912D1C2E24D2C59195A39676BE574B8D47FE729931719
SHA-512:	AFEA97F7786ED9F5A965E05D4C1708B045070CDA2F2CB27F510824A9C42F4CFA41F91699B294ECB34489A08D0386AC536A2E57C257B42B4845F202F74065AF97
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:49:54.100 1488 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2020/11/22-11:49:54.101 1488 Recovering log #3.2020/11/22-11:49:54.102 1488 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17938

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_1_metadata\computed_hashes.json	
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49I C
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41EIU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2I/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
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):	20480
Entropy (8bit):	2.614292655458195
Encrypted:	false
SSDEEP:	96:0BC2i/hhWshhKLoc59BqaN7+AoBy0/MsbhIh:mZi/hhWshhRFaNP0/MsbhIh
MD5:	0FACA10F3D056F011B5049B29C595B64
SHA1:	7DA170159905026D91F5E43FDAC33EF129C5A927
SHA-256:	876E6320869FCFC5075496292CD440FF998D671C6E410C96E9642240A013657F
SHA-512:	8D961CF52B934E894DA20AF30622975D27D4277803C6D9B8ECCA82F56E7F80007C16244505EA838FB2C1D4D05AAB1F2492569224542C6C8CA74916135EB33876
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Entropy (8bit):	0.776562620520789
Encrypted:	false
SSDEEP:	24:dJyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwBs13n:dJdBmw6fUKs13n
MD5:	FE272B02724E60F357B93A542FBB50D7
SHA1:	CCF15811C76009EEEDE3FA534A7B04BD31979D5B
SHA-256:	2EB8765EF857ED17C7AB47C9611231D21F76C3FD456CE578E59B036F0D67F0D0
SHA-512:	C803BD25EC98DFFC8812066541D05E2ACB4961D5B560348643B1407B4BE59719E41784E6F512AB0FA176A8043AA5438C04AEBC71B58DD7F20C9795856DBC852
Malicious:	false
Reputation:	low
Preview:	.....N..... ....

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):	5.228082831553659
Encrypted:	false
SSDEEP:	6:vcRNAVq2PWXp+N23iKKdK25+Xqx8chI+IFUtwgsuAgZmwyg0AIkwOWXp+N23iKKN:vGAVva5KkTXfchI3FUtwgsuAg/yg0AI6
MD5:	6D0FBF046EC32A8E4114C05B2A34968E
SHA1:	76F354462DBC3EA6E86C25F19D28C6805C0C1EC5
SHA-256:	3E71A3C1619E00EB0CA66C3BB73D5193A344A27A13722EFA909677B312F7FB35
SHA-512:	4F7B6C2A3532A32FD2088EF24D2EBC7BE84F29625C1EB80B3E0945A1AD72AD9A06427A76C3E7A356AB5D26D25B5C743A7131FA0CF6B9E3E7995506C80603F23
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:50:03.542 1bb4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2020/11/22-11:50:03.543 1bb4 Recovering log #3.2020/11/22-11:50:03.544 1bb4 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):	5.234293400902707
Encrypted:	false
SSDEEP:	6:vI4AVq2PWXp+N23iKKdK25+XuoIFUtwgLuAgZmwygG6LAIkwOWXp+N23iKKdK25y:vI4AVva5KkTXYFUtwgKAg/ygLAI5f5Ky
MD5:	76902ABF279DE6DCF8072350737FA094
SHA1:	0AE00164BC581C04327BEEF31240BEB7C693125D
SHA-256:	FEF1BBB9717B66EB0209B95CD8FAA2FB253D6DF3B4BBF539A0573A7060F22A3E
SHA-512:	AEF65D0C1EF478ECE39343F67B81325B93784BE0FCAEDE4C9F08662BC5D11BC4DD1D6B88750F1A816DC43A790B964C43EC8534E20198B6B91F3CA9103321DEA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Preview:	2020/11/22-11:50:03.536 1bb4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2020/11/22-11:50:03.537 1bb4 Recovering log #3.2020/11/22-11:50:03.538 1bb4 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):	5.179779719985346
Encrypted:	false
SSDEEP:	6:vvvAVq2PWXp+N23iKKdKWT5g1IdqIFUtwgIAgZmwygSyAIkwOWXp+N23iKKdKWTk:vvAva5Kkg5gSRFUtwga/yg35f5Kkg5gZ
MD5:	94EDFCE726DF84E8AD753EF5E413C6B6
SHA1:	A667EBE44BFD19026FC1B270701710F7F626CE8D
SHA-256:	B23356BC569829D9C1379BE26F079D5767DFC2200E06FBEC69842038F97834B4
SHA-512:	40D8C2B8C92F9E6E7BA3ECFA48222A69C2B9EF80AE6F11DEAD55107ABF2E3C8BBEE8FD25158811A8B9AC27A591F5241BFBAF0BBB80CA4279D57C2DBB5F67EB6B
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:50:03.431 1440 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2020/11/22-11:50:03.438 1440 Recovering log #3.2020/11/22-11:50:03.444 1440 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):	0.8705126531253687
Encrypted:	false
SSDEEP:	48:Tp9JXtY7tYytYCL9rtYmtYytYCL95+/u02tY7tYytYCL9OtYmtYytYCL9i9n:l3shhV/hhnPNshh0/hhg9
MD5:	ECC5F3987254CE5B621E940E4F7BEA50
SHA1:	274ABC2816647D19BFCBED02454ACEB28C5DB5B2
SHA-256:	EB6340463F97F8568DF9C0F7875DBAF1B4010CD813C9EC76344BFB7AF567D43E
SHA-512:	37923D1DEAC7368B294A55A47F192EFA260C7FF831946F3110EB28F8A4EFF35F942854EE03E3538355562AEB8A5E1C161173D19992C5A4E7DAFCA04AC433B36D
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):	2849
Entropy (8bit):	6.06120411067521
Encrypted:	false
SSDEEP:	48:ltYLEqtYZwogwxAo75PLrw2/5tYmtYytYCL92J96btY7tYytYCL97:lgDdoKQNh/hhmsshhB
MD5:	07566E9A996C260BA516767B9F04E3FE
SHA1:	9890BC0AECAD1F9E85B2406A0DB7D7363CDD2D3A
SHA-256:	2423E907784B93E80CE7E556AED41F1BD5627E39A53704AB2C09683D2B017FF5
SHA-512:	7E6C2A708D65660890CC733ED6959BFB51A2B3AF25FF9E6C46F90419F69225F1E9A963B59E65C650D41F2C5443AD3757F5B77DB7CC752061541683B30FC21256
Malicious:	false
Reputation:	low
Preview:	."......11..13inboxlightaspxn..202010..22..49.g55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0zzvhdhykjevfzlyjvlkfytwgbbdtvkb5k..a0zzvhdhykjevfzlyjvl.@baf44faa1aca4678dda1777f816dc02ec58281cb8f0417fdc8f6d408390804e2..gb..gov..https..jmanathenghat..jnhbtrvr4r..key..mail..net..phcc..qa..rand..wtseticket..56hbgfd3xs..helmeitas23*.....11.....13inboxlightaspxn.....202010.....22.....49...k.g55ame3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855a0zzvhdhykjevfzlyjvlkfytwgbbdtvkb5k.....56hbgfd3xs.....a0zzvhdhykjevfzlyjvl...D.@baf44faa1aca4678dda1777f816dc02ec58281cb8f0417fdc8f6d408390804e2.....gb.....gov.....helmeitas23.....https.....jmanathenghat.....jnhbtrvr4r.....key.....mail.....net.....phcc.....qa.....rand.....wtseticket..2...#.....0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....a.....b.....c.....d.....e.....f..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11662617582927648
Encrypted:	false
SSDEEP:	6:+DbYMg9bNFlWCj/l2+/l3lOv4/fMt76Y4QZVRtRex99pG/UUbqR4EZY4QZv8fO0i:+DEMqLBj/5t3lOv4nMWQA9LHZBQZ8fOb
MD5:	AD83DE903A6FDA229558EACBA22B9323
SHA1:	D546430FE15A681898B294E9D6C1BDAE89462B8E
SHA-256:	F283708011049780FC57496BCEF199FC8FA59BCA1CD9E25E00B64B5E45C28E40
SHA-512:	BED1597702E88302377F2A96960405AF6E003816CB984E948AB76529E35892C4C4FA2E48E33E1106636C5E4A75774907F77BA744E31CA97E951C6D5C7C0C22CE
Malicious:	false
Reputation:	low
Preview:	.....PJ..... ....

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):	2954
Entropy (8bit):	5.461786870733217
Encrypted:	false
SSDEEP:	48:KVhG2ZcX8a7V8MJz8dbxGZtpt4bQSefgGRNrS0U9RdiN9z:uJqX8a7V8MJAdbxGZtpt4bQ5fgGrrS0h
MD5:	61387B2ADF6A3139360A207BD9EC0CBD
SHA1:	679BC7FC20133B4063BEC29779B0F39F74B674BF
SHA-256:	A1576F430737D4FA990466FEDEB935E77B2D0F042D591AD812216CC103AE486A
SHA-512:	F1BF856F8FCB9984B03A69154D8BDB0CD6ED092438547E2BE9A0C972FD5628EC3DDFAA39AC04CD7BF1C8D8FA707B66A5600EC608BDE53DE535AAAB9BFB7B4940
Malicious:	false
Reputation:	low
Preview:	...^...*.....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..52446000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2020-11-22 11:50:04.80][INFO][mr.Init] MR instance ID: 8459c02b-6940-42de-bea7-96685345fcae\n","[2020-11-22 11:50:04.80][INFO][mr.Init] Native Cast MRP is disabled.\n","[2020-11-22 11:50:04.80][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2020-11-22 11:50:04.80][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2020-11-22 11:50:04.80][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2020-11-22 11:50:04.80][INFO][mr.CastProvider] Query enabled: true\n","[2020-11-22 11:50:04.80][INFO][mr.CloudProvider] I

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.1905311717101545
Encrypted:	false
SSDEEP:	6:T4q2PWXp+N23iKKdK8a2jMGIFUtw7pJZmwycDkwOWXp+N23iKKdK8a2jMmLJ:T4va5Kk8EFUtw7pJ/ycD5f5Kk8bJ
MD5:	324793EB449CA360E4FD5018C11550F8
SHA1:	E420207ECF03A1C21DC9DCCB7CE13CA0F618CA02
SHA-256:	AE3D81DAD5A9E07E2B8246E23C8159BEC1AE2027E8BD063B74C1C27805516AB1
SHA-512:	541ED9ABBA94A9DA53D7584A51EBD497ECD029FF62FF20D9255C8BBFDBF97CD4E3F55F6EC4B229A28159027E9371ADBD982918857F9E9DD7F31894178BDACEB3
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:49:51.675 1160 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2020/11/22-11:49:51.676 1160 Recovering log #3.2020/11/22-11:49:51.679 1160 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.207059050040406
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
SSDEEP:	6:fwL+q2PWXp+N23iKKdKgXz4rRIFUtw7iT1Zmwy7iFLVkwOWXp+N23iKKdKgXz4qG:4yva5KkgXiuFUtw7u/y7WR5f5KkgX2J
MD5:	1FC9CDDE929FE95A7FD0BA2B48D58F7C
SHA1:	41FD6AD6AB474719FE7254D4D3152F37D51C8C48
SHA-256:	BB389C2C4EA636EF4F7D687DF7BB62CC491F8C96E63ACE5724CDDCFC5F60C9C4
SHA-512:	A7D687102520AE256414909BC811E99220CE7A1CD3DCAFBEADA3D3D965FBE14303192E283690CB8CE6E45F811CE0ABB1B20CF3F13814861423E8F7CE4C4B7EC
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:49:51.949 11c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2020/11/22-11:49:51.951 11c8 Recovering log #3.2020/11/22-11:49:51.951 11c8 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\Reporting and NEL	
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):	28672
Entropy (8bit):	1.0813852566198552
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUduzvZojW6FQxO:wIElwQF8mpcS5K5eX
MD5:	C8F2BECCE0D9D2A63FFD3AD7D7D5FC69
SHA1:	A566AF08901AA1ABB375F88D8CB20BCBB32867EB
SHA-256:	74F1A06CE789656148B33F38BC080E6665AEBC05379E10C9353DFC0A7ACF672A
SHA-512:	5DE233FA8514D7A978FD70CC0E5A5C4B0053F826D15B4304A371719A3EE230A5E9372911023AC4C9E03E7D552AD42B5AF67B37B4766346C971D080685D297E09
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.626546086936788
Encrypted:	false
SSDEEP:	48:4AqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUd4:4AhIElwQF8mpcSm
MD5:	163AEBFC5A34E23664138C153DABFE6D
SHA1:	AE7C1D3AB76165349B0F5DCDCC3FE1095CF815ED
SHA-256:	27D3B2995FBDEDD73E2FFBECD246FDC3AAB1A620B4DBCBB81FC75499C29EA02E
SHA-512:	C56DE4821018A6AF88A75DE7534CE1D351604856C79BCE5F6F38A73E75AF2EC7BF6916877E89E3C7916099DF9E1616B342B0E6DC9C0E00D9B2FB4CACB7DD7CB
Malicious:	false
Reputation:	low
Preview:	.....h.>n..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
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):	5.222061784448966
Encrypted:	false
SSDEEP:	6:aGIq2PWXp+N23iKKdKrQMxIFUtwJXZmwyURFkwOWXp+N23iKKdKrQMFLJ:7Iva5KkCFUtwl/yURF5f5KktJ
MD5:	25D728474A019DC41EDB2B409AE3AAEF
SHA1:	975F9D0B1DAA49E894931F1FD698F05266F26013
SHA-256:	3FFB3E3D3009B378844D7A06E23BAB7DBC06489E27CA2137327406207C44F190
SHA-512:	2B6AA7C56999B6F0FC1211EBC46B972AA26B2B12BA6A641627ECBA3AB079F884A4DFB2F8419FB7751D16EF7F55401807C38E34C3B472DE74C5FD423C94020CF D
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:49:51.846 17d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2020/11/22-1 1:49:51.847 17d4 Recovering log #3.2020/11/22-11:49:51.848 17d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/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):	5.126740053085937
Encrypted:	false
SSDEEP:	6:NFUM4q2PWXp+N23iKKdK7Uh2ghZIFUtwiFpJZmwyiFpDkwOWXp+N23iKKdK7Uh2w:NFUM4va5KklhHh2FUtw4J/y4D5f5KkIT
MD5:	54C01DB7C00F2194C8BA233128916321
SHA1:	3AA33E4C3C2CD0BFE0F4AFF29E210ACC0D1BCC0E
SHA-256:	949AB0F892F2617E1621BA89B56587684829BF00CB4110C2BC5B943846D70508
SHA-512:	B6331639AFD2E2CDBFFA188F8E555C382B3FBD09B92677F841B2FB71A076E32E851AB471EC38F15B2B7AE5486EEBD9A8244F2E2D73EBA18B58408DFD5320C3D 1
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:49:51.620 1160 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2020/11/22-11:49:51.622 1160 Recovering log #3.2020/11/22-11:49:51.622 1160 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.251957844585565

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Encrypted:	false
SSDEEP:	6:Gq2PWXp+N23iKKdKusNpV/2jMGIFUtwlZmwyjOkwOWXp+N23iKKdKusNpV/2jMmd:Gva5KkFFUtwl/yjO5f5KkOJ
MD5:	61626348B402C308824124FEEF5408BB
SHA1:	A783317C0CA62AEA2C63B7BA06B67C458012810E
SHA-256:	7051591B92046BDEA10095F620572BE37B2D93FA8B0A2DF51B9BE285989D74B9
SHA-512:	979E725DCDBB055D57D781A3EFF974054EFE2009A3A01EBC9393B84E752EB2ED00FC648F56BB17C79B339C1572C3854151125DE8E94C1E0F8418CA314D5BDF1
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:49:51.901 17d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2020/11/22-11:49:51.902 17d4 Recovering log #3.2020/11/22-11:49:51.903 17d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.3198236722523955
Encrypted:	false
SSDEEP:	6:qdt+q2PWXp+N23iKKdKusNpqz4rRIFUtw+zZmwyMpHNVkwOWXp+N23iKKdKusNpH:qGva5KkmiuFUtw+z/yE5f5Kkm2J
MD5:	8C3F1BA961EB7423B0DB83ECB979F53D
SHA1:	FB3BA9AD3085A8DCE508DEC7961E2AA772A9A61E
SHA-256:	8374A659830ACF53E2144D2ED013620AEDE02DB97C791E2973B194352E5E2A1D
SHA-512:	AEA27D840359F4129D93FA6ED585DF418CA826D14063365C29507464DB5F3D372B6405EE7C4CB4A5270C3B4F65468078A3149E364D1F296A3BF8AAA89EBF5DA
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:49:51.942 1788 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2020/11/22-11:49:51.947 1788 Recovering log #3.2020/11/22-11:49:51.949 1788 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.221790592820144
Encrypted:	false
SSDEEP:	6:vDoq2PWXp+N23iKKdKusNpZQMxIFUtwgDzkhZmwygDzk7kwOWXp+N23iKKdKusNP:vDova5KkMFUtwgDU/ygDU5f5KkTJ
MD5:	FCB39087BEFF36ACDADC074C5FA1CE3C
SHA1:	7D4185FBF3BCB4B6B54561CD50B809F9FC3BF176
SHA-256:	26A0A06D3A59974CA0206FA5B5AE2BD9597CEFC6C621064728003F341A90964B
SHA-512:	0F674EFD9710C831333F7015D43EA4FE212C57C06AF25F8950F4B288FE2A19EDFBB9286A78B5A6F0690856165B0023E6024B10FA7355AC96D0BACB052896A8EA
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:50:08.115 1750 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2020/11/22-11:50:08.116 1750 Recovering log #3.2020/11/22-11:50:08.116 1750 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\eee21476-17e8-42b7-90c0-2f0a91af8bbd.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\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):	5.186101723898298
Encrypted:	false
SSDEEP:	12:vaGva5KkkGHArBFUtwgu5/ygHuuT5f5KkkGHAryJ:Xa5KkkGgPgUUWuIf5KkkGga
MD5:	7C4D95BA08922CA544A8065C6EB38BDD
SHA1:	BEE884A5BDCA6A615BD074275CDE0E0AA21E97BF
SHA-256:	AA25939D95C579210445EF993D8B932AE80A36A59ED52E023A7FB488466F135F
SHA-512:	576A303B02CD24F0605E329B46B74F2137D77BDE2DD26BB47DDEA7781CECD3D45FB6E53DA7F1DEE2286CEE4CF78A5788CFF416DEEA35E7524AF6831AEB52DD1F
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:50:03.879 1788 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2020/11/22-11:50:03.880 1788 Recovering log #3.2020/11/22-11:50:03.881 1788 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.191212755012941
Encrypted:	false
SSDEEP:	12:vk4va5KkkGHArqiuFUtwgo3J/ygjD5f5KkkGHArq2J:8Ka5KkkGgCgO3EsVf5KkkGg7
MD5:	D44F541F98477559B89907D56448FD6C
SHA1:	A69A421B0B8B01B2755D3962D70716045D1108F3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
SHA-256:	B2637C6F29237D2049FF57D5A9A5E9E7E8E07996F153B7C5689F3983E2D52190
SHA-512:	B83B905BCF5CE4DDE4FAC34BDA1528BB8B8F9DEE536299819904F829E6E8841A731BA20072D787AD68522DCC7A95865A8A411E043E04C97AC3747EFC89D70B 2
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:50:03.888 1160 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2020/11/22-11:50:03.891 1160 Recovering log #3.2020/11/22-11:50:03.892 1160 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.187719144854331
Encrypted:	false
SSDEEP:	12:vgva5KkkGHArAFUtwg8n/ygcF5f5KkkGHArfJ:6a5KkkGgkgqKjXf5KkkGgV
MD5:	D5194420B9CF24658A3382978C58132A
SHA1:	00562538050D4186AB4D045E43D6EEA5D95DA07C
SHA-256:	30C03575E02415A4A3AA80B5A5B667F1E3E164483CBCA96D0848B79F93288C27
SHA-512:	59C484E5F2B85CF451393D8B211E5A4CC1B2490FCFC4668E7BF40FF6A26518EF10EB72B0084338A8896D34E4DE21CF47351A4C0050CB997741F92A4CBD030018
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:50:19.176 16a8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2020/11/22-11:50:19.177 16a8 Recovering log #3.2020/11/22-11:50:19.197 16a8 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\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\cc5a7900-931d-49f1-a8f7-e43f714d350a.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"},{"adve rtised_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\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.229736111708147
Encrypted:	false
SSDEEP:	6:04q2PWXp+N23iKKdKpIFUtwJF3JZmwyyINDkwOWXp+N23iKKdKa/WLJ:04va5KkmFUtwJNJ/yID5f5KkaUJ
MD5:	5E63859DE1A048E18845BC7DB6CCDD94
SHA1:	AA5C9E35F7FC7F52F7974451282A26962447B32D
SHA-256:	9FD34F8ECF1B0B8330F8EA384AA06BCF8F42C476AB906D223EB0A78984D42C62
SHA-512:	ED8FACC10A0BC1AA903965BA6E54720C9FFF32A563389DDC977F3E0C9B9E38D0EA3561F9BDF8F034B528B620743D842FE379ABFEC59868410F27EE9A6A79D28 2
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:49:51.634 1160 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2020/11/22-11:49:51.638 1160 Recovering log #3.2020/11/22-11:49:51.640 1160 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.313387705826105
Encrypted:	false
SSDEEP:	12:vnk34va5KkkOrsFUtwgn6J/ygn6D5f5KkkOrzJ:vk3Ka5Kk+gZ6Ek6Vf5Kkn
MD5:	60BCEAC7A4160E3EA933554A5FD2F79F
SHA1:	0CBC1A69CF57C3C3F7BDDFEC67F8DD9D0BB114DD
SHA-256:	807056D57948818E0E3EB69E2876B5F5B1E6277D0327078A6AA7D466C0322EAA
SHA-512:	36732041FF1010DC1A0D528B51F7AED38864D95DEF66424F29B2586EF62FD8B7151E3E9F44BF73561939B6A999322A3FB86CD75F64F9A3440307EB7D2AA3274B
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:50:04.791 1160 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2020/11/22-11:50:04.795 1160 Recovering log #3.2020/11/22-11:50:04.795 1160 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):	36
Entropy (8bit):	4.266332639970622
Encrypted:	false
SSDEEP:	3:lnd9/Fb2rsAT:ldHMsE
MD5:	D9C694227657B4054CBC3E897292A600
SHA1:	FCAA481123E9720050C68CABE9A1B21953BDCF40
SHA-256:	43BA0E8FE93E84F74319AE6A268C6CF93730520C7B61E6768A6D3DB3567A7828

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
SHA-512:	0DA3ACB95BBBAA8C38F3753AEA3962EDA6D98B00F02B21A05A1753511A7FFDFA81CC9574509060109CCA554E094B6607061EF2E9BE14B38DFEC078BEF90942 6
Malicious:	false
Reputation:	low
Preview:	.......:R........H.u~..........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a066e6ee-5dd8-4715-8003-ea99bffcebb4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16763
Entropy (8bit):	5.5782004630517426
Encrypted:	false
SSDEEP:	384:TjUtwLlXGXO1kXqKf/pUZNCgVLH2HfDRrU8b3r4z:DLlcO1kXqKf/pUZNCgVLH2HfVrU8rrg
MD5:	8F02B8986D68719A29748D4345B5D909
SHA1:	0D59C86465127A260CEC5F547883CE24F5F3FAA6
SHA-256:	1577D99513F8765CFB2F29608D965EFC0891E24B3FDD9E3A7E50BE163F859B1B
SHA-512:	EA30EDA4B4EBD76E4BA20A9CB3460A1DADECB6342486202717BBCA11229952DCC78102498EEB570747E1CDE70825FC44A8B4F4B8082487A2FF586D0DFE7180 B9
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":"13250548191642391","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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c96a8ce5-2d72-4bfd-81ed-79ef3b27fbef.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):	5645
Entropy (8bit):	5.1708354939599035
Encrypted:	false
SSDEEP:	96:ntr7GB43+wlyAVcVVok0JCKL8Bk818bOTQVuwn:ntY4rcu4Kck8s
MD5:	67A64EA390BB25B2CCD01FE2075B20CC
SHA1:	585FBDB3556A2D29A9D0A1FFD69D0DA1D32EFC29
SHA-256:	D08E69409DA1946D93B328B42172FE4499CA7FD3D826B727D00985FD047809AB
SHA-512:	5A73CF9AC06535E4B091285C6F43A989E876A4E0663853FE363EEE9E3063B17C5B0487473AC117BFE8D0437D939FA3DF3BF725EA7E9E488CFC2D893207FA934
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250548191876782","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",

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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.319078467519536
Encrypted:	false
SSDEEP:	3:tVP39SdeRvAGKWZmwvKg9VXRPhR1V8ng9VjUfhhR1WGv:v8oZAgZmwygFh7VSgvwh7tv
MD5:	B69CC081D180D00B2A61277821B660CB
SHA1:	B501D6AC7AB4909E0FC5B007AAF64749CF6D0572
SHA-256:	C910F6D22CBA01ABC743DCE5F89771A1464B09FE4FF3DB65575812B9E064F8F1
SHA-512:	7976FAA65AAFBC0FBB7FD0BD778F4AAE62491C0CDE289771E2DD71E79703C4EC9A9DE628784A59C5409850DFCB19599A9FEA9991432762C6233F9DDBA076CA7
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:50:03.208 1440 Recovering log #3.2020/11/22-11:50:03.273 1440 Delete type=0 #3.2020/11/22-11:50:03.274 1440 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.211475434818209
Encrypted:	false
SSDEEP:	6:vDq2PWXp+N23iKKdKfrzAdIFUtwgsXZmwygsFkwOWXp+N23iKKdKfrzILJ:vDva5Kk9FUtwgsX/ygsF5f5Kk2J
MD5:	0D0E6ADCAE36CF4B257FC002014E5ED8
SHA1:	C14BA60CC98D187D1E6E55E132FA6BFCE7A70C7A
SHA-256:	9AE8897CAA51C85CBAD45E7895136C165C69D38EE458078133725F107EFDD030
SHA-512:	B0BA6A022B3514A5F7759A5B10A13536366EADF06E1B0986AE75B3B3C92BAF86AE474549B9F0DEB9145CCCBA14FC23C0979FF32159FA4F82F943279A7A65C26B
Malicious:	false
Reputation:	low
Preview:	2020/11/22-11:50:03.691 17d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2020/11/22-11:50:03.693 17d4 Recovering log #3.2020/11/22-11:50:03.693 17d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
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\a468f033-22b9-400a-b58b-81df53725ad6.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):	162442
Entropy (8bit):	6.08271781596182
Encrypted:	false
SSDEEP:	3072:y2HA2NNCxQM9b0q+szv+tnMIGFcbXafIB0u1GOJmA3iuRR:DHrExQM9b7fD+ZMHaqfIlUOoSiuRR
MD5:	8B4CABC451BAEBE17B6FE771BC482F3A
SHA1:	B5A5A826CFD2F745E4FFD37F107E2DF84DBC7A2B
SHA-256:	F4B3AA9144DFC9EC36F6409A291C9AA25741FA2356CFC707DC5649C083416BD6
SHA-512:	745061EA113DBA1230CCC68510505F952E1E0C6C6CF76D939148045AAD1A4989BBD25AC602A072C0309E66512F50D4F07B40B2409E2F6CCE57DCBC27BBBDAE4
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":1.606074594850637e+12,"network":1.606042197e+12,"ticks":97852424.0,"uncertainty":4881188.0}},"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\a6156209-53c1-481b-b88a-645a13c3f007.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):	162442
Entropy (8bit):	6.082717143137579
Encrypted:	false
SSDEEP:	3072:ya6A2NNCxQM9b0q+szv+tnMIGFcbXafIB0u1GOJmA3iuRR:f6rExQM9b7fD+ZMHaqfIlUOoSiuRR
MD5:	DEEAA2FB9156C25A7C6928A1F5B49016
SHA1:	7C41EF85CF23A63601769DD56F72B458CC206942
SHA-256:	C66BB1250A3C9BEE9301A62A470B57E97C1F273A2149DBE87A053326EA9282B1
SHA-512:	957F1C518A7B2A1BF89C67229AE3A328212A3EB0B6B8DBA659D2C013A435304AC8F848619A25C777C48EE9EB48788482AAA897710D812FA589A47F28D3A338C5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\a6156209-53c1-481b-b88a-645a13c3f007.tmp	
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":1.606074594850637e+12,"network":1.606042197e+12,"ticks":97852424.0,"uncertainty":4881188.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+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\aa31a3d0-b2b9-46e4-bd6b-7bf77b1a2dad.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.75095531051238
Encrypted:	false
SSDEEP:	384:T7U7jB+ABRmHCNHrkvzZ30zxgH5QGonryNXzxktNpsr2Lm2BO5HH/gOt1vNa1/e2:0Kl9q9wI0eLbN9InnupKLZ3R8
MD5:	700DB2B700271348A32A29BA6FEEE676
SHA1:	80CB0661A238954E9BF2EC9B2E6F116844A23F74
SHA-256:	1E27D7CC3D3F9ABF851D92E492336A8068ACBAF7E24627126AD32D2C0F9BA5F4
SHA-512:	2F85542E3C7E49149D98DD77CF01D958F9614441D0110CFDEA49298E27561F8ABF92176A86A4B1A59C4D2BE112A96F639FB5C3946E72B3E0400187C6B62B68E7
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\bf55c2ae-d3cd-48c5-9149-6164ab43d5c4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7516801306259575
Encrypted:	false
SSDEEP:	384:97U7jB+A1KRdVKAHCNHrkvzZ30zxgH5QGonryNXzxktNpsr2Lm2BO5HH/gOt1vNE:9eKl9q9wI0eLbN9InnupKLZ3R4
MD5:	3F30AA1419623F6FFDC7A3044CE301A0
SHA1:	4361247321ED4A825DE8BCF8C828E38C0AE04A72
SHA-256:	22C80DCAD6E9CAAB8EF1F3842B3E68C220933E36D21D57F0098D4A1C67A2CD3D
SHA-512:	95900BDDFDFC0C6EE3A6B821CC6E90CA138216D72937B98AD28E471A0E554E4920EB2B61362A691F0BB49B4E3B2EA52E469D72BB3222FFB505648FAF3450191
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....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\e29e5fe6-4f06-46fb-80dc-58e3c4cef36e.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):	162442
Entropy (8bit):	6.082715835750806
Encrypted:	false
SSDEEP:	3072:l2HA2NNCxQM9b0q+szv+tnMIGFcbXafIB0u1GOJmA3iuRR:wHrExQM9b7fD+ZMHaqfIlUOoSiuRR
MD5:	C770260CEAB02AA6DB01A4A8D446192A
SHA1:	9F8EFA03EE7DA6E78D62EC3CEB3ACE83607CA22E
SHA-256:	96DA5DF06521CBE2BE27014FBD8503A5364BFF70AB4A33C41F4A403E138284F4
SHA-512:	B6C11E2AE02FC3F099951B54F97C9593962CF183B024EAB6BBBF62796BFC8169018034CEA7B620AAE86ED757E9D6866E3EDCD0F1FC5D2550A4953528E40D190B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\e29e5fe6-4f06-46fb-80dc-58e3c4cef36e.tmp	
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":1.606074594850637e+12,"network":1.606042197e+12,"ticks":97852424.0,"uncertainty":4881188.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016631053"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Temp\06cd4102-c795-46df-9da8-e2d7942b3cd3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	300953
Entropy (8bit):	7.973503294353402
Encrypted:	false
SSDEEP:	6144:0sb1v/4nxPbqqBbWbFsw+wh3bC5NFv++S/hup0XcaxlnJ9:7l/4nxPZbOFsw+y3d+S6WnX
MD5:	1FE8E0AEB768437A23CEEAE6053E5822
SHA1:	5529A275644B729009E22035F6125879450F4ABB
SHA-256:	25A2F515CEC98CF2ACF11B34C59723D76820A4B5734E223D7EBEA55E5A851468
SHA-512:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA56812320
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....L.18..Y.~..%...~._.....O\..p,...eY.0=.!..+.SoZA7...:t.G...VZ<..d....MN.....T..{1\.T...P,...i...NrD...e.2..u....5.....1.n.Zu.E...!..XR..j.:.E.gUw.-s7:T.c_...(.i..iU.).M=yF<..`.....F...@)..IK.. b.4.o..mC'...N.*@OtT...`.&|.8.M;.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....RI.G.,2.....[..T'....."ct.).s#.(/.D..C..4..RKf.W....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...H0F.!...L..\.j.1.d.....==v.....-

C:\Users\user\AppData\Local\Temp\3034f2cc-36c8-4c71-b77e-080033401c46.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\c4631ce3-193c-4648-8b94-81a5d10189c9.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\eaa9f83e-1a3f-4df0-bdd7-17063a9b3080.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3

C:\Users\user\AppData\Local\Temp\eaa9f83e-1a3f-4df0-bdd7-17063a9b3080.tmp	
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o..,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\06cd4102-c795-46df-9da8-e2d7942b3cd3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	300953
Entropy (8bit):	7.973503294353402
Encrypted:	false
SSDEEP:	6144:0sb1v/4nxPbqqBbWbFsw+wh3bC5NFv++S/hup0XcaxlnJ9:7l/4nxPZbOFsw+y3d+S6WnX
MD5:	1FE8E0AEB768437A23CEEAE6053E5822
SHA1:	5529A275644B729009E22035F6125879450F4ABB
SHA-256:	25A2F515CEC98CF2ACF11B34C59723D76820A4B5734E223D7EBEA55E5A851468
SHA-512:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA56812320
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....L.18..Y.~..%...~._.....O\..p,...eY.0=.!..+.SoZA7...:t.G...VZ<..d....MN.....T..{1\.T...P,...i...NrD...e.2..u....5.....1.n.Zu.E...!..XR..j.:.E.gUw.-s7:T.c_...(.i..iU.).M=yF<..`.....F...@)..IK.. b.4.o..mC'...N.*@OtT...`.&|.8.M;.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.l)N.|b.l....{.K@]6.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....RI.G.,2.....[..T'.....".ct.).s#.(/.D..C..4..RKf.W....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...H0F.!...L..\.j.1.d.....==v.....-

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\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):	886
Entropy (8bit):	4.799570700992651
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyIDEK:1HE7n4gn8WYpYrbhz8ZpotHOPjsrdaD
MD5:	0F604F138A921EE7270C45E520621C30
SHA1:	E2BA940AF44609BEAC49B603EB1C379E43F4AAEB
SHA-256:	A149D52858570C9544E33B183915556230B7F66CF4ABAD4DDB00B1409476FBE1
SHA-512:	D87C8C7D0C998B37E34B7E4E6F5212FF4A0588C15F1273A55CD36B4A6FB13B7FDAE4F3B23EA469E7ACAF22B8BF53EB67476D897B96CA5C15C113EC078071A6D
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": "..... .. .., ...-.....".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\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):	705
Entropy (8bit):	4.576619033098666
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyFJKtOi2V2Te:1HE5baib6WYpm31Lt0Z8Zp8pxOaKtwVl

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\ca\messages.json	
MD5:	DDD77BA67108D8D88D66E35AA72A8048
SHA1:	F9C217728E756728B788C969F5101484D0557065
SHA-256:	3DB4D2B1586C020EC679C09148DB226DBB23857D326BECBB6CC48976036C391F
SHA-512:	6CA88083CECF6166503A1441BE8BB726CF08DEA8CFD61F1E81A970FE623284039FB9A530990E8E2008A4B1128399022AFE4F517E85CC7B069B670F5BA659F4F6
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": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "No s'ha pogut completar la transacci.. Torneu-ho a provar m.s tard.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\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):	663
Entropy (8bit):	4.771803710371731
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyN+/sFfmSYWc:1HEl4G8WYpdt8Zpq5TOT0FfmR
MD5:	B587AF92ECD087AAE3EF210364960844
SHA1:	AD78B31888863D3F0EC0D8CDCA316EDE9EBD7543
SHA-256:	9796A230BA459EF31E3D102B02575B73D6F1C812BF11F4D1E55B17C17891D2C5
SHA-512:	D2771ABB1174C3B6AF70BA1640837DE1B28137319307841B12A7D03C0A605AAECFC93069026A3906B289BAE12D33F4457FB54D7D27ABC5DC674C5C4C1E9F7CE 1
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": "Transakci nebylo mo.n. dokon.it. Zkuste to znovu pozd.ji.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\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):	642
Entropy (8bit):	4.533570611298554
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyNz31m8tbYzD:1HErMKfqMKVWYpM6lL8ZpDNOOQ84D
MD5:	639CEF5231701AE13F81DBB67730BB95
SHA1:	E249FE0C70B0F85B033730719B6D1B30F0B04431
SHA-256:	6C71F9D37006245D0E2E956D6D2C1815FFEB43236DD3D427A02F8DD348AC93C5
SHA-512:	D040D25ADD9666050544F9173EF61E044F7EBBAE8C528FC4077880734141205AAE60566668E6854D0B9C8D59924E22D1665D2C93085ED7F7E1F4DA91B951F09E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "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": "Transaktionen kunne ikke gennemf.res. Pr.v igen senere.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\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):	701
Entropy (8bit):	4.598783840405771
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603Oy91Lj8SYJ6K:1HEzWWYp3Bewv8Zp7k4OALlhj
MD5:	6E1B49ABC0AA5C1E2764E48EB1EA256A
SHA1:	604E76C89D4763C002C51908CEFE8C11AF7CBBE5
SHA-256:	B692DB1A249223E62E62DE9725334039419B5942AF715669F0F0F4BDEDAC5733
SHA-512:	EE527D48178D09D66120C0D1EA2584A7397404109A074AC09487D6AE8507A593193B31D3197C2418A162BB3E7DCC46FA5844D4951BB09650FC2A4AA10EAB811C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\de\messages.json	
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": "Die Transaktion konnte nicht abgeschlossen werden. Bitte versuchen Sie es sp.ter erneut.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\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):	875
Entropy (8bit):	4.920210350678433
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOBINZXD:WguYpCZnpEZb6fD
MD5:	41BB0DB6EC99E4664C6E2247EC704151
SHA1:	BF2268F9A77218384F1F73951F98829296318452
SHA-256:	90FC75C419D7359C2241F54562177252655526F3074E7E419E36F5C473843842
SHA-512:	738F7C254825E0D00D4BDF909FA6957D5A6027BCBCDF76F1385210FA5F908C2C94C038B6DF4309C68774C96B84447079AAF514F46519E60876BE4A8F4ABC9E6(
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "... ....".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\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):	617
Entropy (8bit):	4.481995064086158
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOtiCsHTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOthFD
MD5:	64CBD0878A320F70E8F9DC2AD540C8DE
SHA1:	E95BC23E053C078BA4C269B2F75C22159450C2F2
SHA-256:	E99F26D0540E2C71802716B24668D9B4611E9BC429CD681606963E095D18EDFD
SHA-512:	10BAF5423314EF0352FD56D3649CF73713BE8D5EE8A2E21E7E02AAA46EE92635A1EEF87DC62D3E999A1B3704720C51D3281FB28CB9523395EB5A21C4AB3C6D(A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "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 try again later.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\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):	617
Entropy (8bit):	4.481995064086158
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOtiCsHTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOthFD
MD5:	64CBD0878A320F70E8F9DC2AD540C8DE
SHA1:	E95BC23E053C078BA4C269B2F75C22159450C2F2
SHA-256:	E99F26D0540E2C71802716B24668D9B4611E9BC429CD681606963E095D18EDFD
SHA-512:	10BAF5423314EF0352FD56D3649CF73713BE8D5EE8A2E21E7E02AAA46EE92635A1EEF87DC62D3E999A1B3704720C51D3281FB28CB9523395EB5A21C4AB3C6D(A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "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 try again later.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\es\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	696
Entropy (8bit):	4.469493700399435
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyFJhwtOLLY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OahwtyD
MD5:	B4B479436878DA0B032F1B656B310637
SHA1:	F525EDB5B376CE665280DB32EFE3684CE6DC10DC
SHA-256:	3B3DEB56AD7A5F85ED5AB944172B715A5F5F49E3C5A0F7915DB879BF8ACCFEE0
SHA-512:	56C5CCA31DFF155E608723EFEBE01B421DFA3AB43EDFB586778BD76C6EB1AAF57CF904BDE0EA0FB5E912CCB445788136DE319653A882DC2E844046847D201E 0D
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": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "No se ha podido completar la transacci.n. Vuelve a intentarlo m.s tarde.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\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):	667
Entropy (8bit):	4.49547663693789
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyFJ2tOLLYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOa2t4D
MD5:	807730218B74CA040AD8DD01E5B2E0D8
SHA1:	ADA0042296C448DCD5C2B22F520C9304526FE9AD
SHA-256:	2823F6DDBF6905D9F4459091A85073644E64B5F7AAAA7FC435495C50DC5ECE68
SHA-512:	5ED86C91A0A435417CB0EDF984AA4DF2177BE37C27D0C805147CEB11ABF75C642416443DB88049A538F63BED9CCCBA95973DAC795498A1A7E022DD6ED36204 2
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": "No se pudo completar la transacci.n. Vuelve a intentarlo m.s tarde.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\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):	609
Entropy (8bit):	4.483029436148137
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyQQUe1YgoLIR:1HEdvqlWYpTeObk8ZpT/O3QU1LIR
MD5:	B5DF9CEA0A2FEAE9816F8D41470D744E
SHA1:	65C86CD677A68FF7E11A789EAB078FB932A9E157
SHA-256:	AD75B59775C8F6688FFA9F0453868999996E04B9EE9645721765D1C731D04578
SHA-512:	10C30393C29829FFC535559C57B31EBDCC370ABB5C2ED2A6F04E9CC5590FB8587DAB330E4E9367F3E762314EFE913802B98821136D17E9B9A437B56885F259F8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "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": "Tehingut ei saa l.pule viia. Proovige hiljem uuesti.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\fi\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):	673
Entropy (8bit):	4.6221501785662396
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03Oy0EyOxAxWeY5HN:1HEFcWYpPNa8ZpD+FO4zxAWHN

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\fi\messages.json	
MD5:	50EF678CECF0C82675B9DF64CC3CF72E
SHA1:	F9D9A994530C86C1A99B6D104E86666AB56AD4DA
SHA-256:	7F5B921E0D0B01D8D3287D3293729BFFF07ABC7DBCB1227134823A404DF29E83
SHA-512:	62A96C70F496CEA0FF0765E4ED7E014F1A2C7B394F7438C887C094C62885F5B9CD2822B0A9BB83C45471076CA5CF47954C0D5C46D4B45AA7AD5910D57CD2AF
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "Tapahtumaa ei voi suorittaa loppuun. Yrit. my.hemmin uudelleen.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	692
Entropy (8bit):	4.519947404204655
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OytnmHQnJvYHf9:1HEYah6WYp7TUSoxOS8Zp7TOsO4wXX2w
MD5:	0CA8EE1D816E684D781E7DF18C18455D
SHA1:	F711596B4049CBAA99296AD3755CCC0E79D47051
SHA-256:	CA9739F4FA8514C8669AE6221842B1F5D148BD80492888CECBA7410CB32225A8
SHA-512:	3BE7CA9E781E0D0BF17F3E894FD75CF7FCCCB0BEEB9A0FC7C17D3F5BC142B662ACFDC7254AA75D2AF9933D0FB70057297E29E8A5815F29469906F9DC8F339(2E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "Hindi makumpleto ang transaksyon. Pakisubukang muli sa ibang pagkakataon.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\fr\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):	708
Entropy (8bit):	4.573921094123133
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03Oynha3Gg:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOshi
MD5:	BE3C2C2BF4551641D84A60EC9F1E6E15
SHA1:	AAB0C8097A5B35FA40F2B137E1889677CB105B40
SHA-256:	DDDDAA9A83C34BF2874CBBE0214351C15E2620C0DC3863B2B79C4ACF9C2A4637
SHA-512:	4F263F78B61075525FA94493FB5C6297A53395F61E630E2DE81F14393BD2D5B3E687F35BF321C1009C0AF9A230A0C49D188F68AA7F2E4F61F3358596A86A6C2D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "Impossible de finaliser la transaction. Veuillez r.essayer plus tard.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\hi\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):	955
Entropy (8bit):	4.664681647654927
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOjSvzdlmLzSLm:Wh7qgYp1CMLUph1jSv3mLzSLm
MD5:	8CFF82EB516A180F2BFA22DA0B18D9E7
SHA1:	87053836FFDB4103302D17D221BC76C8DB842A28
SHA-256:	EA0020B530B3E047559248C076B54E90EFEF6A233DA130D5F43445C25BCB2008
SHA-512:	DEADC807AE4F254A4A73D31A12C2BC274D0E2E25413A36DCEF565B155BA72037BD3A14B5067A8B0325A86CB126C3B223A7DDFC66D5981CB48F1975E962AFBE E6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\hi\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "messa ge": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "...-... ....".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

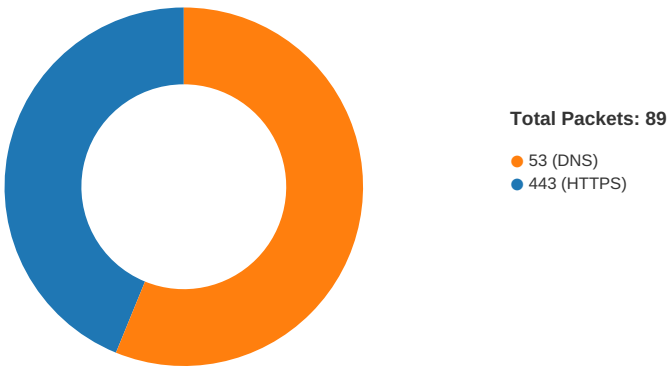
C:\Users\user\AppData\Local\Temp\scoped_dir5984_303993994\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	633
Entropy (8bit):	4.602004893403632
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphc:1HE4H4TH8WYpNjTta28ZpQVLP0SOv3XD
MD5:	5A777479C6072C009FF6EEEDD167B205
SHA1:	D4B509E3AD07A7EABEB32E7EF06166D5A60D4B54
SHA-256:	1650A45BF772FA06F99EB68015FD356B8BCC1DD4AEE0A4213C626BA2216D9D43
SHA-512:	8E13AD3DF747E6F082D813E4BC5321F1AB1A6D8C203EB9E0A01EF8B5B496DE74F5FCAE956239C85A18DD26399847177325FAADD84C60AC507818E9F26BBB53D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "Transakcija nije dovr.ena. Poku.ajte ponovo kasnije.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 11:49:54.727401018 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:54.729604006 CET	49725	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:54.881443977 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:54.881561995 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:54.881891012 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:54.883326054 CET	443	49725	103.153.182.184	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 11:49:54.883455038 CET	49725	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:54.886794090 CET	49725	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.035772085 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.040751934 CET	443	49725	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.057768106 CET	443	49725	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.057876110 CET	443	49725	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.057933092 CET	443	49725	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.057975054 CET	49725	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.058002949 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.058065891 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.058113098 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.058155060 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.058171034 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.058295012 CET	443	49725	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.073591948 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.074137926 CET	49725	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.074466944 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.228061914 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.231034040 CET	443	49725	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.241070986 CET	443	49725	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.241144896 CET	49725	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.241416931 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.242193937 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.242364883 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.446469069 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.446532011 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.446666956 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.455046892 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.495924950 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.509042025 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.665067911 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.665107965 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.665221930 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.669826984 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.862941027 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.919209003 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.919269085 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.919300079 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.919388056 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.919550896 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.919593096 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.919619083 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.919714928 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.919917107 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.919959068 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.919986010 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.920052052 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.920212030 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.920701981 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.920802116 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.920830965 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.920861959 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.926453114 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:55.926538944 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:55.985408068 CET	49725	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:56.073456049 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.073498964 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.073524952 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.073571920 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:56.073703051 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.073744059 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.073779106 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.073796988 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:56.074106932 CET	443	49722	103.153.182.184	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 11:49:56.074146986 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.074172020 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.074204922 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:56.074393988 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.074434996 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.074460983 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.074492931 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:56.074636936 CET	443	49722	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.114917040 CET	49722	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:56.141554117 CET	443	49725	103.153.182.184	192.168.2.3
Nov 22, 2020 11:49:56.182061911 CET	49725	443	192.168.2.3	103.153.182.184
Nov 22, 2020 11:49:56.231848955 CET	49742	443	192.168.2.3	104.16.18.94
Nov 22, 2020 11:49:56.248238087 CET	443	49742	104.16.18.94	192.168.2.3
Nov 22, 2020 11:49:56.248410940 CET	49742	443	192.168.2.3	104.16.18.94
Nov 22, 2020 11:49:56.248568058 CET	49742	443	192.168.2.3	104.16.18.94
Nov 22, 2020 11:49:56.264960051 CET	443	49742	104.16.18.94	192.168.2.3
Nov 22, 2020 11:49:56.266408920 CET	443	49742	104.16.18.94	192.168.2.3
Nov 22, 2020 11:49:56.266458988 CET	443	49742	104.16.18.94	192.168.2.3
Nov 22, 2020 11:49:56.266537905 CET	49742	443	192.168.2.3	104.16.18.94
Nov 22, 2020 11:49:56.283756971 CET	49742	443	192.168.2.3	104.16.18.94
Nov 22, 2020 11:49:56.283886909 CET	49742	443	192.168.2.3	104.16.18.94
Nov 22, 2020 11:49:56.284147978 CET	49742	443	192.168.2.3	104.16.18.94
Nov 22, 2020 11:49:56.300132036 CET	443	49742	104.16.18.94	192.168.2.3
Nov 22, 2020 11:49:56.300162077 CET	443	49742	104.16.18.94	192.168.2.3
Nov 22, 2020 11:49:56.300447941 CET	443	49742	104.16.18.94	192.168.2.3
Nov 22, 2020 11:49:56.302136898 CET	443	49742	104.16.18.94	192.168.2.3
Nov 22, 2020 11:49:56.302367926 CET	49742	443	192.168.2.3	104.16.18.94
Nov 22, 2020 11:49:56.309056997 CET	443	49742	104.16.18.94	192.168.2.3
Nov 22, 2020 11:49:56.309082985 CET	443	49742	104.16.18.94	192.168.2.3
Nov 22, 2020 11:49:56.309122086 CET	49742	443	192.168.2.3	104.16.18.94

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 11:49:46.424529076 CET	58361	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:46.453165054 CET	53	58361	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:47.117482901 CET	63492	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:47.145092964 CET	53	63492	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:47.759644985 CET	60831	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:47.786721945 CET	53	60831	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:49.147111893 CET	60100	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:49.174284935 CET	53	60100	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:50.046202898 CET	53195	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:50.073564053 CET	53	53195	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:51.240683079 CET	50141	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:51.267826080 CET	53	50141	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:52.841181993 CET	53023	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:52.868745089 CET	53	53023	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:54.181268930 CET	59349	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:54.220758915 CET	53	59349	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:54.676867008 CET	57084	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:54.678308964 CET	58823	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:54.682291985 CET	57568	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:54.685820103 CET	50540	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:54.720074892 CET	53	57084	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:54.721558094 CET	53	50540	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:54.725645065 CET	53	57568	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:54.734939098 CET	53	58823	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:54.848408937 CET	54366	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:54.875535965 CET	53	54366	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:55.014856100 CET	53034	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:55.058228970 CET	53	53034	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:55.113143921 CET	57762	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:55.156852961 CET	53	57762	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 11:49:55.506053925 CET	55435	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:55.533222914 CET	53	55435	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:55.981172085 CET	56132	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:55.983484983 CET	58987	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:55.984949112 CET	56579	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:55.987190962 CET	60633	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:55.989406109 CET	61292	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:56.010628939 CET	53	58987	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.014172077 CET	53	60633	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.027097940 CET	53	56132	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.028925896 CET	53	56579	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.037302017 CET	53	61292	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.203516960 CET	63619	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:56.203640938 CET	64938	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:56.203656912 CET	61946	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:56.225244999 CET	64910	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:56.226047039 CET	52123	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:56.230514050 CET	53	63619	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.230550051 CET	53	64938	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.239120007 CET	53	61946	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.253000021 CET	53	52123	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.262145996 CET	53	64910	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.274133921 CET	56130	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:56.301137924 CET	53	56130	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:56.958966970 CET	56338	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:57.015613079 CET	53	56338	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:57.222018003 CET	59420	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:57.248971939 CET	53	59420	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:57.547275066 CET	58784	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:57.548958063 CET	63978	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:57.583009958 CET	53	58784	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:57.596229076 CET	53	63978	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:57.602421999 CET	62938	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:57.629587889 CET	53	62938	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:58.248961926 CET	55708	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:58.276256084 CET	53	55708	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:58.509371996 CET	56803	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:58.547410965 CET	53	56803	8.8.8.8	192.168.2.3
Nov 22, 2020 11:49:58.930597067 CET	57145	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:49:58.966330051 CET	53	57145	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:02.096353054 CET	49361	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:02.148313046 CET	53	49361	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:03.892494917 CET	56881	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:03.938761950 CET	53	56881	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:05.139899969 CET	55667	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:05.183779001 CET	53	55667	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:15.291182041 CET	54833	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:15.318597078 CET	53	54833	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:20.809844017 CET	62476	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:20.861601114 CET	53	62476	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:30.383311987 CET	49705	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:30.427179098 CET	53	49705	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:35.083899021 CET	61477	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:35.121330976 CET	53	61477	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:36.460675001 CET	61633	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:36.496493101 CET	53	61633	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:37.984354973 CET	55949	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:38.011519909 CET	53	55949	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:41.555593014 CET	57601	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:41.592900038 CET	53	57601	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:52.500333071 CET	49342	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:52.544152975 CET	53	49342	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:52.863524914 CET	49667	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:52.899169922 CET	53	49667	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 11:50:52.951914072 CET	55439	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:52.997505903 CET	53	55439	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:53.089665890 CET	57069	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:53.133148909 CET	53	57069	8.8.8.8	192.168.2.3
Nov 22, 2020 11:50:53.520579100 CET	57659	53	192.168.2.3	8.8.8.8
Nov 22, 2020 11:50:53.556430101 CET	53	57659	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 11:49:54.685820103 CET	192.168.2.3	8.8.8.8	0x3edd	Standard query (0)	wtseticket.gb.net	A (IP address)	IN (0x0001)
Nov 22, 2020 11:49:55.983484983 CET	192.168.2.3	8.8.8.8	0x991e	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 22, 2020 11:49:55.987190962 CET	192.168.2.3	8.8.8.8	0xbeb7	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Nov 22, 2020 11:49:56.203516960 CET	192.168.2.3	8.8.8.8	0xbb57	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 22, 2020 11:49:56.203640938 CET	192.168.2.3	8.8.8.8	0xe49a	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 22, 2020 11:49:56.203656912 CET	192.168.2.3	8.8.8.8	0xf96c	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 22, 2020 11:49:57.222018003 CET	192.168.2.3	8.8.8.8	0xb0dc	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Nov 22, 2020 11:50:02.096353054 CET	192.168.2.3	8.8.8.8	0xc7e9	Standard query (0)	www.politikesgeuseis.gr	A (IP address)	IN (0x0001)
Nov 22, 2020 11:50:03.892494917 CET	192.168.2.3	8.8.8.8	0xa0cc	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 11:49:54.721558094 CET	8.8.8.8	192.168.2.3	0x3edd	No error (0)	wtseticket.gb.net		103.153.182.184	A (IP address)	IN (0x0001)
Nov 22, 2020 11:49:56.010628939 CET	8.8.8.8	192.168.2.3	0x991e	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 11:49:56.014172077 CET	8.8.8.8	192.168.2.3	0xbeb7	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 11:49:56.230514050 CET	8.8.8.8	192.168.2.3	0xbb57	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 22, 2020 11:49:56.230514050 CET	8.8.8.8	192.168.2.3	0xbb57	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 22, 2020 11:49:56.230550051 CET	8.8.8.8	192.168.2.3	0xe49a	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 11:49:56.239120007 CET	8.8.8.8	192.168.2.3	0xf96c	No error (0)	stackpath.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 11:49:57.248971939 CET	8.8.8.8	192.168.2.3	0xb0dc	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 11:50:02.148313046 CET	8.8.8.8	192.168.2.3	0xc7e9	No error (0)	www.politikesgeuseis.gr		35.214.201.112	A (IP address)	IN (0x0001)
Nov 22, 2020 11:50:03.938761950 CET	8.8.8.8	192.168.2.3	0xa0cc	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 11:50:03.938761950 CET	8.8.8.8	192.168.2.3	0xa0cc	No error (0)	googlehosted.l.googleusercontent.com		172.217.16.193	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5984 Parent PID: 2844

General

Start time:	11:49:50
Start date:	22/11/2020
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://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat@phcc.gov.qa'
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: 1708 Parent PID: 5984

General

Start time:	11:49:52
Start date:	22/11/2020
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=1516,10236018493698859480,3773363086378492193,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1872 /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

Disassembly