ID: 471906
Cookbook: browseurl.jbs
Time: 07:49:45
Date: 26/08/2021
Version: 33.0.0 White Diamond

Table of Contents

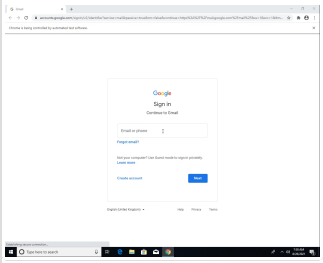
Windows Analysis Report http://covidteamclapham@gm…

Overview

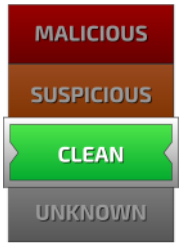
General Information

Sample URL:	http://covidteamclapham@gmail.com
Analysis ID:	471906
Infos:	

Most interesting Screenshot:



Detection

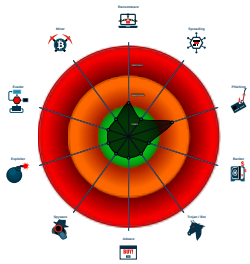


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- URL contains potential PII (phishing…
- Found iframes
- No HTML title found
- Unusual large HTML page

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3528 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://covidteamclapham@gmail.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4904 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1600,818200865018122053,4149282262256251718,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1764 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6828 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1600,818200865018122053,4149282262256251718,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5704 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6860 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1600,818200865018122053,4149282262256251718,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=5720 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

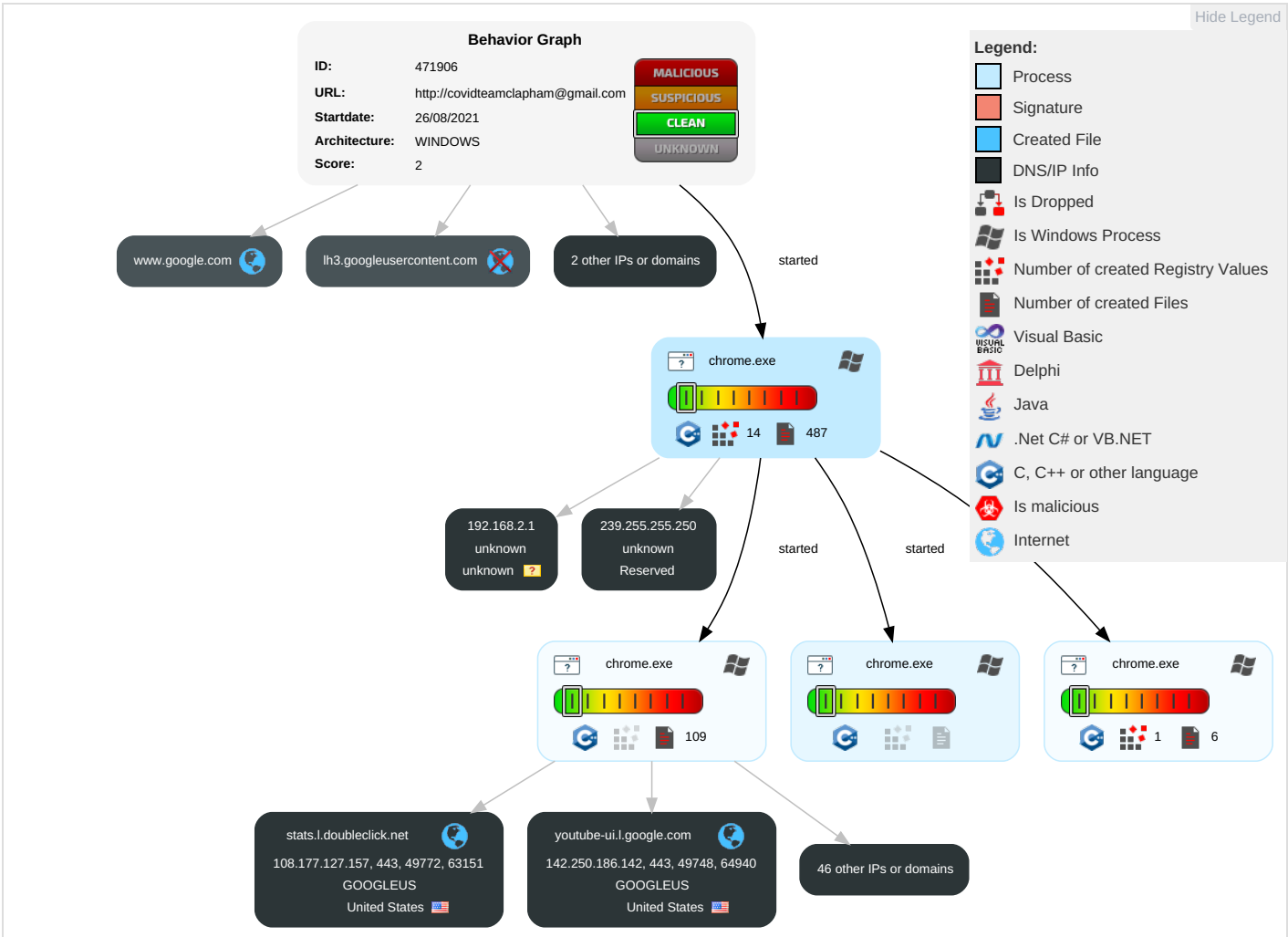
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Drive-by Compromise 1	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
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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

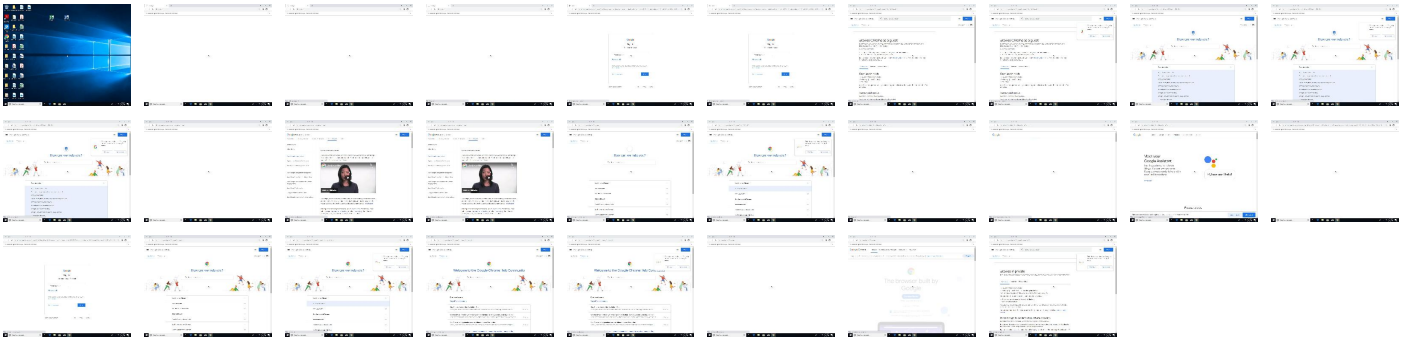
Behavior Graph

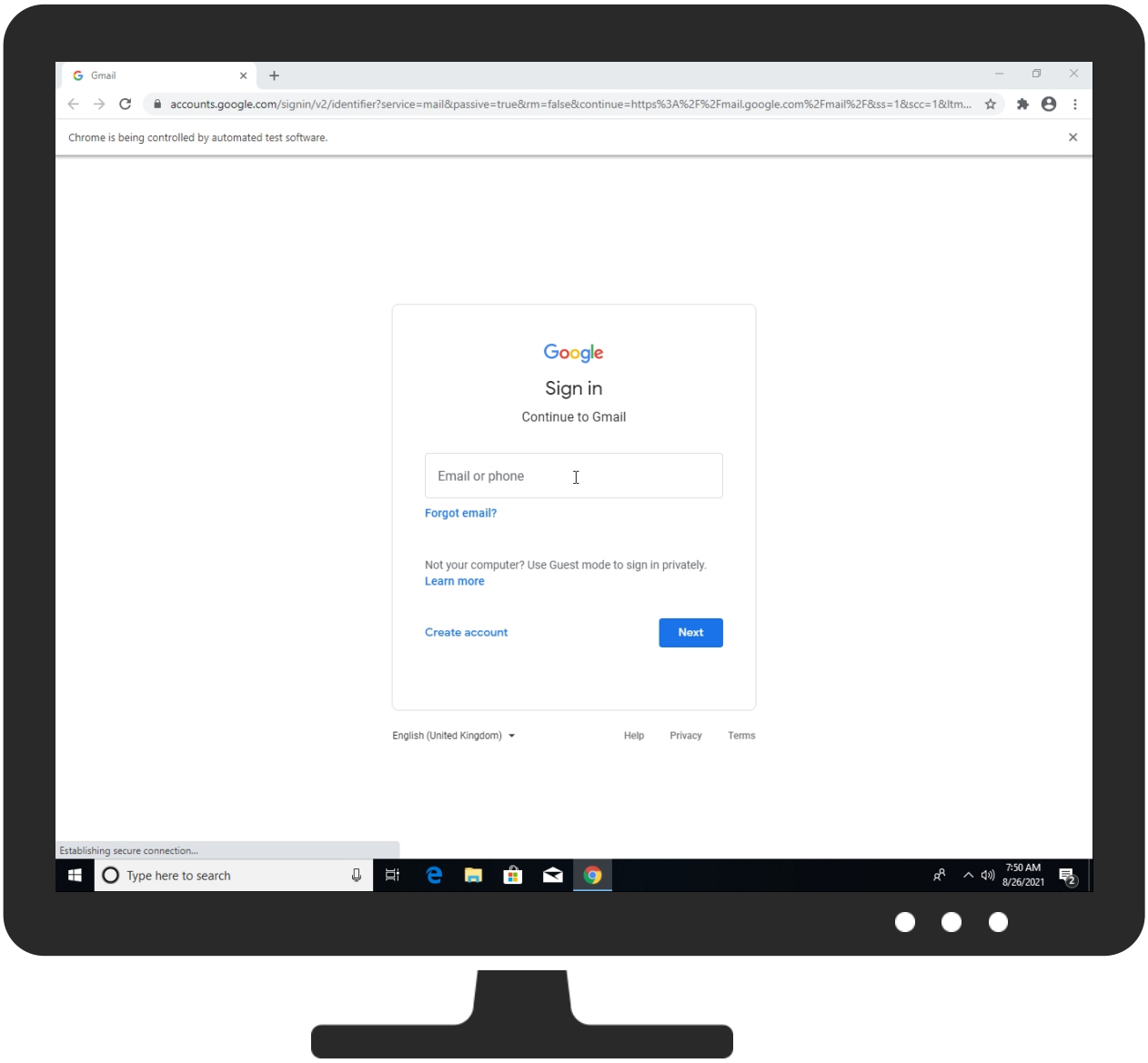


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://covidteamclapham@gmail.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
about.google	0%	Virustotal		Browse
ghs-svc-https-sni.ghs-ssl.googlehosted.com	0%	Virustotal		Browse
csp.withgoogle.com	0%	Virustotal		Browse
www.google.co.uk	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://about.google/9	0%	Avira URL Cloud	safe	
http://https://about.google/intl/en-GB/products/?tab=uh6Browse	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://accounts.google.comh	0%	URL Reputation	safe	
http://https://about.google/	0%	URL Reputation	safe	
http://https://about.google/intl/en-GB/products?tab=uhBrowse	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/i/dc_pre=CIj886__zfICFdaTGwodwDAOFg;src=2542116;type=chrom322	0%	Avira URL Cloud	safe	
http://https://about.google/R	0%	Avira URL Cloud	safe	
http://https://support.google.com-_https://support.google.com	0%	Avira URL Cloud	safe	
http://https://about.google/S	0%	Avira URL Cloud	safe	
http://https://about.google/L	0%	Avira URL Cloud	safe	
http://https://about.google/favicon.ico	0%	URL Reputation	safe	
http://https://about.google/x	0%	Avira URL Cloud	safe	
http://https://about.google/favicon.ico0	0%	URL Reputation	safe	
http://https://about.google/intl/en-GB/products/?tab=uhBrowse	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.3	true	false		high
scone-pa.clients6.google.com	172.217.168.10	true	false		high
dart.l.doubleclick.net	216.58.215.230	true	false		high
i.ytimg.com	172.217.168.54	true	false		high
support.google.com	142.250.203.110	true	false		high
policies.google.com	172.217.168.46	true	false		high
adservice.google.com	142.250.203.98	true	false		high
about.google	216.239.32.29	true	false	• 0%, Virustotal, Browse	unknown
photos-ugc.l.googleusercontent.com	172.217.168.1	true	false		high
ghs-svc-https-sni.ghs-ssl.googlehosted.com	142.250.203.115	true	false	• 0%, Virustotal, Browse	unknown
www.google.com	172.217.168.68	true	false		high
s.ytimg.com	172.217.168.14	true	false		high
pagead46.l.doubleclick.net	216.58.215.226	true	false		high
csp.withgoogle.com	216.58.215.241	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	172.217.168.45	true	false		high
www-google-analytics.l.google.com	216.58.215.238	true	false		high
plus.l.google.com	172.217.168.78	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stats.l.doubleclick.net	108.177.127.157	true	false		high
www-googletagmanager.l.google.com	172.217.168.8	true	false		high
gmail.com	172.217.168.69	true	false		high
static-doubleclick-net.l.google.com	172.217.168.70	true	false		high
youtube-ui.l.google.com	142.250.186.142	true	false		high
www3.l.google.com	142.250.203.110	true	false		high
play.google.com	172.217.168.78	true	false		high
googleads.g.doubleclick.net	216.58.215.226	true	false		high
googlemail.l.google.com	216.58.215.229	true	false		high
www.google.co.uk	172.217.168.3	true	false	• 0%, Virustotal, Browse	unknown
tools.l.google.com	216.58.215.238	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
www.blog.google	unknown	unknown	false		high
mail.google.com	unknown	unknown	false		high
ogs.google.com	unknown	unknown	false		high
lh3.googleusercontent.com	unknown	unknown	false		high
adservice.google.co.uk	unknown	unknown	false		unknown
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
2542116.fls.doubleclick.net	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
lh4.ggpht.com	unknown	unknown	false		high
static.doubleclick.net	unknown	unknown	false		high
accounts.youtube.com	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high
www.youtube-nocookie.com	unknown	unknown	false		high
tools.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://adservice.google.com/ddm/fls/i/dc_pre=CIj886__zfICFdaTGwodwDAOFg;src=2542116;type=chrom322;cat=chrom01g;ord=680803654523;gtm=2wg8n0;~oref=https%3A%2F%2Fwww.google.com%2Fchrome%2F	false		high
http://https://www.google.com/chrome/	false		high
http://https://ogs.google.com/widget/callout?prid=19022645&pgid=1151720448&puid=61a0eb6c838359b5&cce=1&dc=1&bc=1&origin=https%3A%2F%2Fsupport.google.com&cn=callout&pid=117&spid=117&hl=en-GB	false		high
http://https://ogs.google.com/widget/callout?prid=19022645&pgid=1151720448&puid=43a541cbad6c87d4&cce=1&dc=1&bc=1&origin=https%3A%2F%2Fsupport.google.com&cn=callout&pid=117&spid=117&hl=en	false		high
http://https://support.google.com/accounts?hl=en-GB#topic=3382296	false		high
http://https://2542116.fls.doubleclick.net/activityi;dc_pre=CIj886__zfICFdaTGwodwDAOFg;src=2542116;type=chrom322;cat=chrom01g;ord=680803654523;gtm=2wg8n0;~oref=https%3A%2F%2Fwww.google.com%2Fchrome%2F?	false		high
http://https://support.google.com/chrome/answer/6130773?hl=en-GB	false		high
http://https://www.youtube-nocookie.com/embed/TBR-xtJVq7E?rel=0&showinfo=0&theme=light&version=3&hl=en-GB&cc_lang_pref=en-GB&cc_load_policy=1	false		high
http://https://support.google.com/chrome/answer/95464	false		high
http://https://policies.google.com/technologies/cookies	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.115	ghs-svc-https-sni.ghs-ssl.googlehosted.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.215.238	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	support.google.com	United States		15169	GOOGLEUS	false
216.58.215.230	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.46	policies.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.168.8	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.69	gmail.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
172.217.168.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.98	adservice.google.com	United States		15169	GOOGLEUS	false
216.239.32.29	about.google	United States		15169	GOOGLEUS	false
216.58.215.229	googlemail.l.google.com	United States		15169	GOOGLEUS	false
216.58.215.226	pagead46.l.doubleclick.net	United States		15169	GOOGLEUS	false
172.217.168.70	static-doubleclick-net.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.1	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
108.177.127.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
216.58.215.241	csp.withgoogle.com	United States		15169	GOOGLEUS	false
172.217.168.78	plus.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.54	i.ytimg.com	United States		15169	GOOGLEUS	false
142.250.186.142	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	471906
Start date:	26.08.2021
Start time:	07:49:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://covidteamclapham@gmail.com
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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.win@50/303@39/25

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://support.google.com/chrome/answer/6130773?hl=en-GB • Browse: https://support.google.com/accounts?hl=en-GB • Browse: https://policies.google.com/technologies/cookies • Browse: https://support.google.com/chrome • Browse: https://www.google.co.uk/intl/en-GB/about/products?tab=uh • Browse: https://accounts.google.com/ServiceLogin?hl=en-GB&passive=true&continue=http://support.google.com/chrome/answer/6130773%3Fhl%3Den-GB&ec=GAZAdQ • Browse: https://support.google.com/chrome/?hl=en-GB • Browse: https://support.google.com/chrome/community?hl=en-GB • Browse: https://www.google.com/chrome • Browse: https://support.google.com/chrome/answer/95464
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\0cc76579-0b9d-4444-827a-b20e5bf2a239.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):	178081
Entropy (8bit):	6.078790450148885
Encrypted:	false
SSDEEP:	3072:GjQmm8A1PCyn3BOIrdvrVsWFcbXafIB0u1GOJmA3iuRF:6QP8oPjxfaqfllUOoSiuRF
MD5:	1E8268BAEF30702A7C28EE856E226F90
SHA1:	4142A598C43FB844171E4D2500EC89AB9B6E2F2C
SHA-256:	1ADD0CBB19929EF0EF161A7861BA3E7230226E4B535B254B5F17D71118CB641E
SHA-512:	6B247C07524DB9A84B99E2FA2B2F322B6D024010A06136F57AA21DF977748DBE4621541BD2A4438D35AB69BB2B39D7030C120367074F2167748EA8B942846C41
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":1.629989435586842e+12,"network":1.629957038e+12,"ticks":6444768894.0,"uncertainty":5556999.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951015966570"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\1d501b30-ef03-4ecf-a9cf-08e399494651.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.746002215045949
Encrypted:	false
SSDEEP:	384:9j9myMzJ0T4WVLNyxNurLvCK3xKUNHodG18rnU+0xpY88PrnCmL/ZnEWKaROA0SR:d2y1xik4tUej8G8Mnv2+KkSmx3
MD5:	F7FD7F5B28A7BAF4B463F4BE612C8460
SHA1:	4000D57AC358027E2712286E545940CD78FA2463
SHA-256:	E8D3B48EA0F1E05AFB01091B6160A6F37FE8DADF742F91C4B4631DC8AFE24F62
SHA-512:	182995A150D09FB586555598E5C8489BEAB1A7D50B3A28F2F8E4C6AACF04C88EA76F369E6D666A20E27A0A1462DDC1F8CBA60BE08988C8FFBBA922686106C041
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....C8.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\2cf9fd8c-8a6a-4bec-93ef-b65b8957f3d7.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):	178081
Entropy (8bit):	6.0787899846834135
Encrypted:	false
SSDEEP:	3072:7uXmm8A1PCyn3BOIrdvrVsWFcbXafIB0u1GOJmA3iuRF:KXP8oPjxfaqfllUOoSiuRF
MD5:	724D44CF3A1A82DC88E3F3ACDB7750FB
SHA1:	AE8DD01A20DC0D92AF5313F9250A7F8E1566B2C3
SHA-256:	E17C339F29E04672090867A5A536263AB92B7903A65A7712BF2D391504B7DCF2
SHA-512:	33B0D59C774DBEFC9DD321D7DEC34C9D454BB456DA13931BBEF4DC10B1A7D5A3F2D630BB09CCF2F76244F0471F84E408EAB3DDE1DB52DCFDC96AD815120EE68
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\2cf9fd8c-8a6a-4bec-93ef-b65b8957f3d7.tmp	
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":1.629989435586842e+12,"network":1.629957038e+12,"ticks":6444768894.0,"uncertainty":5556999.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\7a725eeb-0be0-4541-8c1a-e8076bc955e3.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):	178081
Entropy (8bit):	6.078790769885374
Encrypted:	false
SSDEEP:	3072:7J8mm8A1PCyn3BOIrdvrVsWFcbXafIB0u1GOJmA3iuRF:V8P8oPjxfaqfIlUOoSiuRF
MD5:	CBFE4913D7C5EF65C68143EC42A76212
SHA1:	FD000361A7D0A9046282385BEF2C153B956ACAE7
SHA-256:	67F4780E532929480EEA348DFC5442E1E7C5D73B1DF94F0E1F3A5C06265E5A78
SHA-512:	582B5E987B876D0F4212BB8473260F8EBE40512C11CF32EEECB6EDC16B9AF49BFCDC71BF29AD90266ACB3E7AF9B417A94333556BD66D946135F11B7C0BAA0B6F
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":1.629989435586842e+12,"network":1.629957038e+12,"ticks":6444768894.0,"uncertainty":5556999.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\87a2aacf-c1e8-4e67-a271-1800b3cb7bb7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.746057578072341
Encrypted:	false
SSDEEP:	384:Nj9myMzJ0T4WVLNyxNurLvCK3xKUNHodG18rnU+0xpY88PrnCmLonEWKaROA0SNf:N2y1xikBtUej8G8Mnv2+KkSmxn
MD5:	5CE1533446E282A174914669C55CBB38
SHA1:	BDFDA5BA87F518DDC76509B979BE5A9F25E4DF74
SHA-256:	0C7EA973E8455B2ACC14C9531385F8158CF4D74F81316E8D65CDB66C9353B6EC
SHA-512:	092834D5514597063ABC433F4E49FB49F18CE42FB9C07BF22DCFCF139975EE56F73A6D5402582E1D8A194AE12DEB38EFD19E904577D2878B17BCCC45A6E5126
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....C.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\9fcbbc8e-e4e1-4e94-a63a-9adb74409151.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):	169607
Entropy (8bit):	6.048900290135362
Encrypted:	false
SSDEEP:	3072:Ymm8A1PCyn3BOIrdvrVsWFcbXafIB0u1GOJmA3iuRF:YP8oPjxfaqfIlUOoSiuRF
MD5:	A4EFFB4AE2F4645D41B294FE1428B67D
SHA1:	36E3B9BDA3CC4CF13FB5B4490C406497F04EF8B0
SHA-256:	C66B4D5F2CE6653C31C9A065C6389C8E7250915B0ADBCE0586FFDEA15C1E01CD
SHA-512:	61E271DED9C782734321531ACD5C1FAE1CD4425C9E7B0B7296531F7A9C10CEBCECE115CDC7B3DB3BE9B5FDB3489E4D5A1BF5066AD65E1FF0F523F5209B20785
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\9fcbbc8e-e4e1-4e94-a63a-9adb74409151.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":1.629989435586842e+12,"network":1.629957038e+12,"ticks":6444768894.0,"uncertainty":5556999.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951015966570"},"plugins":{"metadata":{"adobe-flash-player":{"dis

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:+ftlE1G1mkftlE1G1mkftlE1n
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\12297bd5-177c-4634-b7af-4bed38d13b2e.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):	22596
Entropy (8bit):	5.535850518354553
Encrypted:	false
SSDEEP:	384:8l4tjLlV9Xv1kXqKf/pUZNCgVLH2HfDgrUrHGxnTMfmUH40:VLlnv1kXqKf/pUZNCgVLH2Hf0rU7Gxni
MD5:	2A221BE47A9C67B5D5AD6729E6242358
SHA1:	797868CADFDF8ADE048627003B8998BD8B4FCA25
SHA-256:	8EC16E8C1EE976AED5FE02566DA6630248A100B4D8E4ECA096062DB9B40EB361
SHA-512:	882E687423ADBBAD2C770CCA56446D2A1A195C4C15D168B63B0C6EFC44B97EC35D8427F0BC7F0BFE2F426D6A5E72A956178A50F49BEF988271048582C007C49
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":"13274463031981034","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\199e4535-a4d7-4b4c-95d1-de625835cffd.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):	2376
Entropy (8bit):	5.6006423439981985
Encrypted:	false
SSDEEP:	48:YwkUnSyeUM8ieUr6UUhGUgUtSUGXKUTUaRqPeUTgTsUR/UefTbwUCUFpUG:8UnxeUM8ieUuUUEUgU0U+KUTUaMPeUih
MD5:	260F620D9470D8C8906F9299B0C1D8E0
SHA1:	FFFA54FE998CCCED73519A95A111447A9028AE6E
SHA-256:	0FB33E79A4139D5DF863C9E93CBB2B7D2FD1F0D31F869D33260525EC94028380
SHA-512:	878155C7F8FDA982427E01E1D9E76E2CDF7FBD480CB2DC8D2AB26B8E12F162AAC1C0AD701D330FECCFBB0B2ECF072FDDEFBE446D2458F951283A4C5EF49C324E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\199e4535-a4d7-4b4c-95d1-de625835cffd.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1661525484.090108,"host":"KVivTTKTVC3D7/hfpnbDFfPAgoVJQnjFfXBq+8P8zk8=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629989484.090113},{"expiry":1640875883.670767,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989483.670774},{"expiry":1661525482.260099,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989482.260107},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1640875849.57971,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989449.579716},{"expiry":1661525455.206836,"host":"kYxWDeIDVgesBS02XkmPRTIpB0nkimBvKZESXctn8eA=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1dc73b28-5297-4f94-a3e0-bdd7d8a02db2.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):	6501
Entropy (8bit):	4.881730011331731
Encrypted:	false
SSDEEP:	192:Jzqwaqx9nEp4xDAK/x50VB6VG6tNESREsx/XD5TSgoDit:Jmwaqx9nEp4xDX/x50/6VG6t2SREsx/l
MD5:	A6BFDE656BFC5DDC5E3145B73FF16692
SHA1:	8D923D3904346122684F4854781936841640FFAD
SHA-256:	20CA581E01B009880EEEBFB7608294417A8D15C49C299BC0E672E4BACC710093
SHA-512:	1895CC392A276DEBCDF22A290ACF30CEA7BD1694E3FD37751BB2FEB11C94A2D0E1DE8E4E5F2B9966BECAFA069CA8CA7F35796F55C6AEBBFEDE91375C3BF2E6CC
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13277055037774260","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13277055037936556","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13277055037936559","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r5---sn-4g5ednsd.gvt1.com"},{"isolation":[],"server":"https://mail.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13277055048242867","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13277055043940968","port":443,"protocol_str":"quic"}],"isolation":[],"server":"ht

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1e707100-6a74-42b9-996f-e2c0e9ba3d89.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):	2042
Entropy (8bit):	5.597390838396505
Encrypted:	false
SSDEEP:	48:Y6eUz6UUhGUgUtSUAseKUexUaSfqPeUj/TsUvUef+wUAUCQUE:VeUmUUEUgU0UA3KUuUaDPeUnsUvUE7UP
MD5:	7D206DCD76945E0B2D31753E09E6E322
SHA1:	468E9CFA658B10196E8CD86A34485A0183540C58
SHA-256:	89198A6D0A91B9498DBDF86422B61DAB89CE28B96707EA2B588CA5DA07D092C5
SHA-512:	01063D6A99D42708449D9FA0CA690983017D4A23D18C3D678A09FD5EA13C573F4121079F35ED7BA4E1B47D51BB1D00FE9996E1818220A72A08D6EFCC76612B87
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1640875866.688768,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989466.688774},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1640875849.57971,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989449.579716},{"expiry":1661525455.206836,"host":"kYxWDeIDVgesBS02XkmPRTIpB0nkimBvKZESXctn8eA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629989455.206841},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1661525465.89244,"host":"sDdUHFeNXQYN3ZmOGsRDJNdZ+IwkPs1LrXOjilyGul0=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2b5e8da1-3006-4395-9164-79d76b7a12ce.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):	1038
Entropy (8bit):	5.566484128465509
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXvo7wUARUenHQ:YI6UUhVseKUewqPeUer2Uef+wUkUenw
MD5:	4CAA185ED58F9784C5A53886844AC5C6
SHA1:	522D454A3DED6D7C3B9198ACF9399BB94271B3A0
SHA-256:	26428A4AEF5C6971CA5A9E8384A58C0C5F78FFF97D7212208FB7284E5E12528B
SHA-512:	C2B71F8E98F45282E2E20C0A2E174FC31D81AC09DC73B6A571DC0F7CB23398ADCE6FAB7E6CA3EE0A300657C7E1B7B7D181A6EA40128CC84F9310FCCDD907680
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2b5e8da1-3006-4395-9164-79d76b7a12ce.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1661525440.166272,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989440.166278},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\39f8c41a-d41f-4341-b575-72564adf3230.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\445945ed-e89d-4362-8582-be41d5d7d2df.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):	5157
Entropy (8bit):	4.98491475029944
Encrypted:	false
SSDEEP:	96:nwCaGX9pcKIqok0JCKL8akL1qubOTQVuwn:nwCv9pcj4KrkLg8
MD5:	779B2CA51F254F2E3474108420EB17DC
SHA1:	C87107171EA850F07E9AC40DDE49CF80313FE1D4
SHA-256:	F124A46BE9DDD44E0037B238CAC0A395205C88317163D158F9CE7E16B4030960
SHA-512:	BF6A7576235495020BC866082ABA82F74FCE20DE4D2DF50C2AD55FF77DD39062FD342379C40B3CEA927CA3E53AB2F79516480B22E6D2E2AC04DDC31848D1DC6
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13274463032264195","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\55f56374-9aa7-4067-be79-8c75213392c0.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):	5788
Entropy (8bit):	5.1796226403261185
Encrypted:	false
SSDEEP:	96:nwCk/097MScKI6ok0JCKL8akL1qubOTQVuwn:nwCP97lcz4KrkLg8
MD5:	6F9216158D0A417EACFA4D1A5E7C62F5
SHA1:	6E0A5FC3E94A5E3495EE28FD7DAC0F13958DA0FA
SHA-256:	50170D37707F4BB9E78A7B41CE8E849843A9B534706B4B687506A62B7FE144D0
SHA-512:	9D565F8FB3AF9AAC57C70DEF262DFDBFF180DCA94BAFC0EB24A7039D559B7435615E3AFBC8AD5D654DE15E21E07007732ADE9CAE238EC71F584D3D016DED859C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\55f56374-9aa7-4067-be79-8c75213392c0.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13274463032264195","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5952fa3e-fe6c-4b96-87e0-a8b4ec310098.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):	2377
Entropy (8bit):	5.606205891744173
Encrypted:	false
SSDEEP:	48:YwkUnSyeUM8ieUr6UUhGUgUtSUGXKUTUahqPeUGTsUKUefUK6wUPUCrUT:8UnxeUM8ieUuUUEUgU0U+KUTUa8PeU0m
MD5:	C8F79F6C00B5EFB1EC253839518510E5
SHA1:	FD393AC15F1BEF1B24BB82A867F0EEADD631DFDB
SHA-256:	C533EF644C3E8C02D427C8321024CAE9D5677813AFAB671E9752E6022FA28943
SHA-512:	4458D5590F192C5BC27FF0AD70A6A2EED96AFB7FC131B2C56A43F1E1A29512A28F24AE68654BA5C792F2C2CA7B6301D4E56C306D134B3C59B568343388D90D2
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1661525484.090108,"host":"KVivTTKTVC3D7/hfpnbDFfPAgoVJQnjFfXBq+8P8zk8=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629989484.090113},{"expiry":1640875883.670767,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989483.670774},{"expiry":1661525482.260099,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989482.260107},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1640875849.57971,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989449.579716},{"expiry":1661525455.206836,"host":"kYxWDeIDVgesBS02XkmPRTIpB0nkimBvKZESXctn8eA=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6e60ad45-8125-4be9-89fb-482eddb31b1c.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7184790c-a2d4-4908-8ba4-603a6bfa696a.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):	5788
Entropy (8bit):	5.1797541471005975
Encrypted:	false
SSDEEP:	96:nwCA/097MScKImok0JCKL8akL1qubOTQVuwn:nwC797lcH4KrkLg8
MD5:	B531D150C99DBBBC64E5493DE17BC87F
SHA1:	B1AE47F5C8C6152C73B1304216B76BF110BA2D14
SHA-256:	D9E07BA5B2A1871E42054586A05A4C655F3A0992A0A4C08B48BC3914803A2AB6
SHA-512:	598B02521ADC4DE01DB2D2483441C8F435624533B3673F6AA4F43EA8C9ACD7A066FDFB6B3AD60252D6E2514916397C9D4764737B344AF90027381C7C98BE736D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13274463032264195","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\72143710-eb23-452c-b244-7d0d6d060b46.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):	5788
Entropy (8bit):	5.1797631656691765
Encrypted:	false
SSDEEP:	96:nwCk/097MScKI1ok0JCKL8akL1qubOTQVuwn:nwCP97lcm4KrkLg8
MD5:	DD9FDFAD03FDB17F0379AC1646821763
SHA1:	347111D6A51B5DA715D4653F65E5092900CC4BD5
SHA-256:	5AEA14D14CAFFB5CC6F88DB8FBC75B591ABCC14845041603FC8422C984256345
SHA-512:	BE737300DE00AF73BD64A02EB5F8F88598E4F641D348492401ADF98360DB3888381529E24CDFE00CB954BF7E90C1BD905BAFA77518E14030DBD4F1CE0F9795A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13274463032264195","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\72c8e538-b784-4ad8-81bc-c7ff847badb1.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):	16745
Entropy (8bit):	5.577565352639444
Encrypted:	false
SSDEEP:	384:8l4t6LlV9Xv1kXqKf/pUZNCgVLH2HfDgrUFEH4DH:sLlnv1kXqKf/pUZNCgVLH2Hf0rUyHoH
MD5:	1F02AC877546DFBF55024998B68540A6
SHA1:	80B96DA3A618DDB9A7ED002DF9E542E06C7AD855
SHA-256:	C277057CABD9D6139587468A8A2548A22E1F88F2D33C076F81420EF4F3C208A8
SHA-512:	94D37CA1F9783D9E7E5D147E197D558C4384FCABFD1F555E0782E25B9BD354D9928B1F3724A64FA3D88B7185C043C27968AB04CEE8C811336A5FB389E865F1A
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":"13274463031981034","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\90c71b78-a18b-4d37-8790-84cf6a0ab6fb.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):	1708
Entropy (8bit):	5.58232899607893
Encrypted:	false
SSDEEP:	48:YI6UUhGUgUtSUAseKUepfqPeUj/TsUvUef+wUfUkUE:GUUEUgU0UA3KUhPeUnsUvUE7UfUkUE
MD5:	145431819ADE8A61B924F31C83D1A273
SHA1:	A11E379E66E78300739C493463184F32E8AE2115
SHA-256:	4CF23D98942E873B4C841572FA206F4E8BC4A20883A9150FEA39FDB7AF45C1A1
SHA-512:	AC7AD6402FF6581CD94C11343A162A8246F5D3AE6C19E51C38794D39E166BA14E0E64CC1AF06C7728D7B5669BE8B670BE93CB2EC5EFFC8DD7FBB93895F3A918
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1640875849.57971,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989449.579716},{"expiry":1661525455.206836,"host":"kYxWDeIDVgesBS02XkmPRTIpB0nkimBvKZESXctn8eA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629989455.206841},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1661525455.503412,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629989455.503419},{"expiry":1640875855.854177,"host":"2lkpJCeDA/iPFazSWca3N4hZCz/cVnuSdphlO2veD4Q=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\98545cb9-f608-42a3-85d5-b3095af279fe.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\98545cb9-f608-42a3-85d5-b3095af279fe.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2546
Entropy (8bit):	5.5989750337115805
Encrypted:	false
SSDEEP:	48:Y9SU3TakUnweUyXieUn6UUh/UBtSUZmKU9yUafqPeUMTsUbUefQwU54UQxU7:hUjrUnweUuieU6UU5UB0UoKU4UaCPeUL
MD5:	0D043EE9E03F90CE24D822ECCA2F1D97
SHA1:	DD139CCA77AC563D2D34E10B701405557FFADB1A
SHA-256:	41BDEB91206033F294F6C51826E14415C4CB930B50D9B8D53DFE7702A1957DCC
SHA-512:	556A618E582AE78F7404355C56310F4545D4232804DDAF4A0EECF0BEE1800777AE3EE2C80B500370175942FD75CA82ECAC2F843F4FB7198258B12721A33DC387
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1630011099.751657,"host":"Bgr28EGzaqFzUXieBdnVZmUK1Wm4iy7JUTELEIadp84=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629989499.751661},{"expiry":1661525484.090108,"host":"KVivTTKTVC3D7/hfpnbDFfPAgoVJQnjFfXBq+8P8zk8=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629989484.090113},{"expiry":1640875899.747816,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989499.747821},{"expiry":1661525499.291745,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629989499.291749},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1661525499.576978,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_ob

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):	5.296968528704211
Encrypted:	false
SSDEEP:	6:mDMq2PWXp+N23iKKdK9RXXTZIFUtpqI5ZmwPGkwOWXp+N23iKKdK9RXX5LJ:lva5Kk7XT2FUtpqO/PG5f5Kk7XVJ
MD5:	242F2CD234472467F0B63E99F50406C0
SHA1:	4976F0D7CF399BD916603CF65AFE414D1CD32656
SHA-256:	F767C1827A9750789FB5506AD1CB6962296A31C94F5EC1D335995E06C8F90168
SHA-512:	A9CF15B0FFBAFBFEB9336F8E028785126D8F66939E3C5B812C3A4F8BA5DF00A2FB8B3D457E226D1D9BBAB662BDBFC3D734BFE5CE05DC6BA60902E13F977CDD0B
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:50:44.691 1b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/26-07:50:44.692 1b64 Recovering log #3.2021/08/26-07:50:44.693 1b64 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\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.296968528704211
Encrypted:	false
SSDEEP:	6:mDMq2PWXp+N23iKKdK9RXXTZIFUtpqI5ZmwPGkwOWXp+N23iKKdK9RXX5LJ:lva5Kk7XT2FUtpqO/PG5f5Kk7XVJ
MD5:	242F2CD234472467F0B63E99F50406C0
SHA1:	4976F0D7CF399BD916603CF65AFE414D1CD32656
SHA-256:	F767C1827A9750789FB5506AD1CB6962296A31C94F5EC1D335995E06C8F90168
SHA-512:	A9CF15B0FFBAFBFEB9336F8E028785126D8F66939E3C5B812C3A4F8BA5DF00A2FB8B3D457E226D1D9BBAB662BDBFC3D734BFE5CE05DC6BA60902E13F977CDD0B
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:50:44.691 1b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/26-07:50:44.692 1b64 Recovering log #3.2021/08/26-07:50:44.693 1b64 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):	5.273424885647703
Encrypted:	false
SSDEEP:	6:mrq2PWXp+N23iKKdKyDZIFUtpRZmwPLkwOWXp+N23iKKdKyJLJ:qva5Kk02FUtpR/PL5f5KkWJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
MD5:	F76B654EEAAA74D043708AB598DD3772
SHA1:	AA24737BAB81EA01455310CE709147F17EECF9DE
SHA-256:	E34DD8D8F330917D605EA2520B93EEFEB362962210C39CC2F85378CDA57A4C88
SHA-512:	20F6B2983B30CD98F9921809540D49DFCF53E1B82FFF485F1E9220F1B44BF41B9C79F48E64A01B4E4F2284766086B98A5D00DB7ABB2AAFC7061C4488E00197ED
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:50:44.683 1b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/26-07:50:44.685 1b64 Recovering log #3.2021/08/26-07:50:44.685 1b64 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\BudgetDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.273424885647703
Encrypted:	false
SSDEEP:	6:mrq2PWXp+N23iKKdKyDZIFUtpRZmwPLkwOWXp+N23iKKdKyJLJ:qva5Kk02FUtpR/PL5f5KkWJ
MD5:	F76B654EEAAA74D043708AB598DD3772
SHA1:	AA24737BAB81EA01455310CE709147F17EECF9DE
SHA-256:	E34DD8D8F330917D605EA2520B93EEFEB362962210C39CC2F85378CDA57A4C88
SHA-512:	20F6B2983B30CD98F9921809540D49DFCF53E1B82FFF485F1E9220F1B44BF41B9C79F48E64A01B4E4F2284766086B98A5D00DB7ABB2AAFC7061C4488E00197ED
Malicious:	false
Reputation:	low
Preview:	2021/08/26-07:50:44.683 1b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/26-07:50:44.685 1b64 Recovering log #3.2021/08/26-07:50:44.685 1b64 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\092afaa13060536d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.4061163879512275
Encrypted:	false
SSDEEP:	3:m+l3lK8RzYrWPJupQuVNRp2KZl1qlH/lHC18lUTd9HPHG5hsN4kvRmFD5tllpK+:mcnYp+0dZDqlHg1PTddCilAFD5RK6t
MD5:	E9D20DAB4A3FA77895160A87CE88E210
SHA1:	965E3094E13BDD9632E5CDFE559C11449A2BA456
SHA-256:	07B22A6C2CF39C85CDB658C9560C1A34C91DB785BF850AEDFC1D5DBEC6216B81
SHA-512:	31ECA3F8879E868BF0B43B4D10C5D7A500C116D244FDBE649AF6ABFF909A507575349D0A226BE556A600719D4040B33A69553A1216485FC3D0B8FEBE85922DE7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?.....u..._keyhttps://apis.google.com/js/client.js .https://about.google/...../.....7.....2.932..W^.X..*..<U.i..s....*...A..Eo.....A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a57bd28b832522f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.445562695439058
Encrypted:	false
SSDEEP:	6:mYbYGLKda6AaxO3iMQIZKgqS1oGIXw2HhMnK6t:PeQ6ANQyKk1bIA2S
MD5:	25009148C8E61F63C5CE141C487148CE
SHA1:	AF3756335A1543993F415CD746869BF51FA849A7
SHA-256:	ABBDCE27A6CD7FFB1488717E33C5DA0B25054797E4526330FC9A8D1A0FF3CC50
SHA-512:	C1986AE602066A326FF4E38F31D454A626E4C6C32EFA6C7A00F72F4A83EF04E3EA8AFBABB1F7CD9DAE3F8AAB959A16CD2B1E8D3BF9DF526268C1173920BDF4CD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p...OW....._keyhttps://www.gstatic.com/external_hosted/ng_ui_router/release/angular-ui-router.min.js .https://about.google/.^...)/.....3.....tby.cuV.&.....O.\...h.%({..A..Eo.....i.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0adffc88fc30071f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	974
Entropy (8bit):	6.1977854744684135
Encrypted:	false
SSDEEP:	24:bLCY8B6oAkKexwjpjT9bQ8hmu+S0KDrw/71VuLFcwyNM:b2YVNkKex38hmu+xKMhVcsNM
MD5:	A140C74780FCB823B7DBF5666F81A0F3
SHA1:	EE8248443031C44221A93BE09C71E6524660E041
SHA-256:	2D14D7F5590E004FF6BC93BA6CE38F96F404EBB20F5783015722CBECD908FDE1
SHA-512:	6BC43B74F6339AE667EF0059F59360F43FE1BD89D9ACFE22432D9383F3B59D39F22C441D7503F675F060C0C114615DE36C7D07C341BC80E6998D00B631B4A680
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G...._keyhttps://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en.iRny_Wkefus.es5.O/ck=boq-one-google.OneGoogleWidgetUi.JPk-aNkftDA.L.B1.O/am=WAAAEA/d=1/exm=LEikZe,_b,_tp,byfTOb,lsjVmc/excm=_b,_tp,calloutview/ed=1/wt=2/rs=AM-SdHuqGlTqF50PcbuHE8DjFQoN0CMcIw/m=n73qwf,ws9Tlc,IZT63,e5qFLc,GkRiKb,UUJqVe,O1Gjze,xUdipf,blwjVc,fKUV3e,aurFic,COQbmf,U0aPgd,ZwDk9d,V3dDOb,mI3LFb,O6y8ed,PrPYRd,MpJwZc,NwH0H,OmgaI,lazG7b,XVMNvd,L1AAkb,KUM7Z,lfpdyf,s39S4,lwddkf,gychg,w9hDv,RMhBfe,SdcwHb,aW3pY,PQaYAf,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,mdR7q,MdUzUe,xQtZb,lPKSwe,JNoxi,MI6k7c,kjKdXe,yDVVkb,QIhFr,hKSk3e,KG2eXe,hc6Ubd,SpsfSb,VwDzFe,zbML3c,A7fCU,Uas9Hd,BVgquf,lsPsHb,pjICDe,hnN99e,yYB61 .https://google.com/..A..)/.....b.....o.g>.&..,.&D.4Jn...DdT+.F..%A...A..Eo.....L..J.....A..Eo.....A..)/..y..004CFD8234650B0BE23B0D93237031F7ACFFF7CBB78346CF988F1820CCFEEFDE.o.g>.&..,.&D.4Jn...DdT+.F..%A...A..Eo.....m.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0cd82a09b7413176_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.403266275275203
Encrypted:	false
SSDEEP:	6:mQ/XYGLKdakM/RJaZzu0gRgKlllg/DP4RhK6t:dqQF/Rtlj/YDP67
MD5:	9F36050831175C13142417A361DD99B8
SHA1:	E0EF534A7E9F31DB8358D49163FDAE6219BC018E
SHA-256:	176F54E1456710CE4462BA44467F312742FBF9C6EC888410A279505D99A90EA7
SHA-512:	1A973FDB8892DF1686F38972E95620E15EF8456FF79DB5AD9B844766074D235C53E87F74EA328ECE42D2B06218FF77E129F33F2DE30E07E5469CCFED773C314A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b.....P...._keyhttps://www.gstatic.com/external_hosted/scrollmagic/animation.gsap.min.js .https://google.com/w,...)/.....v.....]..WE....m.p8?..{K..X..y.A..Eo....._.}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0faaa62c8524df0d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	364
Entropy (8bit):	5.808337898197953
Encrypted:	false
SSDEEP:	6:mgYGLKdGMwjM71pwXz/6acQote9Tv1cum5lgsxXwD4jnK6t:o9wwhOlcrtyTv1Nm5llF0Sp
MD5:	9CE350F869CFD8CF930D5173F276F021
SHA1:	36F324EBC8252E11403827D4FD58C74699245282
SHA-256:	A8E345452BFA8028065BA96CA9823FD06CF15CD70BAF9E7C7DD0D75A67C6A92B
SHA-512:	2C018B8971AA9ECBF066393F3C89BF764033576520BFFE921091C318A991BE04097853648DA165B3E8384F7593933427269C8B122984E7751DCD817998BE5AD3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....4.f2...._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.IdentityPoliciesUi.en_GB.WJPKByKq9sg.es5.O/am=FBBA/d=1/excm=_b,_tp,techcookiesview/ed=1/dg=0/wt=2/rs=AOaEmlEcql0c_n7v3yBdLpkSHsfTdflgTQ/m=_b,_tp .https://google.com/.....)/.....K.....,g(t..r..d1.....W.....J..&.#.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1154c6710157da27_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.445586999162659
Encrypted:	false
SSDEEP:	3:m+loGxlzA8RzYrSLLiMIwJJSp2KZlGH+H/lHCl1vqrMjWxkh6qUmF/7XlpK5kt:mWj9YGL+MIwJJGZoeHgIjjWc/FK6t
MD5:	4130DC8CCC7C4DA0E24452B05EC4D269

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1154c6710157da27_0	
SHA1:	CC77419CC963706802893A15037017760DD53BEF
SHA-256:	6DEB7C7B76D720823DC539F3F87178DEA7F8EDFCDC6233EBFE1E326A0C6BB4D3
SHA-512:	CEE42666D40FC5DE535D2F5526B603C54D69E9E053F34BF9E0ECA443D017D5B37751B44B3D555322D3BAB940553EC6888848A7C090C1D2D663FA4EFC87206DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...6..N...._keyhttps://www.google-analytics.com/analytics.js .https://about.google/...../.....8.....3k...w[..).`P_s..Y...`W.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\11872aa7eaefe3b0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.530789585522105
Encrypted:	false
SSDEEP:	3:m+l/il/gOA8RzYrSL1cdMyw0YcMcHEyMuSfKrEnMt/uFvDp2KZl0k/lHCNgl/M7P:mOuYGLKday7iirVIZSkgNRiE+4RK6t
MD5:	A8063CE8FC666BE350C977EE8768B2EA
SHA1:	EB18B0BE78A298C93D8CD6B1FD8A5703516BBB8C
SHA-256:	B80467ED969D58429603425643E972EEB7CCEFD5D747C716ADB905FD3C5A100D
SHA-512:	9AE871B2AB1BC7EB68F9773215481DD311B1CD15F5BFF73F0CEECE38601FFD4FB0EAAAE82CF12F4786632378A534B442C5DA801FE40103ECDD957949F4B80A 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}.....u...._keyhttps://www.gstatic.com/external_hosted/intersectionobserver_polyfill/intersection-observer.min.js .https://about.google/9`...)/.....(3.....g .'?..Q.`.P...|.bV....]..T.m.A..Eo.....O;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\12318cd0c335b8e0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.394586721814577
Encrypted:	false
SSDEEP:	6:mcYGLIgNa9NXgOXLZzua4gFwW8NnxK6t:iv9gOXFqa4M8NL
MD5:	80A5232D34239F522411F6AECA90CE32
SHA1:	DED283ECAF9525A0E85170F83578449E304F96B8
SHA-256:	247F8FFCEB049FF5E04CF77255174CF641D449B6D86748F20E3A4B1A1E42F54E
SHA-512:	66496AC2582EF8A5BAE64B558B64D720AE30943CD5A44C8826DB06DB952306B97DC719D7F058C4B93F3CAD9C1EADFB129112C3B7142CE901649F2C99A9EE58 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q.....w...._keyhttps://www.google.com/chrome/static/js/installer.min.js .https://google.com/.<...)/.....v.....<...c..5.A....$.....D.....A..Eo.....@x.....A..Eo .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\157ac5dc69855318_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	5.527013607961217
Encrypted:	false
SSDEEP:	24:NaRPkpbaRJyAbaRUCbaRfsbaRG6MbaRh5jzH:s9cmLyAmiCmlsmkxm9PH
MD5:	9F9CEBED49AB710B036F1564E5B03087
SHA1:	3B10E63E452B6708084C9E57D9AAEC8CE6F0604C
SHA-256:	404EF7B3DD679C88010C3D7AB082B6781B57CEFD6F42AE811E8ED17A929F8AED
SHA-512:	B85478BD113B31BE0F2167E2879AD6057DAF45E3EA0C4E360B8AEF33B4B793FD5A8A567539931ED0969D4BE903ECCEF837B44953987772D58239D198908A4F4F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....?3....._keyhttps://www.gstatic.com/feedback/js/help/prod/service/lazy.min.js .https://google.com/.e...)/.....3.....9zB.p.e...MaH...-%P.h...A..Eo..... ....A..Eo.....0\r..m.....Z....?3....._keyhttps://www.gstatic.com/feedback/js/help/prod/service/lazy.min.js .https://google.com/.r...)/.....z.....3.....9zB.p.e...MaH...- %P.h...A..Eo.....A..Eo.....0\r..m.....Z....?3....._keyhttps://www.gstatic.com/feedback/js/help/prod/service/lazy.min.js .https://google.com/..9..)/.....3 .....9zB.p.e...MaH...-%P.h...A..Eo.....!tQ.....A..Eo.....0\r..m.....Z....?3....._keyhttps://www.gstatic.com/feedback/js/help/prod/service/lazy.min.js .https:// google.com/N....)/.....S.....3.....9zB.p.e...MaH...-%P.h...A..Eo.....4.....A..Eo.....0\r..m.....Z....?3....._keyhttps://www.gstatic.com/feedback/js/help/pro d/service/lazy.min.js .https://google.co

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\15a5acad06e31190_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.494880431011466
Encrypted:	false
SSDEEP:	6:mms9YGLSmXZC6ngguq+Hg9A5MH5kNH46DK6t:xs9bgxqu+d5kNHj1
MD5:	1210F0E739144B0427AD50A4DD2E7409
SHA1:	E281F6E2920C9450D6A5199D49C3253B63F99A9D
SHA-256:	834EE63F53EAD4E2DBAC26139896F623D2772D6C89E54545449112648681DBC4
SHA-512:	F75760CEC557B917989851CA9103FABDE518CC2D9F99A4A0FEA35F46C7895091E889276D0453A1F232CA745B543FBB87DC1C8D115EEF23EFFEA6E7DA27899F2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....=^...._keyhttps://www.googletagmanager.com/gtag/js?id=UA-26908291-4 .https://google.com/.A...)/.....%w.....FS....N3..Q.p.ap.....d.b..A..Eo.....J .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1d9307e50ef6b7b0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	5.406039086314047
Encrypted:	false
SSDEEP:	6:maYGLKdZgRbLe8lNdZj0gTn/vd49gL/bK6t:mjybLlINQul/N
MD5:	B5817B405815A351E369ABFBABE23757
SHA1:	93B837366F5FF4B8D57C688F9DF9926FE4055D88
SHA-256:	FC3FAE81DAAAC600287C8982835BB7A379A514F71A7C4D4ECA8943242CD8F5D5
SHA-512:	58A723B9078FCED1F6FF48F6C6FA7B8204826DB13430AA9589094491A58882ABA673B10DD69C5437CF6D09D422E94C419A08A49965D93743F537DE2C25485257
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t...P_k%...._keyhttps://www.gstatic.com/brandstudio/kato/cookie_choice_component/cookie_consent_bar.v3.js .https://about.google/.`...)/.....66.....ex. {T.;4.a[..Tt.NzpL..q.@..8...A..Eo.....>.r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\25f13bc86c899fc9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.587765954190951
Encrypted:	false
SSDEEP:	3:m+lzLb/08RzYrSLSELDXZCLRlH03uut/lHChXJH4yhzK5mzEuhtlpK5kt:mA/VYGLSmXZCLRwu6gh6yhm4zEmZK6t
MD5:	E765E8101B17C5D45E30E383389DB504
SHA1:	081B13970C791D4865705EEF90FA32BD15B14C04
SHA-256:	036EFB7B6B38484CC327DA1A220C3BA5A13B9BC0A780C47E769C1D393B7EA9C5
SHA-512:	2EEBBD93062A204A255BEC0DB8B18AE43A52087CE24BB179470E82703BEF877989ED0D593E21CF8DD005B803F4B2EAE895466E0E22D9822ABC3E80EBCFCE79 4D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....y<...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-PZ6TRJB .https://google.com/T:...)/.....w.....5..Q..x..j.....Kc.....g7.....A..Eo.....~!K..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c9e2bb71fa794ce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	358984
Entropy (8bit):	5.843304516909506
Encrypted:	false
SSDEEP:	3072:ltzpo4UJ9Xv2kp9m5a1d0S0/3wWPPARqsncfpHr6WI0UwqpZUgdraL8w5nCCqhuj:lNJg9uKg3zPARccWmrYYEKXG35
MD5:	B2D89BAB88FB11499A3DC3230BEB8BBE
SHA1:	A79CFE57D3CAB5E5A98E631C98AC16E308EE7517
SHA-256:	9F235E18D4573CF23B45410D855F01C50B8FD66FCAECAC297284FDA7CF55F93B
SHA-512:	EBCC186CB44C84E3EC57AA8FDF46977BE365B9F867BFC8B249CF0C2C7EB98CA8F27183F7E12971102B96D232214566CC736F1581887E641B2EF5318DF11742C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c9e2bb71fa794ce_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....004CFD8234650B0BE23B0D93237031F7ACFFF7CBB78346CF988F1820CCFEEFDE.....'.{q....O[....x...<.....l...*.....\!.....x.....\.....t.....(S.l..`..... L`.....Q.`~$....._F_installCss.....Q...b..r....KL4X6e{background:#eeeeee;bottom:0;left:0;opacity:0;position:absolute;right:0;top:0}.TuA45b{opacity:.8}sentinel{}.....(Q.....default_OneGoogleWidgetUi....(S...m.`.....*L`>.....Rc^.....Qbf..k...._.....Qc..{.....window....Qb.....tC....Qb:.....vC....Qb.....wE....Qb..E.....xE....Qb...>....sv....QbN{<Z....LB....Qb.~.....MB....Qb..q.....NB....Qb..?F....Cv....Qb.@.....Dv....Qb&..G....Ev....Qb.]I....Fv....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2f3ce0ee52f9749b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	154744
Entropy (8bit):	5.82444985264933
Encrypted:	false
SSDEEP:	3072:6qeccl5eNQ5OLV+Lmaq2mRlBldTqsPatXAn7aiwT:Zo5M+OL0t1mtldjPIme
MD5:	9A53E0D73B2CC2EDE5127FA85271FF7F
SHA1:	E8FDA90EEC537AB9EBB0188E4BBEC11D2AA7E3F7
SHA-256:	2D8E61673AB3F56BD0561C6DBC252C742955F78F7F5881264681419CBF3E9B72
SHA-512:	264EB63BC4E7AA633C4000C9D39AA53E4CA792679A8D7756704258BC1EBF677DF1B40081B0A7DE4A3367E960C635CB9E5D9D278B1C9EA3259F94ADDAE8C565F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...m.....C5C7B9F893083797536B968BA5C61A151C1334604AF9E66D8E66A5C90A67934B.....'.....O.....Z..$."..... .....L[.....H.....@.....(S.P..`Z.....L`.....Q.@.QKL....gbar_....(S...M[.`T.....L`.....u.Rc.....Qb.....\_....QcB.....window....Qb.....Nj....Qb.....Pj....Qb..C&....Vj....Qb.....Yj....Qb.T.....Zj....Qb..OR....ak....Qb6.t.....bk....Qb.A.....gk....QbJ.....fk....Qb^..a....ck....Qb..>.....dk....Qb...P....ek....Qbv.....jk....Qb..$....kk....Qb.P.....sk....Qb2!.#....uk....Qb.ynT....wk....Qb..n.....yk....Qb...5....Bk....Qb.....Ck....Qb2._.....Dk....Qb".....Ek....QbRs.I....Fk....Qbba,.....Gk....Qb.W.....Jk....Qb.X.....Ok....Qb..P.....Qk....Qb..Z.....Sk....Qb...(....Rk....Qb..ti....Tk....Qb..%....Uk....Qb.=jc....Vk....Qb~..V....Wk....Qb~F.....Yk....Qb.K^.....al..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2fc3d3a085992c47_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.415411356164397
Encrypted:	false
SSDEEP:	6:mY1wEYGLKdakMyEhu5JRgqllFJpR9aF5/yK6t:F1YQFyP5rD/FC5c
MD5:	7A28EFCA2663546EF263AA6482DB06E6
SHA1:	FC5F15D6538F6C4877B04DD7E138E5F40EF2580A
SHA-256:	32018970A7F408816EF0B78394D69D5FB6BA407EA1D84543921BC616C08F2127
SHA-512:	0138C6396FCAB0869B817562B9FE5B9881EB0CA76924B98BC01BC75D1B62A7AE7C6BBFAF54146FCC1770E3A98DCB1FA0B1BA859C3854241BCE4D31EDB90DDE8
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....d(....._keyhttps://www.gstatic.com/external_hosted/scrollmagic/ScrollMagic.min.js .https://google.com/A..../.....,_v.....|.[..bE....).....~3 .xL..A..Eo.....6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\33b01b663beb49c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	859
Entropy (8bit):	6.074653709861932
Encrypted:	false
SSDEEP:	24:ejwwvCXMOkmL6kGB+T9cHbw0MxDDLw4kp:0NvXOkUGBa92bPGA
MD5:	5238FA15DBC00CB266A69A8E6C3E241B
SHA1:	0A41751758EE5CCBD91ECDAE5FF40597F27CE7E8
SHA-256:	BBFDAE963D6ADA65EFBDF009767DF1C39F54C1B6DC51BE10108A5D8FCB368C6A
SHA-512:	77A999E275A73B6DEF955A3D860B3313081267814E0D2EEEF81DEF4BCC0E36260158D81DAD3098CE725F2DEA97CFD39D7F0DA84453D2FB9C2937FCAB887A989
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\33b01b663beb49c6_0	
Preview:	0\r..m.....*.X0...._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.IdentityPoliciesUi.en_GB.WJPKByKq9sg.es5.O/ck=boq-identity.IdentityPoliciesUi.emeApl-K2Wo.L.B1.O/am=FBBA/d=1/exm=A7fCU,BVgquf,COQbmf,EFQ78c,IZT63,JNoxi,Jis5wf,KG2eXe,KUM7Z,L1AAkb,LEikZe,MdUzUe,MpJwZc,NwH0H,O1Gjze,O6y8ed,OmgaI,PQaYAf,PrPYRd,QIhFr,RMhBfe,Ru0Pgb,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,XVMNvd,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,b7FMof,blwjVc,byfTOb,duFQFc,e5qFLc,fKUV3e,gychg,hTAg0b,hc6Ubd,lPKSwe,lfpdyf,lsjVmc,lwddkf,n73qwf,p8L0ob,pjICDe,pw70Gc,r2V6Pd,s39S4,w9hDv,ws9Tlc,xQtZb,xUdipf,yDVVkb,yJVP7e,zbML3c/excm=_b,_tp,techcookiesview/ed=1/wt=2/rs=AOaEmlEF3bs_4xHLUd0miI14DLuSumW31g/m=FqLSBc,krBSJd,wmlPKb,IavLJc .https://google.com/w..../.....H(.)..#?d.N..u.xt.y."t;~...A..Eo...../.}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\33d8ea273e8e208e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.609643369753543
Encrypted:	false
SSDEEP:	6:mRwwYGLKdaY0fVRJTPwZG0gHgyz+cB74nc//hK6t:mwdQ5NRJTPK5e+cBrr
MD5:	03451D9DB6A2564CC7572C62E5C60025
SHA1:	DF30EAB44A4115A817CBD88DB62E6D75C1C6839D
SHA-256:	9ED3C5127E21764E204C67ED27DB2914FB4A4B3CF643845860815559FB8D738D
SHA-512:	6A5C44BE753D2DDCC314DFBCB45C7101650575BFD7B21E4805866ABDE39155B54D2B9F3F46D053D8EB29095286E40F5CAD1FF6FACDA2C6FF151DBA8286533D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....Ql...._keyhttps://www.gstatic.com/external_hosted/gsap/v1_18_0/plugins/ScrollToPlugin.min.js .https://about.google/$_...)/....."3...../.*.....I...'..#....??..F.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\346866bbe969e451_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.575365607750835
Encrypted:	false
SSDEEP:	6:mGltXYGLKdTdTHifHZFctg+llegLD6ko4rSK6t:qJdTHif5FctpYEDfo/
MD5:	3373A54E4E5197406D23981AB37B1703
SHA1:	74D35AAD7B9DB0E2B302591801264619CD6F2B08
SHA-256:	6C7B8F6649A46B642EE83C5A1DFFA96FCF3F689780AD3AB672E9E4C292124F9C
SHA-512:	699D932C64E5D5FC443D5DBDF817E7BE3B8896CB5D5E8DE1B7C415BB25792F64FA5110955506D85D3404E3288FDB3437662FE190739D1B249844E943654E7576
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\....j...._keyhttps://www.gstatic.com/feedback/js/help/prod/service/lazy.min.js .https://about.google/R..../.....4.....S.....V.....<.._J..U....P...A..Eo..... X.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3653004befb613c5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.5262969325408715
Encrypted:	false
SSDEEP:	24:ViQVAd/adVX/doVX/9RPVo/jrUV9/d0jVq:Vir/aX/dy//q/M/ek
MD5:	729C1ED0F1D67691AA80BAB8E3333F15
SHA1:	C0F053A50BDB5D7A5E180B4A9876386F6990B233
SHA-256:	D1595A2C3C694E2C45B3251A42784DAFCBDEA5C7C1C15423C8A8F4E976EED5EC
SHA-512:	86B400F7E5D1DACB62326FD209527A9976D43ACEEB9EDB80CD23C6449677A936F4A6E18251FD3DB276A91E21AB90CA084484764FF961738123002B6180C92D72
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....A....._keyhttps://apis.google.com/js/googleapis.proxy.js?onload=startup .https://google.com/Zp...)/..... ..B....}#...V.".yx.;...p..4..A..Eo.....*.....A..Eo.....0\r..m.....V....A....._keyhttps://apis.google.com/js/googleapis.proxy.js?onload=startup .https://google.com/.....)/.....j..... ..B....}#...V.".yx.;...p..4..A..Eo.....'RN .....A..Eo.....0\r..m.....V....A....._keyhttps://apis.google.com/js/googleapis.proxy.js?onload=startup .https://google.com/..B..)/..... ..B....}#...V.".yx.;...p..4..A..Eo.....A..Eo.....0\r..m.....V....A....._keyhttps://apis.google.com/js/googleapis.proxy.js?onload=startup .https://google.com/.....)/.....a9.....B....}#...V.".yx.;...p..4..A..Eo.....C.....A..Eo.....0\r..m.....V....A....._keyhttps://apis.google.com/js/googleapis.proxy.js?onload=startup .https://google.com/MO..)/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\36f490bb56fc958e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\36f490bb56fc958e_0	
File Type:	data
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.922015921129114
Encrypted:	false
SSDEEP:	12:OEm80vb01iRlfMMZXQ9+mXa1zK+YEXFhA:OfnvbqZMZXQJXqzKt6k
MD5:	2B3266E3AA601F48C9696455DD8737A4
SHA1:	AB948596BDBCD37F441D9735BC0FEF9C838DA6F2
SHA-256:	30443F63EA2272DF8D7547F9C4F1DDB78301E7520CA7E0F4484B4E7E4A3A3292
SHA-512:	23CB476EBB96CB0C3CC10F4AE2A7C66A77AB228832FA459F4A4B484829FAEEA8E2F374A1637F79200903DF08E438A21D85AEAA65EB69B271389D7C42BACE4D DF
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.wxcShFhZxXM.O/am=B0jRwgiSeAEBAIQcAAAAAEAAAOCwAWXAOXy GDw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax3JsMRB_j3XGRToGaFFZSy2qHwG2A/m=sy32,sy31,i5dxUd,m9oV,RAnnUd,sy2u,sy2v,sy2w,uu7UOe,sy2x,sy2y,sy2z ,soHxf .https://accounts.google.com/?W...)/.....r.u.....A}....;.a{.X.6.....A..Eo.....Ei.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\38d11efdcdf6f350_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	392
Entropy (8bit):	5.745441393830244
Encrypted:	false
SSDEEP:	6:mXeYGLKdbVnIIKG9zJ6MVYG6RfaoG8aT76CeYCWCbCuO2J2QCgu8XFgUk7thK6t:Y77n/KGr6MyNCoG56rWcCzu2QuGFPK
MD5:	00423E089016B3E1C2CDF4DAA1B6D62A
SHA1:	4F1771ABECADF01CEA6FCDC9D213BCB6889C8CD7
SHA-256:	F1A811525A7D9385E41A8D5700F54A6070A9588D564F87056E7B014F30757500
SHA-512:	ACC63284449068696B4BFB91DFD45C1D42FCFDEF3C7D8C5A79306A031F8C845F1267E8DEAD5ED45A5009EA94AD0EE5529587BD027A2BABB2389F410939BACE D0
Malicious:	false
Reputation:	low
Preview:	0\r..m....."W...._keyhttps://www.gstatic.com/og/_/js/k=og.qtm.en_US.eyZtLN7gU00.O/rt=j/m=q_dnp,qmd,qcwid,qapid/exm=qaaw,qabr,qadd,qaid,qalo,qebr,qein,qha w,qhbr,qhch,qhga,qhid,qhin,qhlo,qhmn,qhpc,qhpr,qhsf,qhtt/d=1/ed=1/rs=AA2YrTvbnfZ7vgSllYOF3f_IHBGeFFy7Mg .https://google.com/.r...)/.....h.f...E.H.11 .0.3...W._O...A..Eo.....0.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\39208e3502e0f8fa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.402746359276534
Encrypted:	false
SSDEEP:	6:m2EYGLKdaXWKEjxWImukprg0xTFN/nJrK6t:dhQcgrLdFNv
MD5:	61AF9D8503361279417A0128A61F5F2B
SHA1:	4B18B9FA5CCBA457463CD1A95DAD2D325D64606A
SHA-256:	65FA6B709A1F8FEFABD647C150E9B77CBD13B95B392C86FF4D342AD276716DC7
SHA-512:	26AA29F5A668C4A94C2D53D1C275FA126C28B6A4F73EF5C293301491EDECB1773542D98E7F66C7B436B8B75B146EB76CF257B0B1D47D013D141F6AEF8246A6E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://www.gstatic.com/external_hosted/autotrack/autotrack.js .https://google.com/...../.....s.....S..)...`..*.}.Sq@.....v.....A..Eo.....".4..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bae4111b6f3d84b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	481
Entropy (8bit):	6.01485913055485
Encrypted:	false
SSDEEP:	12:pIZLZ0vJ+N6cBHc5psVMEPHUVBNXWA9e2RkkOO8VYmyd9WA9:mmv7cBW0MiHUB60kkOfYmy
MD5:	4660796C91A3C56ACC614C5AB78DEC99
SHA1:	D75150038A9B0AEE3046297354E7D79358A2FD46
SHA-256:	326B6DF6140A57EF0F0ECE6E28069E18CF425628EF4DD031E6535051FC576B3A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bae4111b6f3d84b_0	
SHA-512:	4AD4998B7876CB77472E91BC0EC409A06FF7E98E6E32A4EEE31EC70215A0CD58156F6C2BCB8B514D8A269C80D8297DF5F5E8F811D1E95E17C5DA33851ACDDE9E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....yWxd...._keyhttps://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.7RphtNcGHDQ.O/m=client/exm=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_-zmYhp_Ir7_CCxM3l-AckMval9A/cb=gapi.loaded_1 .https://google.com/...../.....0.. p.n..R...MhGo.dQ.....e...).A..Eo.....A..Eo.....)/.....3C17A8C519142CB0AF7EBCC330AB0612F4784B61B6232FC81B1B5E65768E186D0.. p.n..R...MhGo.dQ.....e...).A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3dbe54b7c92541c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1748
Entropy (8bit):	5.747153102557772
Encrypted:	false
SSDEEP:	48:fgL/DNta1gL7tSntz1gL0Jt/1gLfr/tj1gLn0tO1gL6UtX1gLK1t5BtrgLLXtg:fgLCgL7MHgLagLXgL5gLPgLEgL
MD5:	0B2E26814955365AE548054E48FCD698
SHA1:	510F795AC7301CB4C14820E6BEC326106390D0B3
SHA-256:	57E9691BB353672B8A107F79D26213AE5B39370BBA769960B682C26164A5E019
SHA-512:	BB02AB0EDA3C88848FDE8038C2C09036D3BD79E84BA4D17C53DD85C8C3D36E96956EE450AF1C9BA69005F156C224DEDCC79D2CC8842015AFFA826D44BE400EC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F...W....._keyhttps://www.google-analytics.com/analytics.js .https://google.com/.P...)/.....R.....f.\M.+.....f.P(G.....v..G.A..Eo.....'.8.....A..Eo.....0\r..m.....F...W....._keyhttps://www.google-analytics.com/analytics.js .https://google.com/.6...)/.....f.\M.+.....f.P(G.....v..G.A..Eo.....ru.....A..Eo.....0\r..m.....F...W....._keyhttps://www.google-analytics.com/analytics.js .https://google.com/....)/.....f.\M.+.....f.P(G.....v..G.A..Eo.....K>Tv.....A..Eo.....0\r..m.....F...W....._keyhttps://www.google-analytics.com/analytics.js .https://google.com/w.0..)/.....f.\M.+.....f.P(G.....v..G.A..Eo.....o}.....A..Eo.....0\r..m.....F...W....._keyhttps://www.google-analytics.com/analytics.js .https://google.com/.+...)/.....Q.....f.\M.+.....f.P(G.....v..G.A..Eo.....kB.a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3eb7118a6f9ed95d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.394547056743523
Encrypted:	false
SSDEEP:	6:msCsYGLKdakM/RJaZIZeYug7aJ7NLK4b/nK6t:bCJQF/R7eFm2NR
MD5:	FDEC10DC8EAC6806DF38A7B5121B8AD9
SHA1:	4FC2CCEED1A13535E4E7BCA3CFDD63D37318E317
SHA-256:	5F5318F479FB8F323BB95753768FC4FFD13BE264D0D9B2BE74A177EFE50BE60E
SHA-512:	6D71FFC39791C3DD71A48C5DBF4E5129B3ADEE98DB9BB6C4F14269309CC8269FE59B2D64556F6B43CA28793E3A2F523F8831325038484284F5F3C853219F318E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...O.v....._keyhttps://www.gstatic.com/external_hosted/scrollmagic/animation.gsap.min.js .https://about.google/a_...)/.....%3...../m.....::.7...l..o.S.A..Eo.....I{.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ef1db799a99929f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.69469334169467
Encrypted:	false
SSDEEP:	6:miR/PYGL+MORm/msl5xj0vNguwMugBSfl+K412/lbK6t:p5LpvlL4VxwMuJflK2tN
MD5:	6D9F7E042F0DA1776F0BE4B84F91FBC8
SHA1:	DD7D2C439DBF7D504AC272B55BDF4BA470AFB526
SHA-256:	B888FBDC54990E46AB7AE4383A7F0793AA085CD4030314087F7E747C4BFDEFAD
SHA-512:	82C36ECC4AD09B64BA30F5A585F3A028EA21B82AEAEF13B1CF98DDCCABE2A009A9F25D20871584328B490B5D7BB535EEBEFB947709F9BC395F4BBBE71025FEF7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....qt...._keyhttps://www.google-analytics.com/gtm/js?id=GTM-N7S69J3&cid=125137350.1629989500 .https://google.com/.\...)/.....yw.....*. .~.....;|;...t..J.s.....A..Eo.....$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\49262f63b44e3629_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	245624
Entropy (8bit):	5.842670678161984
Encrypted:	false
SSDEEP:	3072:2Mia6ZtqcO1HXRvJsEkfTWAK39VkLHnENG0cNH+jMQGS:Z04tyE8TWpSkQNH+YQL
MD5:	85A00013EE4788FF46719B13C771F291
SHA1:	84868D289B7A546C2701F9C3C4297BCCD3CD8864
SHA-256:	5FDBF96AA5994C1F41C6CEC9036D61FC5AF4F0C15EBF33DB3F2D43F1951B9B0E
SHA-512:	1D36C743565D89CDDA860540BFB353B58EEFD8AE3A31C19C54172881B199D8C60BC38BA15B5CBC6BA290E08743291F9922477651E813E401D4E560003B213C6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....<....E827AF92C97F4D8E31BA101A90495E29B9C03BA1BF6F1AA3C0D39906A53D47B5.....'.C.....O?.....bz.....8....$.....p...4..... .....p.....(S.\..`t....L`.....(Q.....default_One GoogleWidgetUi....(S...9.`&.....$L`n.....Rc.....t....Qbf..k...._.....Qc..{....window....Qb.....fa....Qb..7?....Ga....Qb..N.....Wa....Qb..Q.....db....Qb...8....bb....Qb.\,.... .gb....Qb...a....Ab....Qb.....Eb....Qb.o....Ib....QbJ.....fc....Qb..0....pc....Qbr>Co....rc....Qb.Z.{....sc....Qb.....wc....Qbf#j.....Dc....Qb2.ig....Hc....Qb.K.9....Ic....Qb.....K c....Qb..Z.....Nc....Qbzu.P....Qc....Qb.R5~....Id....Qb.....Yc....Qb..U.....qd....Qb.....aa....Qb..O.....rd....Qb..d.....sd....QbjYA.....wd....Qb...)....zd....Qb.p.3....Fd....Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d7e25bd6eba05c4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	977
Entropy (8bit):	6.243101363970585
Encrypted:	false
SSDEEP:	24:VCVoPbqwjpjT9bQ8hmu+S0KDrwjVu0fljT142lumIj:oV8+38hmu+xKP08142lu
MD5:	0C66844083D6D1B83480456A9F3F2A9B
SHA1:	46054D900EE4C730BEE7E3ED387C2455A1997835
SHA-256:	C42A68196C5222D124C84477C22C0BA242BB079D0407F99F6B117F3535A3D9D9
SHA-512:	9388AEBABD85A6C18BEDD58905D9B15D4A6BA69502671BD5985C6A87D02125290D22B5B0EB79FE253E1E99F952D5E59DA20D85AE70E4979320BC639CC8690B 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b..5...._keyhttps://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en_GB.wVRNMqnU4o8.es5.O/ck=boq-one-go ogle.OneGoogleWidgetUi.JPk-aNkftDA.L.B1.O/am=WAAAEA/d=1/exm=LEikZe,_b,_tp,byfTOb,lsjVmc/excm=_b,_tp,calloutview/ed=1/wt=2/rs=AM-SdHuCsQ-hWdO twxEofge3F3rTWPHdHg/m=n73qwf,ws9Tlc,IZT63,e5qFLc,GkRiKb,UUJqVe,O1Gjze,xUdipf,blwjVc,fKUV3e,aurFic,COQbmf,U0aPgd,ZwDk9d,V3dDOb,ml3LFb,O6y8ed, PrPYRd,MpJwZc,NwH0H,OmgaI,lazG7b,XVMNvd,L1AAkb,KUM7Z,lfpdyf,s39S4,lwddkf,gychg,w9hDv,RMhBfe,SdcwHb,aW3pY,PQaYAf,pw70Gc,EFQ78c,Ulmm rd,ZfAoz,mdR7q,MdUzUe,xQtZb,lPKSwe,JNoxi,MI6k7c,kjKdXe,yDVVkb,QIhFr,hKSk3e,KG2eXe,hc6Ubd,SpsfSb,VwDzFe,zbML3c,A7fCU,Uas9Hd,BVgquf,lsPsHb,pjI CDe,hnN99e,yYB61 .https://google.com/.?...)/.....N.....%$[.b8.^.m-I....W.l..*....A..Eo.....55.".....A..Eo.....?...)/..y..7D068FC3F843A086F6714740 FF44524677A3ACCE59F961796F20680B3F10027D.....%$[.b8.^.m-I....W.l..*....A..Eo.....:+L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f5681f2e8ddfb33_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451
Entropy (8bit):	6.063020754778832
Encrypted:	false
SSDEEP:	12:UkuEm80vb01WRlfMMZXrrKl8vAeXcLp+yFUZhGMq:PufnvbqtMZX/k1nt
MD5:	7F827FC46462990C12875C7ED840A717
SHA1:	E90266A6FFCBC87F3446EDAE0FC95CF212A847CA
SHA-256:	3B535A2C56EB9A54B8553FDC2DAD18563A84E6B1636B3B063E87DA3A8E30FE60
SHA-512:	F6A70BAF8465A15A7D1F023844CE028C9F709CDB2D0F27E0B3EF955D4F6F7CBDC0C981CBAAE308AAC76754E6CD877217BBD9F8C9B64B48456CFA616C6A444/ 41
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.wxcShFhZxXM.O/am=B0jRwgiSeAEBAIQcAAAAAAAAAOCwAWXAOXy GDw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax1gbLtMuNhkPy_WFDM6EbCrSJwQ2A/m=n73qwf,MpJwZc,NpD4ec,SF3gsd,O8k1Cd,YLQSd,SWGa5d,o02Jie,rHjpXd,pB6 Zqd,QLpTOd,otPmVb,rINAl .https://accounts.google.com/L....)/.....4E.....SU.....{..G@@..GG..d... ...A..Eo.....XS.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\53a90dd59b2449a8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	434

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\53a90dd59b2449a8_0	
Entropy (8bit):	5.934783253806663
Encrypted:	false
SSDEEP:	12:E8Em80vb01WRlfMMZXrrKt9+mXa1zK+Zx4yX7:E8fnvbqtMZX/0JXqzKkD
MD5:	CFE1957916F2CDBF356570E236439103
SHA1:	D745213EAC6CD28DAC99621543544984082D61D8
SHA-256:	54620AB3E694255A3FF08CA84CEE7B069EFA49481D6EBC8744CF536D5732E428
SHA-512:	6979FC84B8B219572FC7A9F312C1457AA1535BDFD763BA2D06DC7F100493E2EC47F3F02138EC5DEF3444BC8520D3BFB37831A49A5600DF09397DE862FFED669
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b.~...._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.wxcShFhZxXM.O/am=B0jRwgiSeAEBAIQcAAAAAAAAAOCwAWXAOXy GDw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax1gbLtMuNhkPy_WFDM6EbCrSJwQ2A/m=sy32,sy31,i5dxUd,m9oV,RAnnUd,sy2u,sy2v,sy2w,uu7UOe,sy2x,sy2y,sy2z ,soHxf .https://accounts.google.com/V..../.....pE.....v.....m'.)_t`iq.../....c.....A..Eo.....M..m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\588e6311b9075013_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.583667962018578
Encrypted:	false
SSDEEP:	3:m+lQkttgv8RzYrSLSELDXZCLRvLvN3H2KZlh/lHC9jllX1OBdq9nkbKWmJt/pK5M:mutYGLSmXZCLRTTZvg9j/UBdq9/1K6t
MD5:	D11E755C5AC3D90C1277B5E5084FC66B
SHA1:	6AECBA8402FF04A4B191658BF8A3EBEBD7B6F857
SHA-256:	7CF689D4382BC5DEC0B7FA0656819C39D96D135D7E95FDC0828CF2E9448E813D
SHA-512:	43D5D411A219EB9C81E3D7ACBFF3B29FFFF4FA766DB766B1BC1BB185E1B0A46D0ABDE71FC30A67BC33C290F1C162DCFFFFDDDD92B1A2CA78520A532D3007 217
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P.....i...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-WQZB4J .https://about.google/...)/.....6.....$.G...~.o..E...\.....E...Q.3..A..Eo..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5b75b2982b074f80_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	467
Entropy (8bit):	6.08370566508164
Encrypted:	false
SSDEEP:	12:J7LZ0vJ+N6YXoM5psVMEPHEG0zOuAJapgmxBobWqpgmTL:Jfmv700MiHEG0AJapfxBYWqpfT
MD5:	7A21CF8C08DF7301A9B75D1AF358005C
SHA1:	E3ACD395A46B27A2AF81822843211114589042C7
SHA-256:	DF8C59720D7B6B545E4B82481C0A489F307C7F591AB2E454C024527A77CC8896
SHA-512:	09DCD33851947B38B2A5739ABC9176F41DDD3B089EF3A45289ABD9CB18886A35E5340255185B33EACD2AE42ED2BF04A764FE094A2CF04B7DA38BE5D2261413E 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....2....._keyhttps://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.7RphtNcGHDQ.O/m=googleapis_proxy/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_-zmYhp_Ir 7_CCxM3l-AckMvaI9A/cb=gapi.loaded_0?le=ili,ipu .https://google.com/.0...)/..... .....=.}.....T...Y.l..lF5.C%..T....A..Eo.....A..Eo.....0...)/..]..09D156A 0BF652215385D58E0B03B09FDACB47E32FB267E1BF38D29D4C462098C=.}.....T...Y.l..lF5.C%..T....A..Eo.....NL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5cd6a02fcd5e00de_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.428169762671329
Encrypted:	false
SSDEEP:	6:mZR/lXYSHT8NB/JZxwZ8lRgZlCJhnZ9kYdunK6t:MDz8NB/EqRisJ9kH
MD5:	43136DD838C645C95E7C26444993B9C1
SHA1:	DBD9E65219E2A273A126BAB094BABBD48605263D
SHA-256:	B39B1AF557D1865CC1196FF56ED1EC3D3AFEBB46884D96378360211C01753A12
SHA-512:	22121536F5294523BB185C5289D68BF5220A8EED24AB50C6197A1A728567532D2F6697196DF652628834758C92BAE2B72D2F00626BF88C375E446A3A9747A915
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5cd6a02fcd5e00de_0	
Preview:	0\r..m.....g...i?....._keyhttps://ajax.googleapis.com/ajax/libs/angularjs/1.6.6/angular-animate.min.js .https://about.google/....)/.....3.....*....o%.]."....'...T.j.....D.A..Eo.....h.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6718ea04bafb0e3e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.793321276282011
Encrypted:	false
SSDEEP:	6:m0DYpEWuVnfj05fx5nRgsUxE6CdHcVxG0TZ1Ttg9rpJJjkfA//ZK6t:J6H0nwfx5ZgE6CFSG0V1TtwrNjkY
MD5:	F1629901093A44130E827F870A12F973
SHA1:	909444218B74D167783C680462DE27CEEE7BF8D5
SHA-256:	FC60D1013FCB784A7F8158DA85A46906A950CA5BB6B4A9BA07469CD430962086
SHA-512:	6A46B521B15F4F0BC85F00C919530CB5157920BEC691F8640FC00609D72B1E128E3934E0579B588719C4BB5EC6D08CEE16219FABD0BC85046ACBD5F32563DBB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w./....._keyhttps://apis.google.com/_/scs/apps-static/_/js/k=oz.gapi.en_GB.tmPnhifxyTQ.O/m=client/rt=j/sv=1/d=1/ed=1/am=AQ/rs=AGLTcCNwoIQ3FEHTIt d0ffFEpbwP-CV1_g/cb=gapi.loaded_0?le=ili,ipu .https://about.google/L...)/.....8.....b9(... ...r.y..okf.....v...5.A..Eo.....3c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6909786d11ca00c8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.970441988597804
Encrypted:	false
SSDEEP:	12:aeEm80vb01iRlfMMZXuQqnMg+NtiDt+Q:BfnvbqZMZXngCtih
MD5:	25576C1252FAA1168FBB6B556B9AE069
SHA1:	5E5A8C2C4E6298D954D6FB068A3AA35EF75B00E4
SHA-256:	C09AF7B08D97FFDBE8AC5DE3C7D7D909AF98D677A4BB2871A2E704E2CB306A78
SHA-512:	9D9B193B1FA4027754A319EF3BB6CF1B82F09638FF64BE3746219BADB621F719B38414BB5F6072DCC17CE50C76E37E5B04F8E4EF4F8D0F70D1C89D11DF49BE5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.wxcShFhZxXM.O/am=B0jRwgiSeAEBAIQcAAAAAEAAAOCwAWXAOXyG Dw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax3JsMRB_j3XGRToGaFFZSy2qHwG2A/m=i5H9N,sy30,sy38,PHUIyb,qNG0Fc,ywOR5c .https://accounts.google.com/.:...)/... .....LP{.oeB.TR...*v...<.c.....A..Eo.....0.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6f03eee6c655138e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	5.88751601548663
Encrypted:	false
SSDEEP:	6:m2mllXYvEdCN8uVvUCll2x1yZRlfM2NZXmA2Ai7ATlhw+ATKtgpR0TG/m4noDK6t:nSl0Em80vb01iRlfMMZXU+suiRqAmgo1
MD5:	718606BCCB4A75EA479BA26FCF9ED5BA
SHA1:	3DA6226167832E29EEBDBE3B07881D889FFE0A9D
SHA-256:	189B92F927DA6428692D07EC8F6EF488DFB9ADBD1F202B185BA4EE7095F2CC6D
SHA-512:	B14CD510927BA9769895A2F3C17529CF42BEFF5BA199A60DB4F720D715EB4BA18573027A80F1C012257FB719ADE0FEB34F7E451101BFE888224B81D46D2B5425
Malicious:	false
Reputation:	low
Preview:	0\r..m.....".c....._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.wxcShFhZxXM.O/am=B0jRwgiSeAEBAIQcAAAAAEAAAOCwAWXAOXy GDw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax3JsMRB_j3XGRToGaFFZSy2qHwG2A/m=sy33,sy34,sy39,wg1P6b .https://accounts.google.com/7....)/.....v.....v...X 0..Xv.....P$g..=K.v.`..=.A..Eo....._.`).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\708b0d476bdfeb05_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.4539324010776635
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\708b0d476bdfeb05_0	
SSDEEP:	6:msCl/VYGLKdakMdMOMZZ2gEXW1KwCSAFJlDK6t:BsQQa72rHn
MD5:	683FABCD6740C4F3FAB0228464B97E01
SHA1:	56F58DC9C13B3D179F7B064D7B8E0009FD8211C1
SHA-256:	901E9DF33EF4E340F53920D6DAD62A8CF775F4B6E64B61257271AF51698BD500
SHA-512:	AF72443945D613D59516D92B2FD1BEF685CE8C9CE1CBCA7460D555E1054AE3C7911CF9F9FE97949AE715998998CCC971911207B44A98DC0FC9FB1966898467B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...@....._keyhttps://www.gstatic.com/external_hosted/pixi/pixi.min.js .https://about.google/x`...)/.....h3.....T..R-...h'.....1..}.....].A..Eo.....[7l.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76de4dcbb9e41e4e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	401
Entropy (8bit):	5.857603732800586
Encrypted:	false
SSDEEP:	12:2A0Em80vb01iRlfMMZXPpOmX2+n1tin94:2nfnvbqZMZXhrmOinK
MD5:	066A9BA064062CF1A092580DB500C35A
SHA1:	2C0EDAA0B639F1A6064B2D5EB9E67045C60E9320
SHA-256:	E5D91CC3BE84A7CD96D3BF802C784884D6E48D623EC8ED3A431A9A29515C16B4
SHA-512:	B84D772DE482FF99B48B83006885102EF44DEAE04C0EDA7BC78AF8C9AB3A5699FFA2C9ED66B2F40EC0066766CCA75724208445E8BDEB2EE3CB740D980EE163EE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1....._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.wxcShFhZxXM.O/am=B0jRwgiSeAEBAIQcAAAAAEAAAOCwAWXAOXyGDw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax3JsMRB_j3XGRToGaFFZSy2qHwG2A/m=sy3v,sy3w,sy3t,sy28,sy3u,sy5p,pwd_view .https://accounts.google.com/.;...)/.....-.....s.....#..:_..8.R+n./~,.Jh...A..Eo.....JO.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7901112cde0ff08f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	249
Entropy (8bit):	5.6337362096541375
Encrypted:	false
SSDEEP:	6:mqPYGLUxwzlJKvBKIugktgs8TFw81x5RK6t:Pl0BKFgivoFRp
MD5:	C1358AD8C050F0FCAFFBE5911D8EE908
SHA1:	8AA50BB3943165EBA029C3877A97E1E629E99558
SHA-256:	225B799D0E125E79B0C177D7C1B0117816E4BB76F49790A54311E464A1E83277
SHA-512:	EBD7CEE5DF97E3D3B7DD9656593B2810F5B1A82A2B97E53B25FA59CFB19E28ED1F620D082929C5DCC7070EA29B89ABDD18B9AD3329BCC5993C6F0F94054AC51
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u....t0?...._keyhttps://www.youtube-nocookie.com/s/player/31389f53/player_ias.vflset/en_GB/base.js .https://youtube-nocookie.com/....)/.....7.....<.A....(.UV^..f)W..T....~,.Hp.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\799b92ba7b10a353_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.512659886177325
Encrypted:	false
SSDEEP:	6:mOTpXYGLUxwzzLk006gk2ZgdjTtK4e/lhK6t:Fvf06gfZY/0f/N
MD5:	75D14A54DC6117D39FD18A5DCF726219
SHA1:	5C195760AC14F1420918C0DDFF7F7992D136DBB4
SHA-256:	E3A87105CA68E565F4F48EF02E67781BE17DD975CE9C6762B7538A0EDBEFD3AE
SHA-512:	1474235F0AF417ED89D4C085AD738ACFA0EA9C02CFF39A4BAD22836CBEAF531AA50838D57FA8E74EB1A9AA4A84175EB6F6DF44B59735F681DB266B2FD6231CBA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}....Z....._keyhttps://www.youtube-nocookie.com/s/player/31389f53/fetch-polyfill.vflset/fetch-polyfill.js .https://youtube-nocookie.com/u....)/.....8.....%...'.....y#../..%^.7.,...k.A..Eo.....yS.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d5864097a21e950_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	245632
Entropy (8bit):	5.842403933634629
Encrypted:	false
SSDEEP:	3072:1qkHNoIDTq5zcS7VH1Bx+B9DN3BmeoFBJAO3RoSgKIfycNKtPO4:1qE5nyjG9ZBbGBZnZI9NKtPX
MD5:	A0460A03A3B6E3954AF750A7049151E6
SHA1:	9DE50B16D98B36A9E48E44484F2BA05D8EB42A34
SHA-256:	2F0919A9424411BDE8957C69B8665780A65E60E1E83EADBD476578EDE249C735
SHA-512:	52ED376E9EDC056051F6A0120FA92B0823BB91F080D44DC5DFA230C684C3EB8939CAEB2376BFD011F24A1928DEB5F99A493830902A63270A26C995E1E53040B9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....0C3DAA9A9DD7F537C585E92B2E56694BC3D4FB3413771D5DF548B5551922B1F2.....'.B.....O?.....0.O.....8....$.....p...4.....(S.\..`t....L`.....(Q...Stv....default_One GoogleWidgetUi....(S...9.`&.....$L`f.....Rc.....t.....QbB.5....._....Qc&.Ei....window....Qb:.U.....fa....Qb.....Ga....Qb.....Wa....QbN.^....db....Qb.!.....bb....Qb.Kp... ..gb....Qb.M8.....Ab....Qbz.....Eb....Qb..O.....Ib....QbNzb.....fc....Qb.....pc....Qb...>....rc....QbF..A....sc....Qb.k0....wc....QbFAd3....Dc....Qb~..Z....Hc....Qbz.....Ic....Qb..... .Kc....Qb..R.....Nc....Qb.0i|....Qc....Qbz.....ld....Qb..L;....Yc....Qb.....qd....QbnP.....aa....Qb.....rd....Qb26.....sd....Qb~.....wd....QbN..3....zd....Qbr_.....Fd....Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d68fe18908d14d1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	497
Entropy (8bit):	6.1184744090886625
Encrypted:	false
SSDEEP:	6:mqjYGLKd0HjL1vM0olagrBSK/acS7WU51cUcuVgj0bfgrjOhK6ttMz2bbTs7IhIJ:aQ3ZM0olagg9cmbcUNVI0yO7kz2bc30
MD5:	866059963AEEA5D657CDC5F6C6E1A874
SHA1:	FBC221FCA56E19EFE460BE94D38F300D1A431F4D
SHA-256:	A2FCBA53F531429469FDFFC30E2665CEF08883E6C7E6BA12F54FB0402F19C537
SHA-512:	E4CC1BFED8991488F4F88CFB601BF197356E8951AE8E4805CFCA8C125D77CD4726EEB3C388EC1763A140D62DCFF01A569DCD1ED8AC6DDA73D4B0619126A0A2F
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en_GB.wVRNMqnU4o8.es5.O/am=WAAAEA/d=1 /excm=_b,_tp,calloutview/ed=1/dg=0/wt=2/rs=AM-SdHupITiYb3BfjmTemOw__Ed4dad9Bw/m=_b,_tp .https://google.com//f...)/.....c.....1u..q._...4..I.R.*....r....A..Eo .....A..Eo...../f...)/....0C3DAA9A9DD7F537C585E92B2E56694BC3D4FB3413771D5DF548B5551922B1F2...1u..q._...4..I.R.*....r....A..Eo.....Ej.:L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d6ab3bbe008e7cb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	532
Entropy (8bit):	6.095518669158718
Encrypted:	false
SSDEEP:	12:yCq7n/KGhAMyNCoG56rWcCzu2QuUKtnmApPBcqNqcEDR7:BwnRCMECmvV1smA5LU
MD5:	72CC90C542E3AA0C0D5FEF47331D3D6A
SHA1:	DC4343AD8FD0CCA85FA81EC59726F0166E5D8C90
SHA-256:	01A0A1FB0B05B131EDCB43C3D6D8D82F7867D664610B7E80C68AC7CB61F25A1B
SHA-512:	7E8C30B7F673A12AABAEE05EC5E7BCC41937E667F8C4D8530BCCA788744F170EA9675335097C5AF28213B41E1AD2E753507D4F87B87B280FF6B5CA45355B7B6D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....!....._keyhttps://www.gstatic.com/og/_/js/k=og.qtm.en_US.eyZtLN7gU00.O/rt=j/m=q_d,q_sf,q_pc,qmd,qcwid,qapid/exm=qaaw,qabr,qadd,qaid,qalo,qebr, qein,qhaw,qhbr,qhch,qhga,qhid,qhin,qhlo,qhmn,qhpc,qhpr,qhsf,qhtt/d=1/ed=1/rs=AA2YrTvbnfZ7vgSllYOF3f_IHBGeFFy7Mg .https://google.com/z...)/.....52.w..w..a.....}Q.Xx..>...d>T.A..Eo.....u?.....A..Eo.....z...)/.(w..F7A045D81CB11000A0D533C2C5AE1FA0BB7CC81553C48B493DFA59904B9DB5EA.52.w..w..a.....}Q.Xx..>...d>T.A..Eo.....e.wL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\84087b5e6ca28be9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	470
Entropy (8bit):	6.054432599207577
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\84087b5e6ca28be9_0	
SSDEEP:	12:T9LZ0vJ+N6YdwHc5psVMEPHzkjypkx7dTPd2Hgpk:9mv79W0MiH4mmxdwHgm
MD5:	882D8039C37FC9F810E9461F0C43665D
SHA1:	7268493F5FBB3A4EC165B0F62E9C7F123214A2E2
SHA-256:	8A63D86F15694887D34D775B9089F40A23D1DCF2CA7D0FFC2BB8BF592D02FC82
SHA-512:	09799F45819EFC76F75AC140E5BBE0E9A4B5E0148197B1F8FC47F8D6E50AAC9FA7ADFA4A615DAB0F4AE8D171E80147FE4F056215B554EB09EE5E7DD86090AE8F
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.7RphtNcGHDQ.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_-zmYhp_Ir7_CCxM3l-AckMvaI9A/cb=gapi.loaded_0 .https://google.com/.:...)/.....2....."0r`b.....|.8 g`T..R'X....I.A..Eo.....A..Eo.....:...)/.@...3BE8F2724680508B3053930E00FA484635DD9AC4336BAE9AB18998D57E5D3627"0r`b.....|.8 g`T..R'X....I.A..Eo.....{L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\85b7abb2920b83dd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42436
Entropy (8bit):	5.755716089575971
Encrypted:	false
SSDEEP:	768:tyu8W22ifNZ1CKIUMpVgx4WLLDUYt+4+T9AMvgG+dR8WK/1VeCxh1Zxsiy+AlUkW:x2NZIQeg33DxipAMW4LLI
MD5:	70AF88C9C3B788445AF2C378DCD2EA2F
SHA1:	E52C23913BE84B2C244C450FC593F15646B8A0B9
SHA-256:	6F0839139E82A77EE4084F692B98503E848D57F2F34306A7CAD5049C199BFEAB
SHA-512:	5C50C1B5651BED45C19645265DB286B77D1C4301BABFF1FD950D53D05148F3A58AC0DECFCA24F54CC7AAA360D2EEEC5536B7B34302677FDAF4183911D08E27F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....4....N.c..._keyhttps://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en_GB.wVRNMqnU4o8.es5.O/ck=boq-one-google.OneGoogleWidgetUi.JPk-aNkftDA.L.B1.O/am=WAAAEA/d=1/exm=_b,_tp/excm=_b,_tp,calloutview/ed=1/wt=2/rs=AM-SdHuCsQ-hWdOtwxEofge3F3rTWPHdHg/m=byfTOb,lsjVmc,LEikZe .https://google.com/,...)/.....'.B.I(..k..D.R.I~...j..Z.t..z.'.A..Eo.....!$.C.....A..Eo.....'.....O....@...c..R.....(S.\..`t.....L`.....(Q...Stv....default_OneGoogleWidgetUi....(S.....`.=.....L`v....}.Rc.....QbB.5....._.....Qc&.Ei....window....Qb.&/f....Yv...Qbj.....hw....QbZ..Q....Zv....Qbb.P.....aw....Qb..Q.....jw....Qb6ND.....bw....Qb...E....dw....Qb."s.....cw....Qb..$.....gw....Qb:.....ew....Qb.....kw....Qbb.....mw....Qb*.....lw....Qb.M%"....fw....QbbOT.....My....Qb.+.....Ny....Qbz.....Oy....Qb..-.....Py....Qb.]w.....Sy

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8b5d0c63489cc9ed_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	888
Entropy (8bit):	6.069728597362578
Encrypted:	false
SSDEEP:	12:79wwhO8hipgewVOU/UB2g6qVIxB+oSxsjGYsnloHbaBH9xKLtdnmt6PrKNdvp9N:pwwvHdOkmL6kGB+T9nqHbwdxMxNr0b/
MD5:	33422AF6DDEC2DA1470C14F2CE7DCC3F
SHA1:	D6CA7C2E1492A09EFBEE992F712500966A44D54B
SHA-256:	3FC0F3EB1A69E818404B9A88FF5FF20B2BF11146E60DA4178F5F7150DFC992B3
SHA-512:	91B7E684F596E0D0EEB86229453D6C26984AED1A0851446E8EF2A2662A0DF851D76641AD6A649C768107B02AE38122A75CE8D728124F45917B9E5D2829AD5692
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s&....._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.IdentityPoliciesUi.en_GB.WJPKByKq9sg.es5.O/ck=boq-identity.IdentityPoliciesUi.emeApl-K2Wo.L.B1.O/am=FBBA/d=1/exm=A7fCU,BVgquf,COQbmf,EFQ78c,FqLSBc,IZT63,IavLJc,JNoxi,Jis5wf,KG2eXe,KUM7Z,L1AAkb,LEikZe,MdUzUe,MpJwZc,NwH0H,O1Gjze,O6y8ed,OmgaI,PQaYAf,PrPYRd,QIhFr,RMhBfe,Ru0Pgb,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,XVMNvd,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,b7FMof,blwjVc,byfTOb,duFQFc,e5qFLc,fKUV3e,gychg,hTAg0b,hc6Ubd,krBSJd,lPKSwe,lfpdyf,lsjVmc,lwddkf,n73qwf,p8L0ob,pjICDe,pw70Gc,r2V6Pd,s39S4,w9hDv,wmlPKb,ws9Tlc,xQtZb,xUdipf,yDVVkb,yJVP7e,zbML3c/excm=_b,_tp,techcookiesview/ed=1/wt=2/rs=AOaEmlEF3bs_4xHLUd0miI14DLuSumW31g/m=Wt6vjf,_latency,FCpbqb,WhJNk .https://google.com/.[...)/.....$.5.P.*.5.VW...0.g.l8W..3.....A..Eo....._]07.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8e58b43f8513815d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	136168
Entropy (8bit):	5.832356307399121
Encrypted:	false
SSDEEP:	1536:kpeG/Xk+ccph8J8RxwOq5LQqlhYSjb5TkbCFZzmZu+sv1a3WN9LI+Tw2rqInac1:kUGrxw35LQqILb5Q+FZzmZuJaCxI+znR
MD5:	F4246C6B854CA036801DF41865074B97
SHA1:	3308950C4576D8D15CD0045EC30315EE2567B461
SHA-256:	8F21CFC33B7E85C02AE569D42FDCE4F10A850A9D8F670338A213B45D55F76B69

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8e58b43f8513815d_0	
SHA-512:	9BD4C74696D791B7D6CDB43C6FA8540675DCB66A524A66D56AFFC639AFB21621AF60DD16CF7D4A50DB9C28AE7C20E701A3370DB8961CB81E4BC8A3542E75F561
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....0....3BE8F2724680508B3053930E00FA484635DD9AC4336BAE9AB18998D57E5D3627.....'.....O(...x..... .....d.....H..... .....(S.<..`2....L`.....Qbr.=....gapi..Qcn..k....loaded_0.(S....d.`.....L`.....RcR.... .....QbB.5...._..... .....Qc&.Ei....window....Qb.}R.....ja....Qb...b....ka....Qbv.,v....na....Qb..L.....ra....Qb..F.....sa....Qbvba.....ya....QbR.m.....Ha....Qb...Q....Pa....QbB.....Qa....Qb...I....Ia....Qb.z. ....Ma....Qb.=_t....Na....Qb..).....Ra....Qb.....Sa....Qb...H....fb....Qbj.Z.....yb....Qb.M8.....Ab....Qb.....Cb....Qb.....Db....Qb..O.....Ib....Qb:B.s....pb....Qb.e2.....Pb....Qb..[.....Qb....Qb...H....Sb....Qb.. Z....Rb....Qb.$.....Wb....Qb.\m.....hc....Qb~..8....ic....Qb.....jc....QbV&.....kc....Qb.....lc....Qbv.....mc....Qb.9.....nc....Qb.+.....qc....Qb..V .....vc....Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3ce531f12f3367_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	359040
Entropy (8bit):	5.843775507398299
Encrypted:	false
SSDEEP:	3072:OyPjI2kPHHcs2N4V/ROrscMmxdLwZs8VIhyhOVR0O/not8xkdvWjEyh3Lh2raCxK:OyPjT62ZcP9Gs4oYUwKnF0u
MD5:	A5E66CCF97CB7207FA063D82F1043306
SHA1:	209B16A643BFEBBAD02005A5470164F053DF592C
SHA-256:	8DAFF31B2EAD931D5FDEABC3B5D195E66F78EBDF967B46EBD35675938AFFE908
SHA-512:	B0E4D68E311294C0772DE4F687CD094D5A236C954857DED82D6FE53D3F0FE0B195F01AD9A0CB5EE3137A695598D96DEB092044D91E3B92F544779B50AC49C8EA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....7D068FC3F843A086F6714740FF44524677A3ACCE59F961796F20680B3F10027D.....'.~q....O[...@x..IG.n.....l...*.....\!..... .....x.....\..... .....T.....t..... .....(S.I..`..... L`.....Q.`....._F_installCss.....Q.....b.r....KL4X6e{background:#eeeeee;bottom:0;left:0;opacity:0;position:absolute;right:0;top: 0}.TuA45b{opacity:.8}sentinel{}.....(Q...Stv....default_OneGoogleWidgetUi....(S...m.`.....*L`@.....Rc^.....QbB.5...._.....Qc&.Ei....window....Qb...a....tC....Qb.6.n.... vC....QbRE.....wE....Qb.....xE....QbJ3.....sv....Qb.....LB....Qb.....MB....Qb.$.g....NB....Qb..V....Cv....QbN.....Dv....Qb&..v....Ev....Qb.....Fv....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\922dfb03cc343c93_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.457633520718167
Encrypted:	false
SSDEEP:	6:mSYGLKdakWzGuuPRgRt3BpQMom49UtbK6t:OQczJm3G9Y
MD5:	66ED51639DC61C363580A27B6F478863
SHA1:	6045DAF4D0C67DBD4D2DF73E105EE734FDAB36CB
SHA-256:	90909576268C7A0ADB0D3F290D5542365AC4C876F3A67478D6FADC20AEB9450C
SHA-512:	4C906DC807FC7A749279962CD99E46CE7CCD798989EE650CA774E43F27BCE72769CEE65C4F51AB84336F007F4F51E0CEED2A02E62FC7EA95328A48513FA1AA4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...J..+...._keyhttps://www.gstatic.com/external_hosted/modernizr/modernizr.js .https://google.com/...../.....s.....sO.X.s...3].$.S...|_.\+.S..P..A..Eo..... %K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b166c217628efab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.389431966361735
Encrypted:	false
SSDEEP:	6:m9EiVYGLIgNa9NK8aLu0tgwlW3NGVSAfKRK6t:limvk1ykT/W3NBaKr
MD5:	092A8D81300A9A688128E212FE26AF1F
SHA1:	11EAC0DC21DC07B5B147741139D5C0D168DFB8FD
SHA-256:	DB9B32FD7C1F5AEC8CDAA5C81C3C5B2AB991FA0E72EB2BBF4C2B508514A58FC7
SHA-512:	B2C2D865C14CB5DAC60831D7F6B56D46C25F5E6828042241F01AB71C70CE8F163782000E35E559E6AB33248FB32F5C0AF5F0B073176F80D014BF81EA6684562
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b166c217628efab_0	
Preview:	0\r..m.....O....._keyhttps://www.google.com/chrome/static/js/main.v2.min.js .https://google.com/w1.../.....v.....kR.,&.2mhLLfg.&..]..lJI8....A..Eo.....N.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a186a289234292fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	75232
Entropy (8bit):	6.104051237893063
Encrypted:	false
SSDEEP:	1536:gbjGEoDtro7mc1cjwwgxPLI0eXOTnxIyYW4Cp/IaaJ1F9dz+:wjGEOroac1iwwUbTnxEW9pgPJ1F90
MD5:	31FD7EBA198F424A05A0939DD97649E9
SHA1:	E7162912A7750ECC3C0BBC81F878EA67C1F6BE40
SHA-256:	FF697B9A3A2F154DF2B131D877939D3E8723B9798C7A4A2C7C8870896DED1D51
SHA-512:	E509E54C6BE15198AC93A21BD9351257EB28CD5CC579B3A0689EB97713658F61C41DBD32471000EF2AC423BFDFE1F9225DE326E076D166BC38548F776B1FD24
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...I.'Y....BF39F09080E2978284E02D7336E7587ABD0CAF55D5C57F9860390A656CA44C29.....'.y.....O.....$.....<.....`.....L..... .....d.....,.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb...$....n.....Qbv.....q.....Qb.@N.....r.....Qb:$+1....t.....QbF.....v.....Qb.~I^....x.....Qb ..b.....y.....Qb6.8.....z.....QbR N.....A.....Qb..g....B.....Qb...!....C.....Qb..1.....F.....Qb.h$.....E.....Qb.....D.....Qb&O.F....G.....Qb.....H.....Qb..|.....J.....Qb.k.T....I.....QbvLt.....K. ....QbJ.....aa....Qb.....L.....Qb.'+3....N.....Qb:.P.....O.....Qbr.....P.....Qb^.....M.....Qb2.....da....Qbb.V[....ea....Qb...+....Q.....Qb.....S.....Qbvo.....R.....Qb.y.(....ia....Qb.A/@... .U.....Qb.....ha....Qb.r.X....T.....Qb2.....V.....Qb.*|.....W.....Qb.....Z.....QbBG.....Y.....Qb.+.....X.....Qb.=.^....ba....Qb..l....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a5beba0ee4c90e07_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	251
Entropy (8bit):	5.557087690246551
Encrypted:	false
SSDEEP:	6:mgO/XYGLUxwzlJKvBKsuGgkw0gKZffBC8IXd4lFAhK6t:NOnl0BKdGg/0bUhYFA7
MD5:	71ADA905AE5BCA5D5D34202933E9E291
SHA1:	53C41E06E8FA91CEB5B2D96F9E4422E0EAD765C8
SHA-256:	F9C83F58729AD8FC3F7A62FD2E587E010AB365AA9023AB0F63AEEB8EC7EB880E
SHA-512:	C8EAB7CA248D50C56B1C234DE92C9C91636DA7E2216D5BD96CAD500C50D945936008E10358531FD009201CB869E7584AED7E1E8A75581C7BFEB9FECA5C585E 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w....._keyhttps://www.youtube-nocookie.com/s/player/31389f53/player_ias.vflset/en_GB/remote.js .https://youtube-nocookie.com/..../.....1.....uz/..L.d.C .".V...\.XA...4.....A..Eo.....`Q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a67ca6be6ceabe7d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.826460915089713
Encrypted:	false
SSDEEP:	6:mYGYGLKdGMwjM71pwXpR3M71ipJWXs+ZQKWvpsUikvimuNHFg2G09w6jNYhHK6t:fj9wwhO8hipGsEnmHikvi7lFHG05BeJ
MD5:	7F50B2DF4BCACCE52E7E1EF151D22F4C
SHA1:	ECA236153635D98A6728FF19843AD6E166A116DF
SHA-256:	753BCD2B94CA5BF509C5B8C908D7FDD9B57220A5E7DBA17A6F9AA5F9915FC484
SHA-512:	DC092595B2C2674767BD1E126334465D8A93B2FA11DE9088CBCCB5EA3FBC687A8936549302EA0495548E182B1C5512481C7DE4E564B2501BEBAE4904E0AC455
Malicious:	false
Reputation:	low
Preview:	0\r..m.....2...2L.p...._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.IdentityPoliciesUi.en_GB.WJPKByKq9sg.es5.O/ck=boq-identity.IdentityPoliciesUi.emeApl-K2Wo.L.B1.O/am=FBBA/d=1/exm=_b,_tp/excm=_b,_tp,techcookiesview/ed=1/wt=2/rs=AOaEmlEF3bs_4xHLUd0miI14DLuSumW31g/m=byfTOb,lsjVmc,LEikZe .https://google.com/...../.....9p....Dn.M.s..)\...MNi..P.,Q.A..Eo.....143".....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7389ced353d126f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	343

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7389ced353d126f_0	
Entropy (8bit):	5.754176823223501
Encrypted:	false
SSDEEP:	6:mgYpEWuVnfj05bX3XoM5nRgsUxE6CdHcVxG0uutOgnFs47rKK6t:MH0nwbXoM5ZgE6CFSG0zc1z
MD5:	62D2484F09299AC7ED3BD9A367DBCC54
SHA1:	157C977B6E2CA107F400DEA9F048FB304FAD8A9B
SHA-256:	11AE3A7D30510DB7CD24AE9C73A41D1A498AE31396C6C9B802B268E11EBA9B1E
SHA-512:	226741CAC16388029213C935173B0B9FC7755EDBAACE0B01661C2AE4E7B3EFB217CE1EB2AE9E4ACA69993F869009A158D2D928B3394A490B467347C8C75E21C C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^....._keyhttps://apis.google.com/_/scs/apps-static/_/js/k=oz.gapi.en_GB.tmPnhifxyTQ.O/m=googleapis_proxy/rt=j/sv=1/d=1/ed=1/am=AQ/rs=AGLTcCNw oIQ3FEHTItd0ffFEpbwP-CV1_g/cb=gapi.loaded_0?le=ili,ipu .https://google.com/_`...)/.....9.....].Z*M...M\r.m.N.x.....3.I..m..A..Eo.....:)s/.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7fba63d58298f37_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.522137279645753
Encrypted:	false
SSDEEP:	3:m+ltulldA8RzYrSL1cdMyw0YcWGa8Md2vEdLSFvDp2KZlatEH/lHCBfojpFRH9Aa:mVPYGLKdakMyE+ZE0gBNxzn0ZK6t
MD5:	3C409A8896F05193FDB85AE6D157D108
SHA1:	1149EF8EC834901E7F0FC644DCD44F052FCAF8D4
SHA-256:	B09C8479D42B6BCFB9595718AB0D450CEFB04996ADEB1ADE7A7C27A33FC80B97
SHA-512:	C0DEC785E74F5B1FDA1531F5FAE8105C7C448999959FB0CB08EDEE9ACAC0ADC28CBDDE8319A59BDFC38B84AECDC27E03FC5212D706EB24F00286863D944A 33C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a...<..C...._keyhttps://www.gstatic.com/external_hosted/scrollmagic/ScrollMagic.min.js .https://about.google/._...)/.....$3.....{}.U6o.....1;X.i..;.&.A..Eo..... $.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ac3494dff495a4ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451
Entropy (8bit):	6.035990555305575
Encrypted:	false
SSDEEP:	12:UTEm80vb01iRlfMMZXe8vAeXcLp+l0A/zUN:6fnvbqZMZXI140A/zUN
MD5:	838893683B23871E39920C434110119F
SHA1:	69ABF2E470D91760FB2F8DB2D6A45C8210C047FE
SHA-256:	368A33A07DE78A36354FA69C83795510FF901CB1B3916CAFC5F52484026DC68F
SHA-512:	D71C23B88736ACBAF2849F10E6BCC0B2F3DA44AA9978D8E604538F2923839965C3D7930E4F549C62EBABD98796CAF1E2BDAE8FC99D24F97B9C9822E8E20B76 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....5ns...._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.wxcShFhZxXM.O/am=B0jRwgiSeAEBAIQcAAAAAEAAAOCwAWXAOXy GDw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax3JsMRB_j3XGRToGaFFZSy2qHwG2A/m=n73qwf,MpJwZc,NpD4ec,SF3gsd,O8k1Cd,YLQSd,SWGa5d,o02Jie,rHjpXd,pB6 Zqd,QLpTOd,otPmVb,rlNAl .https://accounts.google.com/...../.....h.....sQK..r....6.:+S..b_e.....(..c...A..Eo.....x.*.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae8d89bf4087b90b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.502580216666142
Encrypted:	false
SSDEEP:	6:mWYIZeR0WdWyIPdKE3OVZjug/lDiZ4JGaLH5tbK6t:teR037Pdd3WjuEFiZSGop
MD5:	BDD66B630FF8CF17179DFEF524C649A4
SHA1:	B3A2F82D10EC8172E2C995C96A247659848CB1AB
SHA-256:	6D653ACADEC312E3839C2EE41BD11E1FD9AE1E85386DA27842A9DD274946C8B7
SHA-512:	5C8A0D7F8E6FD6AFB26CBC674806F8640090A7922D15385C5766A86D286EB663CD411B883A407E24C1E2678785BC8DD5C2458A5130A959BAFF7AC05F4AAE707
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae8d89bf4087b90b_0	
Preview:	0\r..m.....\...+}.w...._keyhttps://about.google/assets-products/js/main.min.js?cache=59c1266 .https://about.google/.Y...)/.....5.....!FM..w....wi..d.u...X.t.|.1N..A..Eo .....~3m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b035bfc649683bd5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	399
Entropy (8bit):	6.018451401453329
Encrypted:	false
SSDEEP:	12:q0Em80vb01WRlfMMZXrrKbQqnMg+qtaPRipu:q0fnvbqtMZX/jgDoPcpu
MD5:	FDB77B8836A9F8D51807EAF16159D95A
SHA1:	9AF9730525AA7B6B9DB9E2BF43A5C16EDF1C1580
SHA-256:	97A939E284F18E7B1B8CE4BB555E3A46697B5A61C5DD9718733165E10A29129C
SHA-512:	234F8DFFDC4D3ACECA8D4418595EC72A259D86E4F8D4CBBE4335379053AE667CF68B7712A871C8DFCF17EAF8A2CD9249EDC475BA2B4CF2CD5A29029AFF342ED
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.wxcShFhZxXM.O/am=B0jRwgiSeAEBAIQcAAAAAAAAAOCwAWXAOXyGDw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax1gbLtMuNhkPy_WFDM6EbCrSJwQ2A/m=i5H9N,sy30,sy38,PHUIyb,qNG0Fc,ywOR5c .https://accounts.google.com/.D...)/.....QF.....$..e..!..?..=E...;M.O.#u..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b110e5c2b4ae8737_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	5.501918742060558
Encrypted:	false
SSDEEP:	6:myWYGLUxwzlJKvBKAIESgkCwgRisroLa+4dhK6t:lyl0BKTgrwU5oeN
MD5:	9EBD74CB208D9BEAD26183DDE654C1EC
SHA1:	3762F4320DEEE68947222F0E5D753A3F28B1AE1A
SHA-256:	2AB3BA85FE3FA10B6CA0E1F566A9A3C6C00392AB5E98E813AA0CDE9ED03CFEED
SHA-512:	2775712B13DFE3B2E5AC77893056170540EE74A5096C8F42BB20D08E4B433D2F489C4FC2E8961A82939E5714DD9867FD01BD84AA99FC69490FDE5299B8B5E38D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v....o....._keyhttps://www.youtube-nocookie.com/s/player/31389f53/player_ias.vflset/en_GB/embed.js .https://youtube-nocookie.com/...../.....4.....+t`..U./.....n...{.f..v+..A..Eo.....1.e.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b2cbac092fd30741_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.500340671926843
Encrypted:	false
SSDEEP:	6:mDXXYGLUxGBzxI2c7MNuu2gMDma4JPprEZK6t:ewGB22clJ2VDc1pM
MD5:	6F833ABBE80ECD21AB9A29CE61D2F5AD
SHA1:	61B0610AEE80C9EF864296E689360D15B60E24EA
SHA-256:	B4764A215515BBDA240A7BCB7D69B72A6AB3B49CB0614698FBA9A2C9F51EA16E
SHA-512:	DB7820C7C11FA438C9BFACACD13D3BBFF8AE609F59FEEBE5B45414767712424906EDE9E8B3EA17A0F0A034399DD440E0B342160D45BA5767EDEC9F0114C96F57
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://www.youtube.com/s/player/31389f53/www-widgetapi.vflset/www-widgetapi.js .https://google.com/.-...)/.....oj&..$.....q.=A..,8/.Z...+.....A..Eo.....n.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b36a79757cb1046c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	401
Entropy (8bit):	5.959921377840279
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b36a79757cb1046c_0	
SSDEEP:	6:mHiYvEdCN8uVvUCll2x1ydRlfM2NZXmADrwjTXQpvWqxXSJc1VDw+1gBl6hCn/HD:2BEm80vb01WRlfMMZXrrKgpOmX2+10R
MD5:	9415CE881326BADA8091AD7A4691F490
SHA1:	76C5A7D28B4EF24F14C90D33D561620E8DAFA24A
SHA-256:	C13BBACFC4A8DA825790CF0E988FE799637B6BDCE3B74FF6B04A029C044C7220
SHA-512:	3E1828DD404F11FD9ECD1F3829B42DA2C9FC75C7D06D020B90DD12DEE068FD14EA3B2C207B2C1FB85602FA722508DDBE3D1CEAD88CD74CA2B4B1E9C846E56E8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?../...._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.wxcShFhZxXM.O/am=B0jRwgiSeAEBAIQcAAAAAAAAAOCwAWXAOXyGDw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax1gbLtMuNhkPy_WFDM6EbCrSJwQ2A/m=sy3v,sy3w,sy3t,sy28,sy3u,sy5p,pwd_view .https://accounts.google.com/...../.....E.....[.Zk,.]c.'n..j.....*.^..L.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b37008cdefa8ac53_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	261
Entropy (8bit):	5.616314193616313
Encrypted:	false
SSDEEP:	6:m8YGLUxwzxRj4PY0c71j4GgkzKFggEMEK5KC6ARe/ZK6t:9PsPjcRsGgQuvEFQKzrr
MD5:	D6F3A8A20FE98DED3831A8BDF2CAF88A
SHA1:	01D7F9FCC8362EBEA17D31A17EE9DBF550EB20CA
SHA-256:	1D94E4B00D31B68D6BEA220C8EA2916B9C5190F0D1737D40A2E32824DFF0E2A5
SHA-512:	6BD4784FBA80641EBB7A251900753DBEBC931568F86D619AF6E5ED1198D46A7EA5767D99E212A0F9DCA7273CC4C124FB59F55D40233CD40D4766E093F5694B7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....4...._keyhttps://www.youtube-nocookie.com/s/player/31389f53/www-embed-player.vflset/www-embed-player.js .https://youtube-nocookie.com/..../.....9.....$!.....8_..L..*.g{}.....A..Eo.....{.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b8c3df9b5168fca9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.458431774216459
Encrypted:	false
SSDEEP:	6:mq6EYGLKdakMGrVWJLLPwZblHg+tuO7nM3/9bK6t:v6hQEQLLPKblH/Ynj
MD5:	DE32889868E894F1B3F31451E97127E9
SHA1:	07D919599AB6E2C333CC36034A6759EF16EEF933
SHA-256:	10420F9EEC1A7C8C253DAFCC46582062AAFEFC8607FF7ABE138807F5C138CC8B
SHA-512:	ED8EA27046124C43BD40BD61D39484BBD1349996B1FF9126CA9C65E599B8066ACBC96E487B0918100ADB44D52EA81EC30A66B14AB79484A2CD928DE14084B63F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....|...._keyhttps://www.gstatic.com/external_hosted/picturefill/picturefill.min.js .https://about.google/./s..)/.....I.3.^a:.....L.....A..Eo.....y.c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\be96a6ccc9ef92b1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42441
Entropy (8bit):	5.7526763732578825
Encrypted:	false
SSDEEP:	768:fl8WGRSKn4yZfMplg2ge2n4+SiN+k5T7M9IRWG+dR8WK/1VeCxh1Zxsiy+oBUipq:tINtutJn+JBnMck4oXS
MD5:	8A6B82B5ABDFA3CF15A5F7C544D4A576
SHA1:	23FE4DDA1107F4B287878F0FDC1E24E73468C43B
SHA-256:	ADFCE5EA4B4CFF2B7523401D3172699E11F1670A21C225ACED68DC148F3C9980
SHA-512:	E6322F4F274FD128CF0BCD24AE43F09D6D10FFF53493E4B50BEF551019ED04AE614455C786E3D0B570BFAE90D4E8C74F564688A11D9EC291FF74BB01A00EB20B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\be96a6ccc9ef92b1_0	
Preview:	0\r..m.....1....Z....._keyhttps://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en.iRny_Wkefus.es5.O/ck=boq-one-google.OneGoogleWidgetUi.JPk-aNkftDA.L.B1.O/am=WAAAEA/d=1/exm=_b,_tp/excm=_b,_tp,calloutview/ed=1/wt=2/rs=AM-SdHuqGlTqF50PcbuHE8DjFQoN0CMcIw/m=byfTOb,lsjVmc,LEikZe .https://google.com/U.@..)/.....!m.h.....h .W..AR..W}...0m.A..Eo.....x.....A..Eo.....'.....O....H.....p.....(S.\..`t.....L`.....(Q.....default_OneGoogleWidgetUi....(S.....`.=.....L`x....}.Rc.....Qbf..k...._.....Qc..{.....window....Qb...(....Yv....Qb.....hw....Qb..w$....Zv....Qb.....aw....Qb..o7....jw....Qb.._.....bw....Qb:.....dw....Qb"Wm.....cw....Qbj].....gw....Qbv.....ew....Qb..4.....kw....Qb~U.....mw....Qb>..C....lw....Qb..8.....fw....Qbn.....My....QbJ_.P....Ny....QbFc.....Oy....Qb.....Py....Qb.S.....Sy...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c20153606dcb180a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.387677772370001
Encrypted:	false
SSDEEP:	3:m+l3zdA8RzYrSL1cdqExKoisDp2KZlLrtoR/lHCeWlJhXjOdSO3krZZmMcUllpK+:mOYGLKdqEHZcRgLsSu4ZYdUhK6t
MD5:	9408570B03734DA2F3984B580D204D26
SHA1:	5076614A0425340DB50EA755C04D1CD19C4D6799
SHA-256:	9554347759C0D777E78CE05A1FAEF7D8AD4F1BE81E77FFFA3BBAF5ECA6B4938E
SHA-512:	A24E5FAF1DED3E074885D039E6D237BCD7D726C50531D168119D130926354C92AA6AB256EEFC99E6922F2422200D7A91D65AEC73521C03254DA05B815E3DCB2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C...$.n...._keyhttps://www.gstatic.com/charts/loader.js .https://about.google/...../.....3.....2'.va....4..,.....y+.U....,(..A..Eo.....m.y=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c5ebfc220da3bb5b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	5.722377367814424
Encrypted:	false
SSDEEP:	6:mJYGLIBUkpoyN1vFgk3i0gIE/ILZnTTOhK6t:NBXoE1dgilr+ILBm
MD5:	3F6B7F1D2EBDC44A33E1D686D5B6AF3A
SHA1:	D75264E6F324BA7556E80FF28EE241C7F57BCAB1
SHA-256:	58E7B9051611544B8B2A043725F90DF1A13225782431EE975266843AAA3CEFC8
SHA-512:	216D17B0DE922DD212D51359627929BCFAEF07D0955F4F079DCB493CAAC415E9A11BB33265433A0930C81FBD7317D1F3BAB525DDB1EECD0F87DCAD77455A55
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n...K7.H...._keyhttps://www.google.com/js/th/vn5A_TjKRXDA00Zeyc5KbWJpUGORQjAB309y4DKYpfM.js .https://youtube-nocookie.com/....)/...../.....u.`...5..:.q...._]5.B..Z.A..Eo.....v.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\caab0a9ff213e86d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.496871094261428
Encrypted:	false
SSDEEP:	6:mmGXYSHT8NBDIzZSHKtgjtEmt2o4RH7DK6t:G1z8NBDI1SqtUtaHp
MD5:	8C6177F417E80A72DFA6EBD9764C365B
SHA1:	411EA3520B14F5F905B1BB2E5304C2FB6271D4AF
SHA-256:	70A0EEFDDB403D8EE3AB0FABBD3468171190FAD76F23D4EBE86466CDAB6D662D
SHA-512:	1F9AC40423C345321C65B3FB839CC8EF3F67592738E8DEB031CEC1ACB76AD4514F6E3CCD6681921697BF2B03BC32D2BFEFDC2E5881BE6B50E3EC50FF09AF6A8B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...2....._keyhttps://ajax.googleapis.com/ajax/libs/angularjs/1.6.6/angular-touch.min.js .https://about.google/...../.....3.....I...C~#Z...y.>.|$.....6.j.A..Eo.....*Z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cc687809cee3523e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	494

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cc687809cee3523e_0	
Entropy (8bit):	6.134305274526626
Encrypted:	false
SSDEEP:	6:mWYGLKd0HjL1vM0/MQQBlagrBSK/acSD60cumtglXRqJhK6tMok9dZ/WNE/c5ZFm:WQ3ZM0/8Blagg9cE60NmtgXsqok9JH
MD5:	0B129F112AFC8A8A31EEB5A29BD8208E
SHA1:	FE79631838DC2467F9C3835897C517A56A6C0CAF
SHA-256:	07D322DBC9CC981FCFDAE1223B7B0DCD054160A9F8D7CD6A25ACFD32326DF7DD
SHA-512:	7A6C92E0DEA1D0BACBCD38BB291E85A28572B3662BDA91F8C2C26C9AA49EA6525977A4E4D144CB4E7B94145F61D4E0108E0F69DAE0B47680D4754F1C7B0478AF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...._keyhttps://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en.iRny_Wkefus.es5.O/am=WAAAEA/d=1/excm=_b,_tp,calloutview/ed=1/dg=0/wt=2/rs=AM-SdHuPKtODhSaGxuTNnaiNK93tgINM2g/m=_b,_tp .https://google.com/jT>..)/.....M.....%.eq-X.....qz.....A..Eo.....i..=.....A..Eo.....jT>..)/....E827AF92C97F4D8E31BA101A90495E29B9C03BA1BF6F1AA3C0D39906A53D47B5M.....%.eq-X.....qz.....A..Eo.....''QEL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d49728db3a9d1e14_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	831
Entropy (8bit):	6.069192365663224
Encrypted:	false
SSDEEP:	12:/9wwhO8hip9XnmLSdGPMYvCVHZpqz4scboN84UJgmAcTgrwM4prM7Cl2F:1wwv0kaTtZpqzibQ8hJpAugrwFpwOl+
MD5:	CD6A2E79F4E8001C73D34EC87BCE04F5
SHA1:	33F73E51474D78CF73377FA3BDCFE7BCF0569CC7
SHA-256:	592EC96A0A046469BF53E26EB5E0B4767E124994FEDC2C8D79691B341AAB6353
SHA-512:	AD6BBD1CD3FD76CADA679A626D71C82D5422FC3E3C2B207BE30F59442F5884681CECB0E859CF4AE479A7E69D18D683ED20D18B0BA1B54552FEAA76B7895282C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....+....._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.IdentityPoliciesUi.en_GB.WJPKByKq9sg.es5.O/ck=boq-identity.IdentityPoliciesUi.emeApl-K2Wo.L.B1.O/am=FBBA/d=1/exm=LEikZe,_b,_tp,byfTOb,lsjVmc/excm=_b,_tp,techcookiesview/ed=1/wt=2/rs=AOaEmlEF3bs_4xHLUd0miI14DLuSumW31g/m=n73qwf,ws9Tlc,IZT63,e5qFLc,UUJqVe,O1Gjze,xUdipf,blwjVc,fKUV3e,aurFic,COQbmf,U0aPgd,ZwDk9d,V3dDOb,r2V6Pd,p8L0ob,O6y8ed,PrPYRd,MpJwZc,NwH0H,Omgal,hTAg0b,XVMNvd,L1AAkb,KUM7Z,lfpdyf,duFQFc,s39S4,Jis5wf,lwddkf,gychg,w9hDv,RMhBfe,SdcwHb,aW3pY,PQaYAf,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,Ru0Pgb,xQtZb,lPKSwe,MdUzUe,JNoxi,b7FMof,yDVVkb,QIhFr,KG2eXe,hc6Ubd,SpsfSb,VwDzFe,zbML3c,A7fCU,Uas9Hd,BVgquf,yJVP7e,pjICDe .https://google.com/.o...)/.....s.....Y.A6.|.Mh..+.c.]....'f.y4.xU...A..Eo.....a.Q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d5c2481f810214e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.424127761750498
Encrypted:	false
SSDEEP:	6:msIEYIZeR0WdWyS9KSgRNZfFgVpMBQlvzK43EK6t:kieR03p9wvtQYdvzTW
MD5:	DD3AF569151AA46376FA7FEE93922007
SHA1:	5E8164AB422745D6789866ADDB99F0B26AED5ECB
SHA-256:	07C86CA5E551EA07F4EAAAE0727EDF4FC56EF015E481225B4F4678D5B1C6B557
SHA-512:	F3555F842FCE4A733F94B50A887024E389D1FAE5EA15FFF346D5301F4DB3EB0DD560B0EEC827317EE81E41A51DECF68500E6998A87F647D80294B136F7C41E5(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^.....\...._keyhttps://about.google/assets-products/js/detect.min.js?cache=c84f19a .https://about.google/.W...)/.....06.....o.%.....8..O..~cr.c,f...6.K.-:..A..Eo.....~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d73906a901c7bc7b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.525922175677482
Encrypted:	false
SSDEEP:	3:m+l1PwOA8RzYrSL1cdMyw0YcCWbXUd6gUJ8aWFvDp2KZl96leH/lHCFg/JNacH89:mYPFYGLKdaY0W/wZ6kgFgDaOxnrWK6t
MD5:	0493A869E301CDE3406A281825CE959E
SHA1:	FFE538D3F5F77E2B508F5E3E9BA249F292F7D322
SHA-256:	ACB3BF2805C07182FF53EDEF4AC3659428B80496B10CE7C5C7AD1D86FA13AEEB
SHA-512:	BB445170FCB1E211E79DBF9AA7A5DA5E57E2762369A06C73416BB5473EC8082C530EE70931DCB8947EE261AD26FC5F5030BA28E7F92D894126C171A1556DB29

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d73906a901c7bc7b_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....._keyhttps://www.gstatic.com/external_hosted/gsap/v1_18_0/TweenMax.min.js .https://about.google/._...)/..... 3.....,/V.B...".MQ...X..E.....cX..A ..Eo.....6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dbdcbf2257d3331b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14798
Entropy (8bit):	6.014077378323208
Encrypted:	false
SSDEEP:	192:EQE54QUUhjKiVD2Jv3kRVSu+mi3134Opmn8bpQMfMmp+QNCNDMF7odXkdUupUM/W:EQeUil9URQDm7SflpHEWSM/W
MD5:	C46DD3161A1D342A0EB59511FEF47164
SHA1:	FEE85736471CE430B062A25C0AC01D31D7F1A8A5
SHA-256:	9ACF81591D91AAFD7C4DCA179725105F2CF52E8C5FCE796AE8A676A258069D51
SHA-512:	FA9A8DDA28066A1141AFBD33893A88B575A8A733EC4F5FA9BD4A59DC71DEFF0735A303D953F47E318CA107E7661BEF2E210F845DD04CE81DFC6460480B7A78 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....ff.%...._keyhttps://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en_GB.wVRNMqnU4o8.es5.O/ck=boq-one-go ogle.OneGoogleWidgetUi.JPk-aNkftDA.L.B1.O/am=WAAAEA/d=1/exm=A7fCU,BVgquf,COQbmf,EFQ78c,GkRiKb,IZT63,JNoxi,KG2eXe,KUM7Z,L1AAkb,LEikZe,MI6k7c, MdUzUe,MpJwZc,NwH0H,O1Gjze,O6y8ed,OmgaI,PQaYAf,PrPYRd,QIhFr,RMhBfe,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,XVMNvd, ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,blwjVc,byfTOb,e5qFLc,fKUV3e,gychg,hKSk3e,hc6Ubd,hnN99e,kjKdXe,lPKSwe,lazG7b,lfpdyf,lsPsHb,lsjVmc,lwddkf,ml3LFb,mdR7q, n73qwf,pjICDe,pw70Gc,s39S4,w9hDv,ws9Tlc,xQtZb,xUdipf,yDVVkb,yYB61,zbML3c/excm=_b,_tp,calloutview/ed=1/wt=2/rs=AM-SdHuCsQ-hWdOtwxEofge3F3rTWP HdHg/m=Wt6vjf,_latency,FCpbqb,WhJNk .https://google.com/...../.....&./...?M.GGeO..G4a....7.*X...D.A..Eo.....JHu\.....A..Eo.....'.7.....O.....5. .#..S.....(S.\..`t.....L`.....(Q...Stv....default_On

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\df775ea48d3e6f57_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	190896
Entropy (8bit):	5.9455920431569895
Encrypted:	false
SSDEEP:	3072:sO0aXB3DtatdpWicppwfyY9OHHNNXtv2DKPmzCuNzD1PWTUv:sOR3Dtm6p/htN9vRuOoz5PR
MD5:	099AABE60DE00913D1C3A8D6A63E3F1B
SHA1:	0DC71E42649E9E9D9C91591AD8C25E961A0ADE05
SHA-256:	9CAB776D7B2B7B333F94BB6ADC97E365C8D02FD6FCDE7A6856A2FAE71524DEE6
SHA-512:	AC759E6BD92D514D5A3C0166FF14009D69527791C6E3C30F685C9DE29327144E6E15503803BDE2BEA7E5DA63F23EF2B1B4E0A481B7AE8647C2AB25C4394C8FF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...B.7.....3C17A8C519142CB0AF7EBCC330AB0612F4784B61B6232FC81B1B5E65768E186D.....'..C....O5..... .....0..... ...$.....l...x.....l.....(S.<..`2.....L`.....Qbr.=.....gapi..Qcz*.....loaded_1.(S....`v+.....!.L`.. .....Rc.....QbB.5....._.....Qc&.Ei....window.....Qb.....vn....Qb.....wn....Qb.Y`=....En....Qb.....Fn....Qb..m.....Gn....Qb.t+.....Hn....Qb.#.....In....Qb.g.....Jn....Qb.\.(.. ..Kn....Qb...a....On....QbB.....Pn....Qb...s....Vn....Qbf..^....Wn....Qb^.....Xn....Qb.u.....Yn....Qb^R}y....Zn....Qb.....$n....Qb.<.....bo....Qb..t.....ao....Qb..ec....io....Qb..... ..go....Qb.jb.....ho....Qb~}.....jo....Qb.....ko....Qb~..~....lo....Qb.!.\....mo....QbN..#....no....Qb.(.....oo....QbnE\u....po....QbF.l.....qo....Qb.Y.....uo....Qbz..D....wo....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets
UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 26, 2021 07:50:38.516206026 CEST	192.168.2.3	8.8.8.8	0xdbad	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:38.519994020 CEST	192.168.2.3	8.8.8.8	0xce2e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:38.521984100 CEST	192.168.2.3	8.8.8.8	0xbb7b	Standard query (0)	gmail.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:38.821620941 CEST	192.168.2.3	8.8.8.8	0xc950	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:39.009721041 CEST	192.168.2.3	8.8.8.8	0x2f58	Standard query (0)	mail.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:40.908113003 CEST	192.168.2.3	8.8.8.8	0xb1a4	Standard query (0)	accounts.youtube.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:41.137861967 CEST	192.168.2.3	8.8.8.8	0x2c3c	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:44.878304958 CEST	192.168.2.3	8.8.8.8	0x1d6e	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:45.561065912 CEST	192.168.2.3	8.8.8.8	0x1bea	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:50.237200022 CEST	192.168.2.3	8.8.8.8	0xb510	Standard query (0)	support.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:50.683327913 CEST	192.168.2.3	8.8.8.8	0x172b	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:51.655107021 CEST	192.168.2.3	8.8.8.8	0x773	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:51.685069084 CEST	192.168.2.3	8.8.8.8	0x2ef1	Standard query (0)	ogs.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:52.003148079 CEST	192.168.2.3	8.8.8.8	0x71e4	Standard query (0)	scone-pa.clients6.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:55.678987980 CEST	192.168.2.3	8.8.8.8	0xc731	Standard query (0)	lh4.ggpht.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.056642056 CEST	192.168.2.3	8.8.8.8	0xbd7d	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:06.219965935 CEST	192.168.2.3	8.8.8.8	0xc91a	Standard query (0)	policies.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:06.842032909 CEST	192.168.2.3	8.8.8.8	0xcc4	Standard query (0)	www.youtube-nocookie.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.588038921 CEST	192.168.2.3	8.8.8.8	0xd99	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.589960098 CEST	192.168.2.3	8.8.8.8	0x6764	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.596381903 CEST	192.168.2.3	8.8.8.8	0x8173	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:20.197707891 CEST	192.168.2.3	8.8.8.8	0x9399	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:20.378217936 CEST	192.168.2.3	8.8.8.8	0x8c65	Standard query (0)	about.google	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:23.923405886 CEST	192.168.2.3	8.8.8.8	0x69da	Standard query (0)	www.blog.google	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:26.308671951 CEST	192.168.2.3	8.8.8.8	0x9dd8	Standard query (0)	about.google	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:26.325198889 CEST	192.168.2.3	8.8.8.8	0x80eb	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:38.966625929 CEST	192.168.2.3	8.8.8.8	0x9962	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.129636049 CEST	192.168.2.3	8.8.8.8	0x1fce	Standard query (0)	csp.withgoogle.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.131875038 CEST	192.168.2.3	8.8.8.8	0x175e	Standard query (0)	tools.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.136113882 CEST	192.168.2.3	8.8.8.8	0xa6b0	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.137986898 CEST	192.168.2.3	8.8.8.8	0xb74a	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.191551924 CEST	192.168.2.3	8.8.8.8	0x10c5	Standard query (0)	2542116.fls.doubleclick.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 26, 2021 07:51:39.257846117 CEST	192.168.2.3	8.8.8.8	0x26c5	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.808651924 CEST	192.168.2.3	8.8.8.8	0x3b5d	Standard query (0)	s.ytimg.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:40.282192945 CEST	192.168.2.3	8.8.8.8	0x175e	Standard query (0)	tools.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:41.111269951 CEST	192.168.2.3	8.8.8.8	0x9fd2	Standard query (0)	adservice.google.co.uk	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:41.288043976 CEST	192.168.2.3	8.8.8.8	0x175e	Standard query (0)	tools.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:43.339092970 CEST	192.168.2.3	8.8.8.8	0x175e	Standard query (0)	tools.google.com	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:47.388530016 CEST	192.168.2.3	8.8.8.8	0x175e	Standard query (0)	tools.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 26, 2021 07:50:38.548464060 CEST	8.8.8.8	192.168.2.3	0xdbad	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:50:38.548464060 CEST	8.8.8.8	192.168.2.3	0xdbad	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:38.562093019 CEST	8.8.8.8	192.168.2.3	0xce2e	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:38.565939903 CEST	8.8.8.8	192.168.2.3	0xbb7b	No error (0)	gmail.com		172.217.168.69	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:38.853876114 CEST	8.8.8.8	192.168.2.3	0xc950	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:39.051948071 CEST	8.8.8.8	192.168.2.3	0x2f58	No error (0)	mail.google.com	googlemail.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:50:39.051948071 CEST	8.8.8.8	192.168.2.3	0x2f58	No error (0)	googlemail.l.google.com		216.58.215.229	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:40.162934065 CEST	8.8.8.8	192.168.2.3	0x8e7d	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:40.951283932 CEST	8.8.8.8	192.168.2.3	0xb1a4	No error (0)	accounts.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:50:40.951283932 CEST	8.8.8.8	192.168.2.3	0xb1a4	No error (0)	www3.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:41.165525913 CEST	8.8.8.8	192.168.2.3	0x2c3c	No error (0)	play.google.com		172.217.168.78	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:44.905705929 CEST	8.8.8.8	192.168.2.3	0x1d6e	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:50:44.905705929 CEST	8.8.8.8	192.168.2.3	0x1d6e	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:45.596221924 CEST	8.8.8.8	192.168.2.3	0x1bea	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:50.280122042 CEST	8.8.8.8	192.168.2.3	0xb510	No error (0)	support.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:50.568604946 CEST	8.8.8.8	192.168.2.3	0xe490	No error (0)	www-google-analytics.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:50.715337992 CEST	8.8.8.8	192.168.2.3	0x172b	No error (0)	lh3.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:50:50.715337992 CEST	8.8.8.8	192.168.2.3	0x172b	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:51.695787907 CEST	8.8.8.8	192.168.2.3	0x773	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 26, 2021 07:50:51.695787907 CEST	8.8.8.8	192.168.2.3	0x773	No error (0)	plus.l.google.com		172.217.168.78	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:51.720336914 CEST	8.8.8.8	192.168.2.3	0x2ef1	No error (0)	ogs.google.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:50:51.720336914 CEST	8.8.8.8	192.168.2.3	0x2ef1	No error (0)	www3.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:52.043328047 CEST	8.8.8.8	192.168.2.3	0x71e4	No error (0)	scone-pa.clients6.google.com		172.217.168.10	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:55.719177961 CEST	8.8.8.8	192.168.2.3	0xc731	No error (0)	lh4.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:50:55.719177961 CEST	8.8.8.8	192.168.2.3	0xc731	No error (0)	photos-ugc.l.googleusercontent.com		172.217.168.1	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.186.142	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.186.174	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.184.206	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.184.238	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		172.217.18.110	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		172.217.23.110	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		216.58.212.142	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.185.78	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.185.110	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.185.174	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.185.206	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.185.238	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		142.250.181.238	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		172.217.16.142	A (IP address)	IN (0x0001)
Aug 26, 2021 07:50:56.083241940 CEST	8.8.8.8	192.168.2.3	0xbd7d	No error (0)	youtube-ui.l.google.com		216.58.212.174	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:06.260361910 CEST	8.8.8.8	192.168.2.3	0xc91a	No error (0)	policies.google.com		172.217.168.46	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:06.885406017 CEST	8.8.8.8	192.168.2.3	0xcc4	No error (0)	www.youtube-nocookie.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:06.885406017 CEST	8.8.8.8	192.168.2.3	0xcc4	No error (0)	youtube-ui.l.google.com		172.217.168.46	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 26, 2021 07:51:06.885406017 CEST	8.8.8.8	192.168.2.3	0xcc4	No error (0)	youtube-ui.l.google.com		172.217.168.78	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:06.885406017 CEST	8.8.8.8	192.168.2.3	0xcc4	No error (0)	youtube-ui.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:06.885406017 CEST	8.8.8.8	192.168.2.3	0xcc4	No error (0)	youtube-ui.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:06.885406017 CEST	8.8.8.8	192.168.2.3	0xcc4	No error (0)	youtube-ui.l.google.com		172.217.168.14	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.625021935 CEST	8.8.8.8	192.168.2.3	0xd99	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:07.625021935 CEST	8.8.8.8	192.168.2.3	0xd99	No error (0)	photos-ugc.l.googlusercontent.com		172.217.168.1	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.635401011 CEST	8.8.8.8	192.168.2.3	0x6764	No error (0)	i.ytimg.com		172.217.168.54	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.635401011 CEST	8.8.8.8	192.168.2.3	0x6764	No error (0)	i.ytimg.com		172.217.168.86	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.635401011 CEST	8.8.8.8	192.168.2.3	0x6764	No error (0)	i.ytimg.com		142.250.203.118	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.635401011 CEST	8.8.8.8	192.168.2.3	0x6764	No error (0)	i.ytimg.com		216.58.215.246	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.635401011 CEST	8.8.8.8	192.168.2.3	0x6764	No error (0)	i.ytimg.com		172.217.168.22	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.639066935 CEST	8.8.8.8	192.168.2.3	0x8173	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:07.639066935 CEST	8.8.8.8	192.168.2.3	0x8173	No error (0)	stats.l.doubleclick.net		108.177.127.157	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.639066935 CEST	8.8.8.8	192.168.2.3	0x8173	No error (0)	stats.l.doubleclick.net		108.177.127.154	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.639066935 CEST	8.8.8.8	192.168.2.3	0x8173	No error (0)	stats.l.doubleclick.net		108.177.127.155	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:07.639066935 CEST	8.8.8.8	192.168.2.3	0x8173	No error (0)	stats.l.doubleclick.net		108.177.127.156	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:20.239403009 CEST	8.8.8.8	192.168.2.3	0x9399	No error (0)	www.google.co.uk		172.217.168.3	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:20.410337925 CEST	8.8.8.8	192.168.2.3	0x8c65	No error (0)	about.google		216.239.32.29	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:21.670382023 CEST	8.8.8.8	192.168.2.3	0xe945	No error (0)	www-google-tagmanager.l.google.com		172.217.168.8	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:23.964265108 CEST	8.8.8.8	192.168.2.3	0x69da	No error (0)	www.blog.google	ghs-svc-https-sni.ghs-ssl.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:23.964265108 CEST	8.8.8.8	192.168.2.3	0x69da	No error (0)	ghs-svc-https-sni.ghs-ssl.googlehosted.com		142.250.203.115	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:26.343535900 CEST	8.8.8.8	192.168.2.3	0x9dd8	No error (0)	about.google		216.239.32.29	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:26.358472109 CEST	8.8.8.8	192.168.2.3	0x80eb	No error (0)	lh3.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:26.358472109 CEST	8.8.8.8	192.168.2.3	0x80eb	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:38.992096901 CEST	8.8.8.8	192.168.2.3	0x9962	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.171857119 CEST	8.8.8.8	192.168.2.3	0x175e	No error (0)	tools.google.com	tools.l.google.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 26, 2021 07:51:39.171857119 CEST	8.8.8.8	192.168.2.3	0x175e	No error (0)	tools.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.179110050 CEST	8.8.8.8	192.168.2.3	0xa6b0	No error (0)	googleads.g.doubleclick.net		216.58.215.226	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.184384108 CEST	8.8.8.8	192.168.2.3	0x1fce	No error (0)	csp.withgoogle.com		216.58.215.241	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.191263914 CEST	8.8.8.8	192.168.2.3	0xb74a	No error (0)	static.doubleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:39.191263914 CEST	8.8.8.8	192.168.2.3	0xb74a	No error (0)	static-doubleclick-net.l.google.com		172.217.168.70	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.234755993 CEST	8.8.8.8	192.168.2.3	0x10c5	No error (0)	2542116.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:39.234755993 CEST	8.8.8.8	192.168.2.3	0x10c5	No error (0)	dart.l.doubleclick.net		216.58.215.230	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.282196045 CEST	8.8.8.8	192.168.2.3	0x26c5	No error (0)	adservice.google.com		142.250.203.98	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:39.862101078 CEST	8.8.8.8	192.168.2.3	0x3b5d	No error (0)	s.ytimg.com		172.217.168.14	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:40.309715986 CEST	8.8.8.8	192.168.2.3	0x175e	No error (0)	tools.google.com	tools.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:40.309715986 CEST	8.8.8.8	192.168.2.3	0x175e	No error (0)	tools.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:41.147811890 CEST	8.8.8.8	192.168.2.3	0x9fd2	No error (0)	adservice.google.co.uk	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:41.147811890 CEST	8.8.8.8	192.168.2.3	0x9fd2	No error (0)	pagead46.l.doubleclick.net		216.58.215.226	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:41.323385000 CEST	8.8.8.8	192.168.2.3	0x175e	No error (0)	tools.google.com	tools.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:41.323385000 CEST	8.8.8.8	192.168.2.3	0x175e	No error (0)	tools.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:42.685069084 CEST	8.8.8.8	192.168.2.3	0x8bf5	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:43.371001959 CEST	8.8.8.8	192.168.2.3	0x175e	No error (0)	tools.google.com	tools.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:43.371001959 CEST	8.8.8.8	192.168.2.3	0x175e	No error (0)	tools.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Aug 26, 2021 07:51:47.421471119 CEST	8.8.8.8	192.168.2.3	0x175e	No error (0)	tools.google.com	tools.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 26, 2021 07:51:47.421471119 CEST	8.8.8.8	192.168.2.3	0x175e	No error (0)	tools.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gmail.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49701	172.217.168.69	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 26, 2021 07:50:38.600047112 CEST	1137	OUT	GET / HTTP/1.1 Host: gmail.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 26, 2021 07:50:38.628710032 CEST	1155	IN	HTTP/1.1 301 Moved Permanently Location: https://www.google.com/gmail/ Content-Type: text/html; charset=UTF-8 X-Content-Type-Options: nosniff Date: Thu, 26 Aug 2021 05:48:32 GMT Expires: Thu, 26 Aug 2021 06:18:32 GMT Server: sffe Content-Length: 226 X-XSS-Protection: 0 Cache-Control: public, max-age=1800 Age: 126 Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 67 6d 61 69 6c 2f 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>301 Moved</TITLE></HEAD><BODY><H1>301 Moved</H1>The document has moved<A HREF="https://www.google.com/gmail/">here</A>.</BODY></HTML>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 26, 2021 07:50:45.672666073 CEST	172.217.168.68	443	192.168.2.3	49725	CN=www.google.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jul 26 05:58:56 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Oct 18 05:58:55 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Aug 26, 2021 07:51:26.385251045 CEST	216.239.32.29	443	192.168.2.3	49827	CN=about.google CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jul 26 05:42:32 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Oct 18 05:42:31 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Aug 26, 2021 07:51:26.386300087 CEST	216.239.32.29	443	192.168.2.3	49828	CN=about.google CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jul 26 05:42:32 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Oct 18 05:42:31 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Aug 26, 2021 07:51:26.422502995 CEST	142.250.203.97	443	192.168.2.3	49830	CN=*.googleusercontent.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jul 26 05:00:52 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Oct 18 05:00:51 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Aug 26, 2021 07:51:26.424606085 CEST	142.250.203.97	443	192.168.2.3	49829	CN=*.googleusercontent.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jul 26 05:00:52 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Oct 18 05:00:51 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 3528 Parent PID: 4824

General

Start time:	07:50:31
Start date:	26/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://covidteamclapham@gmail.com'
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 4904 Parent PID: 3528

General

Start time:	07:50:32
Start date:	26/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1600,818200865018122053,4149282262256251718,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1764 /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

Show Windows behavior

Analysis Process: chrome.exe PID: 6828 Parent PID: 3528

General

Start time:	07:50:41
Start date:	26/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1600,818200865018122053,4149282262256251718,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5704 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: 6860 Parent PID: 3528

General

Start time:	07:50:41
Start date:	26/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1600,81820086501812 2053,4149282262256251718,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=5720 /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

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly