ID: 451063
Cookbook: browseurl.jbs
Time: 07:18:40
Date: 20/07/2021
Version: 33.0.0 White Diamond

Table of Contents

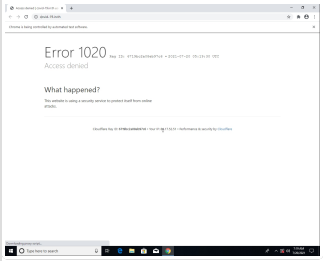
Windows Analysis Report http://covid-19.in.th

Overview

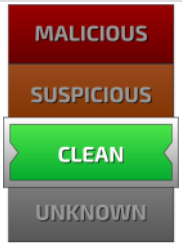
General Information

Sample URL:	http://covid-19.in.th
Analysis ID:	451063
Infos:	

Most interesting Screenshot:



Detection

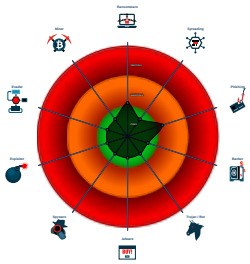


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Found iframes

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3096 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://covid-19.in.th' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5232 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1544,17804831982283933720,7344052518000277292,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1764 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7088 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1544,17804831982283933720,7344052518000277292,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=3720 /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

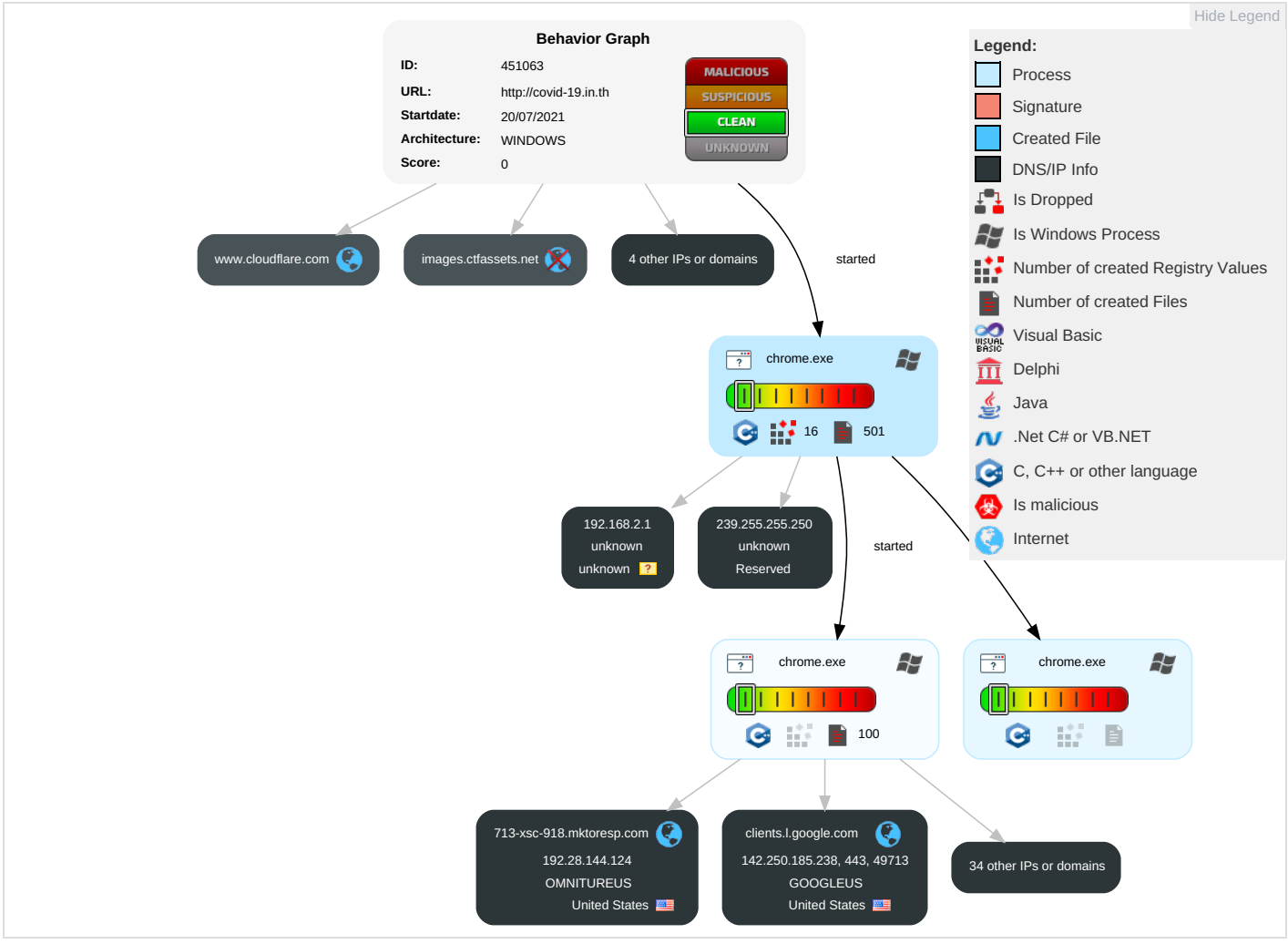
Click to jump to signature section

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 3	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 4	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	

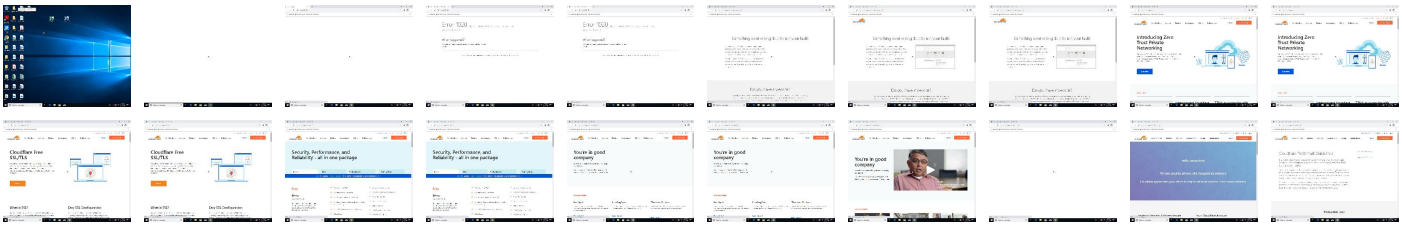
Behavior Graph

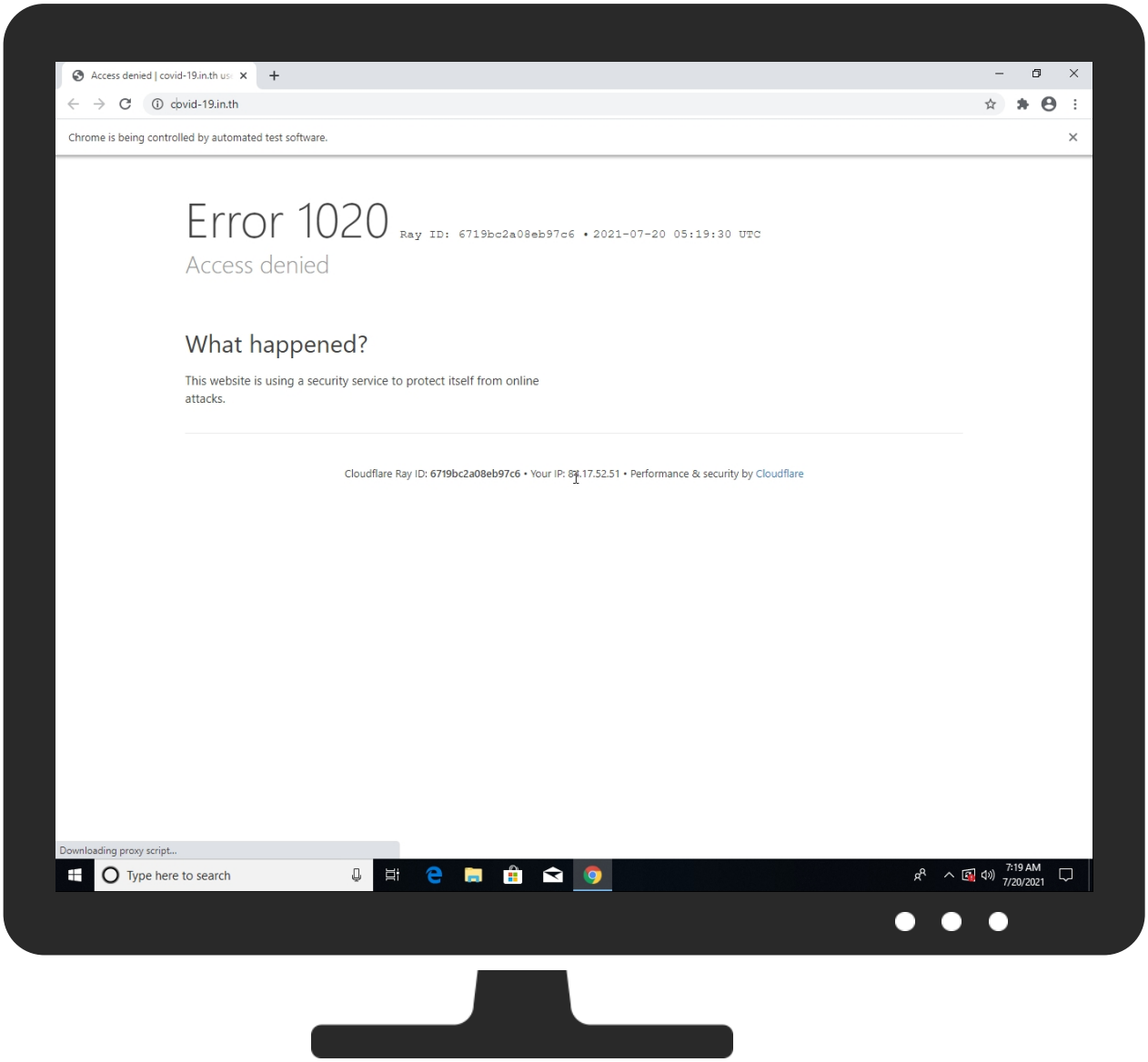


Screenshots

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
http://covid-19.in.th	0%	Virustotal		Browse
http://covid-19.in.th	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
embed.videodelivery.net	0%	Virustotal		Browse
static.cloudflareinsights.com	0%	Virustotal		Browse
videodelivery.net	0%	Virustotal		Browse
covid-19.in.th	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://munchkin.marketo.net/munchkin.jsaD	0%	URL Reputation	safe	
http://https://munchkin.marketo.net/munchkin.jsaD	0%	URL Reputation	safe	
http://https://munchkin.marketo.net/munchkin.jsaD	0%	URL Reputation	safe	
http://https://www.cloudflare.com3_https://www.cloudflare.com	0%	Avira URL Cloud	safe	
http://https://embed.videodelivery.net/embed/5.068adc7c.chunk.js	0%	Avira URL Cloud	safe	
http://https://static.cloudflareinsights.com	0%	Avira URL Cloud	safe	
http://https://www.googleoptimize.com/optimize.js?id=GTM-N4JSZJ8	0%	Avira URL Cloud	safe	
http://https://iframe.videodelivery.net/5efe5eca1517ad1a2f9ff3e75cc9cf5a?poster=https%3A%2F%2Fwww.cloudflar	0%	Avira URL Cloud	safe	
http://https://cookiepedia.co.uk/host/.app.onetrust.com?_ga=2.157675898.1572084395.1556120090-1266459230.15	0%	URL Reputation	safe	
http://https://cookiepedia.co.uk/host/.app.onetrust.com?_ga=2.157675898.1572084395.1556120090-1266459230.15	0%	URL Reputation	safe	
http://https://cookiepedia.co.uk/host/.app.onetrust.com?_ga=2.157675898.1572084395.1556120090-1266459230.15	0%	URL Reputation	safe	
http://https://videodelivery.net/	0%	Avira URL Cloud	safe	
http://https://munchkin.marketo.net/160/munchkin.js	0%	Avira URL Cloud	safe	
http://https://embed.videodelivery.net	0%	Avira URL Cloud	safe	
http://covid-19.in.th/S	0%	Avira URL Cloud	safe	
http://https://embed.videodelivery.net/embed/sdk.latest.js	0%	Avira URL Cloud	safe	
http://https://static.cloudflareinsights.com/beacon.min.js	0%	URL Reputation	safe	
http://https://static.cloudflareinsights.com/beacon.min.js	0%	URL Reputation	safe	
http://https://static.cloudflareinsights.com/beacon.min.js	0%	URL Reputation	safe	
http://covid-19.in.th/cdn-cgi/bm/cv/result?req_id=6719bc2a08eb97c6	0%	Avira URL Cloud	safe	
http://https://iframe.videodelivery.net	0%	Avira URL Cloud	safe	
http://https://embed.videodelivery.net/embed/sdk-iframe-integration.fla9.latest.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
embed.videodelivery.net	104.17.23.75	true	false	• 0%, Virustotal, Browse	unknown
dart.l.doubleclick.net	142.250.186.134	true	false		high
pagead46.l.doubleclick.net	172.217.168.34	true	false		high
d3orhvfyxudxxq.cloudfront.net	13.224.99.49	true	false		high
static.cloudflareinsights.com	104.16.94.65	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	172.217.168.45	true	false		high
stats.l.doubleclick.net	74.125.133.155	true	false		high
videodelivery.net	104.17.23.75	true	false	• 0%, Virustotal, Browse	unknown
tr.www.cloudflare.com	104.16.123.96	true	false		high
assets.www.cloudflare.com	104.16.123.96	true	false		high
adservice.google.com	172.217.168.66	true	false		high
covid-19.in.th	172.67.159.246	true	false	• 0%, Virustotal, Browse	unknown
www.googleoptimize.com	142.250.203.110	true	false		unknown
iframe.videodelivery.net	104.17.22.75	true	false		unknown
www.cloudflare.com	104.16.124.96	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com	52.31.250.1	true	false		high
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.185.238	true	false		high
713-xsc-918.mktoresp.com	192.28.144.124	true	false		unknown
www.google.ch	172.217.168.35	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
ab13.mktossl.com	104.17.74.206	true	false		unknown
d.adroll.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
adservice.google.ch	unknown	unknown	false		high
images.ctfassets.net	unknown	unknown	false		high
munchkin.marketo.net	unknown	unknown	false		unknown
info.cloudflare.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
9309168.fls.doubleclick.net	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.cloudflare.com/disclosure/	false		high
http://https://www.cloudflare.com/plans/	false		high
http://https://www.cloudflare.com/	false		high
http://https://www.cloudflare.com/case-studies/	false		high
http://covid-19.in.th/	false		unknown
http://https://9309168.fls.doubleclick.net/activityi;dc_pre=CKDH-KTz8PECFRAIiwodbzgMAw;src=9309168;type=prici0;cat=us-pr0;ord=5139259049669;gtm=2yg7j0;auiddc=295594570.1626790790;u1=2021%20Jul%2020%2007%3A19%3A58;u2=undefined;u3=https%3A%2F%2Fwww.cloudflare.com%2Fplans%2F;u4=undefined;u10=undefined;~oref=https%3A%2F%2Fwww.cloudflare.com%2Fplans%2F?	false		high
http://https://iframe.videodelivery.net/652f2749728df84fc32f9a6480438364?poster=https%3A%2F%2Fwww.cloudflare.com%2Fstatic%2Fa640feea55584c70b354fc1843efa0ed%2Fthumbnail_stream_case-study_lendingtree.jpg&preload=auto	false		unknown
http://https://info.cloudflare.com/rs/713-XSC-918/images/marketo-xdframe-relative.html	false		high
http://covid-19.in.th/cdn-cgi/bm/cv/result?req_id=6719bc2a08eb97c6	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.125.133.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
192.28.144.124	713-xsc-918.mktoresp.com	United States		15224	OMNITUREUS	false
142.250.203.110	www.googleoptimize.com	United States		15169	GOOGLEUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
172.217.168.66	adservice.google.com	United States		15169	GOOGLEUS	false
13.224.99.49	d3orhvfyxudxxq.cloudfront.net	United States		16509	AMAZON-02US	false
172.67.159.246	covid-19.in.th	United States		13335	CLOUDFLARENETUS	false
104.17.74.206	ab13.mktossl.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.134	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
104.16.124.96	www.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.102	unknown	United States		15169	GOOGLEUS	false
142.250.185.238	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.35	www.google.ch	United States		15169	GOOGLEUS	false
172.217.168.34	pagead46.l.doubleclick.net	United States		15169	GOOGLEUS	false
52.31.250.1	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.17.23.75	embed.videodelivery.net	United States		13335	CLOUDFLARENETUS	false
104.16.94.65	static.cloudflareinsights.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	451063
Start date:	20.07.2021
Start time:	07:18:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://covid-19.in.th
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:	23
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:	clean0.win@48/290@27/22
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.cloudflare.com/5xx-error-landing • Browse: https://www.cloudflare.com/ • Browse: https://www.cloudflare.com/ssl/ • Browse: https://www.cloudflare.com/plans/ • Browse: https://www.cloudflare.com/case-studies/ • Browse: https://www.cloudflare.com/disclosure/ • Browse: https://www.cloudflare.com/trademark/
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
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\0f48197a-0046-4d7a-80c9-6861e7aa1efe.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):	173333
Entropy (8bit):	6.0797758114643505
Encrypted:	false
SSDEEP:	3072:QLv+2r3yOGiQQh7pBxXfC89iXnFcbXafIB0u1GOJmA3iuRG:QvbnSQjaaqfIlUOoSiuRG
MD5:	29FA1DC3A7229FB5B5D6361E2447E037
SHA1:	247FABD39EB4D2F7342480B63A4A87B65E2F47B4
SHA-256:	C058D9A0C6A62BC7DAA844ECA33DD28B06E1AE40C10DCD7EC5983BC0394B884A
SHA-512:	08D823B5114926AE480618E73F82178093C413CA20718C2BAA653E75011B2D1D17C073BC9C0C43EDE4F951746250CE074490F2D84CCB6D77392AB226CB0F2AA(
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\0f48197a-0046-4d7a-80c9-6861e7aa1efe.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":1.626790769580132e+12,"network":1.626758371e+12,"ticks":6401271641.0,"uncertainty":3269599.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016530028"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\11ead4f6-2a63-4f93-9934-57d4040caa56.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7516131489660447
Encrypted:	false
SSDEEP:	384:pjeJZnsCTsLDVoOVwNtruvxr3yFHiHz6G+xrsPxxxSr3PGr09m0gGMrFJ1uOv/R2:RGKVdOjISAeTd3bs/7KnKFbZlQ
MD5:	F82EECBAA4B8E3079A844931C4026D12
SHA1:	974EDB489FA877246E7726AD9C76FDC26526CA11
SHA-256:	55C9ED6D7949EB4E1D16E3A837F6C1D160D12F2F62314C507FACBFAC9EAE77B4
SHA-512:	6D9B1E0714A5D4825AD5608417A9288488499B9FF94AD1E64DDC681AEA14C2677D23A393CC454EEFAE3130E8E01F1034BB59894AEEFE5C6E14BFF9D85B13D662
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...>@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\211f23db-9a95-4e5b-ab0c-e11c4fe565de.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):	164968
Entropy (8bit):	6.050168715655962
Encrypted:	false
SSDEEP:	3072:i+2r3yOGiQQh7pBxXfC89iXnFcbXafIB0u1GOJmA3iuRG:ibnSQjaaqfIlUOoSiuRG
MD5:	CD0A42BE10BD84E783976207B9A00CF8
SHA1:	8107E8AF49C9674C6D083093CBBCD395AEA751C1
SHA-256:	0E724C54D1A6C478223B66EEEE459EA6A02A4A0FF74CDFA0C8F29D8C246D33CC
SHA-512:	E20BAFCF093720BAF4D660ADD43DA9B60A5F8D892B4CAFD48754C056CE35F5F633AFC8570473540109E2D64E839D82452B9E49310ED1B242716202C61A829F7
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":1.626790769580132e+12,"network":1.626758371e+12,"ticks":6401271641.0,"uncertainty":3269599.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016530028"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\44613c03-2e0e-410a-8466-3e2981f17a41.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):	164874
Entropy (8bit):	6.0498909350169265
Encrypted:	false
SSDEEP:	3072:W+2r3yOGiQQh7pBxXfC89iXnFcbXafIB0u1GOJmA3iuRG:WbnSQjaaqfIlUOoSiuRG
MD5:	53B9602538316DE76C24911049024A8E
SHA1:	D7E47B8F4E15BAEDA52451F95FEBD675825CAF5D
SHA-256:	9E08CFE3A36E608B4961B716DF1B2F9B5FE73DAD7EB148F3E6B3DBBCE05DC815
SHA-512:	018E27ED796C1E4A8EA97D4CAB40E5D03B794BAA3681CCE299CC9633FA05243A04EDC4789AB68F9D487550EAE2BBD087DA650A8E706855DFE350DB40E39931D6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\44613c03-2e0e-410a-8466-3e2981f17a41.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":1.626790769580132e+12,"network":1.626758371e+12,"ticks":6401271641.0,"uncertainty":3269599.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016530028"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\469a8494-9d73-46f4-b40d-9b76f077e360.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):	173333
Entropy (8bit):	6.079777024935198
Encrypted:	false
SSDEEP:	3072:nk4+2r3yOGiQQh7pBxXfC89iXnFcbXafIB0u1GOJmA3iuRG:k4bnSQjaaqfIlUOoSiuRG
MD5:	AA0115358E0C2A549D44FCECFC97FCB5
SHA1:	4845891A1650011F51424B6E9866CBA7B7EA8FBF
SHA-256:	A7615CE7F0B637C0D67B3DA4B0C127A06BD983CCF2CD932CF73AC7A5AC97F802
SHA-512:	69A29D0FE9690BADD8230EB7E253530C8A9B96EFFACF8EA9B0BCFB85731BB3E2AFBF087BBF464D54E73CC614E0AAC79271D0413EF57D1DE32862017D42DAA1D3
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":1.626790769580132e+12,"network":1.626758371e+12,"ticks":6401271641.0,"uncertainty":3269599.0}},"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\4d077f68-7ca5-490e-a69d-80cd1c4af977.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):	173332
Entropy (8bit):	6.079776383270949
Encrypted:	false
SSDEEP:	3072:nRy+2r3yOGiQQh7pBxXfC89iXnFcbXafIB0u1GOJmA3iuRG:RybnSQjaaqfIlUOoSiuRG
MD5:	B818E2B509839E29C8990B3B569E7E7E
SHA1:	10DE094BB679C0A0020A756011D21F7D74CE2561
SHA-256:	714C0BC5DA6FF1AF1372BF4BEEC4A2B79E5F65982D1AD443C4DF1C5AC9A1D611
SHA-512:	4F70D2096D2D3B2DE0D47BB5AF4A745B9641C4C499109029C04DE2C1F8D2746CEF3C071D2F7ADABF7BBF98A13C74ACF6AE50DDB5E977564A8B15FE8D11BC54B
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":1.626790769580132e+12,"network":1.626758371e+12,"ticks":6401271641.0,"uncertainty":3269599.0}},"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\9c00506b-1e34-4f83-b979-9d4a0ba87e6f.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):	164874
Entropy (8bit):	6.0498909350169265
Encrypted:	false
SSDEEP:	3072:W+2r3yOGiQQh7pBxXfC89iXnFcbXafIB0u1GOJmA3iuRG:WbnSQjaaqfIlUOoSiuRG
MD5:	53B9602538316DE76C24911049024A8E
SHA1:	D7E47B8F4E15BAEDA52451F95FEBD675825CAF5D
SHA-256:	9E08CFE3A36E608B4961B716DF1B2F9B5FE73DAD7EB148F3E6B3DBBCE05DC815
SHA-512:	018E27ED796C1E4A8EA97D4CAB40E5D03B794BAA3681CCE299CC9633FA05243A04EDC4789AB68F9D487550EAE2BBD087DA650A8E706855DFE350DB40E39931D6
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\9c00506b-1e34-4f83-b979-9d4a0ba87e6f.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":1.626790769580132e+12,"network":1.626758371e+12,"ticks":6401271641.0,"uncertainty":3269599.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016530028"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\9d60a438-f3f0-45d6-b5f9-e77b3d5c724a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7514714493556096
Encrypted:	false
SSDEEP:	384:vjeJZnsCvL0VwNtruvxr3yFHiHz6G+xrsPxxxSr3PGr09m03MrFJ1uOv/RNM1dkp:OKVdOjWSAeTd3bs/7KnKFbZll
MD5:	3DFBD72F4668576F2B99CA52F8EDD7CC
SHA1:	714602B062C9EEC0DE6702D9F0E756B8D461522F
SHA-256:	20C31AC5FCC88FFA1CD6F0E2775A4C2580B086CEC2941AE1D3018BA2F036056A
SHA-512:	8B6EC8C8F894E16F069EC6F36FC681A66A4A21556BEFACE302EE112E835E83C6852E6AC45D0D11C97C081860A929C375D8291624A3ADA9C5318539E492D500E
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...>@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
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\0a2a6490-9191-42e4-bf96-15d5ea3b4a64.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):	1206
Entropy (8bit):	5.578102008312506
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXv0b7wUCWK3UpuewUMRUenHQ:YI6UUhVseKUewqPeUer2UefEwUrK3iw6
MD5:	FD26C7533D2AAF7F4BA1E30576CCA00A
SHA1:	C996D9C9EC0DDD71263A3CB727390B60424667E0
SHA-256:	1D7A0AB0254825AC5060BE624806226A2B44EF7A7820A212F20B66B2421A1B8C
SHA-512:	6820F7D02435D100174487835902430E807E2C59D6EF920C692702D8BBB35C35813590032C422A9663FFB91FCD0E9A4C522A9D262316DB9BCF07532E79E906AC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0a2a6490-9191-42e4-bf96-15d5ea3b4a64.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":1658326770.55928,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626790770.559284},{"expiry":1658326780.373766,"host":"+VzK80JcxHM7Xd/qnZuqoBLw6iEYYewOPd/04cb1NYc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0a7ca285-9872-4552-9d43-982280fd6e51.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):	2210
Entropy (8bit):	5.610090205898448
Encrypted:	false
SSDEEP:	48:YMUyuwUHeU76UUh9U3UaseKUe/IcUXqPeUer2UefpRUBzwULiwUFUenw:9UyLUHeUeUUDGUa3KUzcU6PeU9UEpRUH
MD5:	0B7C5D149BB9E7B45AFDC8D2AB2D0F80
SHA1:	A6FC76009E750AEC3491AD5B7C65DF3FCA4290DF
SHA-256:	0418883E18FD63A0206F28FDCE8C49BB94D152A6905C51D1457A05C130078213
SHA-512:	DAB6B998421D783A3B550B42BE234EFBF09D8BBAB37870CCBAB664E052CFCBA11814E890E43A5A7D69ECC7243D1D03BDFFE1BA9DD5F5F0CC43A1332E8F505 5BD
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1642342803.259748,"host":"BY/bcdOmoK9rlC6qRniKTNBFPQRySUUIWrrR/PUkV/4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626790803.259754},{"expiry":1626812403.048868,"host":"Ie2p1rK5PbkAy3tH/gbQ14Xhq5IimP6vz4V/UKzEP+c=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626790803.048873},{"expiry":1637677183.581073,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626790783.581078},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1642342808.45832,"host":"ZIyqbuBqOyJ3CRPSHhdXFGsxhupXQvSmyFLKICQRXP4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626790808.458324},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1342c6c6-ea02-4742-88e5-99638fa351f9.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):	5786
Entropy (8bit):	5.192049059828668
Encrypted:	false
SSDEEP:	96:nvC06TZMnasiOZfkcKIyok0JCKL8hk81wbOTQVuwn:nvCvMQbcz4Kmk8o
MD5:	FF1386ECB4F05F50620EC1B18FEAD7BC
SHA1:	8C0A6581B90EF32D6F01EF412B613EFC0F816B39
SHA-256:	8C4F9C5DC292315198F94DAFE9613ACECAA1609ED31C169E83D9DC231F090DA5
SHA-512:	A4C2D859338FBD0B9FC8F9584A7656635A2EF2D8EC24AFA4501C14CF0FCE37CA31F30B3E758FCCD80C485F76627DFD9A5913E44E02A1BD410C556DC2E3BAC 55
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271264367376957","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\1463eae6-0dfb-4222-a7e9-4c68015b09fa.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1540
Entropy (8bit):	5.598951729018091
Encrypted:	false
SSDEEP:	48:YzeU76UUhVseKUehcU+lqPeUer2UefEwU/iwUIUenw:UeUeUUX3KUCcU+wPeU9UEJU/PUIUD
MD5:	214789216F67582C9C42A4F5A2D41BBC
SHA1:	5C2D415BA390953203824CA61848EA5B32AF1503
SHA-256:	281D840F2B61277AFFECE64BCEAF795F7D8005BADA523194DC519D6180E8BADD
SHA-512:	76CE9459C106E2581FC7215F664CDB99B08339D34F9F52D7D422931BC11847A8D4FE49C4F597CD2738B9B48B13E607D5971A97F7E02CBA8A1FCB8E896CDB2E7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1463eae6-0dfb-4222-a7e9-4c68015b09fa.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1637677183.581073,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626790783.581078},{"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":1658326789.550751,"host":"opXOuPncEqRjkYSjAgcGEU30CFS/DB8Obxt4KuKod80=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626790789.550755},{"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_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\42c273dc-a07d-41ec-9861-f58e3a21e0ad.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):	24056
Entropy (8bit):	5.5329772132501285
Encrypted:	false
SSDEEP:	384:GL+tvLlgCX51kXqKf/pUZNCgVLH2HfD3rUXHGyHGSnTAOGp4I:/Lld51kXqKf/pUZNCgVLH2HfDrU3GyGf
MD5:	39100BD211926B6D2995F6E45A2AC900
SHA1:	A2FBC0EEF578BFE5AA0497D6485ABBC986365C1B
SHA-256:	20366AC4CBD6067F6392497103FA49AFA12E2A8EB6A6831F6A526AEBBBA81D1D
SHA-512:	EC3404C049710802E93242213AD3C030BCADE9DC64572B278740D92E89F22E89AB3742C905D917DE72D83F37AD0097A66FB3BA5AA308E28A17369400A9861AC8
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":"13271264367167519","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6a02d815-e375-4187-8ee8-df799bf578ce.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):	2044
Entropy (8bit):	5.601088446289512
Encrypted:	false
SSDEEP:	48:YvUruwUHeU76UUhVseKUewscUSqPeUer2UefoKRUDXwUTiwU0xUenw:uUrLUHeUeUUX3KUfscUZPeU9UEoKRUD4
MD5:	B8EB214AAB1FFAB96AB85F56C6156869
SHA1:	49BCEA77A8454433CF000B9D05918513C95BBCB5
SHA-256:	3053319110AC927C07BC5ACD38BF445F8D584A2968EF8476246FBA3D5879033C
SHA-512:	F97E5114778E51D00A956F3211739F59BA9EF4E2F08B18D7C9434B7479FF8752067536AF8B8B699F9C8DE801343B3AEC60095D454717180AAA83026F68E80286
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1642342803.226152,"host":"BY/bcdOmoK9rlC6qRniKTNBFPQRySUUIWrrR/PUkV/4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626790803.226157},{"expiry":1626812403.048868,"host":"Ie2p1rK5PbkAy3tH/gbQ14Xhq5limP6vz4V/UKzEP+c=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626790803.048873},{"expiry":1637677183.581073,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626790783.581078},{"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":1658326801.834238,"host":"opXOuPncEqRjkYSjAgcGEU30CFS/DB8Obxt4KuKod80=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7767bedb-b1a6-4557-a89d-f05989e6c60d.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):	24054
Entropy (8bit):	5.53305020904649
Encrypted:	false
SSDEEP:	384:GL+tKLlgCX51kXqKf/pUZNCgVLH2HfD3rUXHGyHGVnT7OU5p4k:6Lld51kXqKf/pUZNCgVLH2HfDrU3GyGP
MD5:	94E92A440155FA65A6BBA4578336F426
SHA1:	A12A4C3269171026DC178EA695622D80F76146B1
SHA-256:	AD627FC9105D54EA9B1BBDC4C31259A6D83EB407B0C9026BE4821DE9757FA6F0
SHA-512:	2EB085922621EC0B67E23AD7E92F6BA46DDF022EBA4372E12509662F2C0D06BEE6746A3739A168EAFFC747AB822079DE9D9297A515D4D6F75BAD9B1CDC6C940
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7767bedb-b1a6-4557-a89d-f05989e6c60d.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13271264367167519","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\784431e9-0fc3-4a2a-b8ab-75baf3278073.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):	5.5352523893863985
Encrypted:	false
SSDEEP:	384:GL+tvLlgCX51kXqKf/pUZNCgVLH2HfD3rUUHGXnTAO8p4y:/Lld51kXqKf/pUZNCgVLH2HfDrUYGXnE
MD5:	34ABF7BD3EB47A8CE3F4C205397C5DAB
SHA1:	B00B24CF79C48B28F6559046972AC2341033DA5B
SHA-256:	4CA8BE2A1C614EDEC1207606978161723D020F4C7DB9530A95E7AF7A039439F7
SHA-512:	409D2EDF1189119B82FB93D5F3770B9CD28C4E926192C8733ABAF5A9F5EFA9835AE4CDD034523D086037CFBBF6D9C4D3254BF2A915B268D5CBB699F6747C69(
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":"13271264367167519","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\856dd01d-48ab-40dd-9de5-f3efb99bb29a.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):	5760
Entropy (8bit):	5.189223759206593
Encrypted:	false
SSDEEP:	96:nvC0GTZMnasiOZfkcKIFok0JCKL8hk81UbOTQVuwn:nvCHMQbcO4Kmk8M
MD5:	B5BF0F943FB1230E376F68D345B745B4
SHA1:	368AE05298683E103251F8BDDE4F57678099178E
SHA-256:	FBAFF64FC497B2BD5A20921CDBFDEB9F19C9F15C02478F212CF6DED0D385E07D
SHA-512:	E74056BF41DE2F3856617B7928512E2DF9CD6BD985D756F4C8D4D4FDD23A5388312B44F5635329F7D87B0FA8C0041AB646E72A3F7824A2218DB787A1EA203702
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271264367376957","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8a4bd52e-baaa-4d1c-8111-1cc82c2bfcc4.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:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160:
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8a4bd52e-baaa-4d1c-8111-1cc82c2bfcc4.tmp	
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\8a73e87f-6b02-4f59-bcd1-0c99b0976e7a.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):	5760
Entropy (8bit):	5.18928925372123
Encrypted:	false
SSDEEP:	96:nvC0GTZMnasiOZfkcKIyok0JCKL8hk81UbOTQVuwn:nvCHMQbcz4Kmk8M
MD5:	7D970C65AC131ED7BEDEA087C5BC8D2C
SHA1:	27DB7FA1A4956F07CC3E216129A824016C0EC248
SHA-256:	1EF528FABC988439FE84D6E1ECBFB47F61674F3A3E206616CD75D969E9494AE4
SHA-512:	ED35202CCFA57417A4E000057A319D90745BF6C937149A5BA8B7284656A7A21EE911A0DAEB41FC120549EE61875BA6DE3846FD735B6272EC714F620BCAEF30BC
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271264367376957","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9a5ad0b0-a80f-4f90-ac72-3f0e62351f52.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):	2210
Entropy (8bit):	5.613142089077329
Encrypted:	false
SSDEEP:	48:YMUyuwUHeU76UUh9U3UaseKUelcUtqPeUer2UefpRUBzwU3iwU1pUenw:9UyLUHeUeUUDGUa3KUWcUYPeU9UEpRUt
MD5:	B7DA23E24040BB909740A141737040A6
SHA1:	C9C7933D06539D8E54CF7FB02F70304B43A0FE91
SHA-256:	134C928C79120B39EBA3B15B5B0F8D0814D09901A5658E429F9BA0D326AC4A66
SHA-512:	A797C463E9FC3EE947F161A4DE79C965E9CC31D35E765A4B8DD0E793AA65743B07AFFA7DB51564796A69EDAD475D50958960AD1153AB0244B1B5370CC7CC3B3
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1642342803.259748,"host":"BY/bcdOmoK9rlC6qRniKTNBFPQRySUUIWrrR/PUkV/4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626790803.259754},{"expiry":1626812403.048868,"host":"Ie2p1rK5PbkAy3tH/gbQ14Xhq5IimP6vz4V/UKzEP+c=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626790803.048873},{"expiry":1637677183.581073,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626790783.581078},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1642342808.45832,"host":"ZIyqbuBqOyJ3CRPSHhdXFGsxhupXQvSmyFLKICQRXP4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626790808.458324},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9dd9b22c-6d38-4225-a37a-fa4d7ce21021.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):	5747
Entropy (8bit):	5.187984120631316
Encrypted:	false
SSDEEP:	96:nvCAoTZMnasiOZfkcKIPok0JCKL8hk81UbOTQVuwn:nvCfMQbco4Kmk8M
MD5:	85129332173DE991964F3B096366AB83
SHA1:	0ABD7F9498E88E02212483BABBA0B9D88F9AFE5C
SHA-256:	1F5B0B1238F23EF36A3C00A5D315877CAF91E221EACC1F658B5C9CB21D86B7B2
SHA-512:	D8579FF665A31B848057E0C46BA748C7954ECB12E7DA7F3A9938DEC022E5B5F9F7047E3D66DFC47E19991AFDC8DE89A4AC011BE74B9AAF2D3831778A38E326[illegible]F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9dd9b22c-6d38-4225-a37a-fa4d7ce21021.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271264367376957","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.251601810130959
Encrypted:	false
SSDEEP:	6:mY39+q2PWXp+N23iKKdK9RXXTZIFUtp3ZZmwP8VkwOWXp+N23iKKdK9RXX5LJ:B34va5Kk7XT2FUtpp/P85f5Kk7XVJ
MD5:	4C65AD6F1ECE4DE3A7847568114386A0
SHA1:	2C7FA01A65FC1A0C0232BB0132AA03D7CFE5573C
SHA-256:	6AC64618D60781841F9FC9E616605E0F6D21F2642CFFC9F7832A536C2DDBDDD1
SHA-512:	EBE3852AB4609B50D01574CA158C2AF342C0BE5993823AF76289A920DBF04A4EC07FF5C3D9DFC3D7D1E929C24C3DBC30551D87044F7D531D0A6BC5BC63BBB8 E7
Malicious:	false
Reputation:	low
Preview:	2021/07/20-07:19:35.132 958 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/20-07:19:35.138 958 Recovering log #3.2021/07/20-07:19:35.139 958 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):	315
Entropy (8bit):	5.214627947627847
Encrypted:	false
SSDEEP:	6:mlm69+q2PWXp+N23iKKdKyDZIFUtp1cINJZmwP6VkwOWXp+N23iKKdKyJLJ:m4va5Kk02FUtpWIX/Py5f5KkWJ
MD5:	1F21044B478F41074CDF2FDEECFCB584
SHA1:	FEEC67E67639404103FF93FD0A6EC8ADE6D19127
SHA-256:	94E1E6706A606ADB69008E674D44E883E9D5E21A1C942074F11D5C4BEA05BEF3
SHA-512:	8CF9C9E49A721520F27EEE58752D57B16D5C18F80446C80B578E7FBF9EDD355D4C335EB8BA071B24F59600D1D9A04417EBB17E3B7FFA3693A7B01B82672C993
Malicious:	false
Reputation:	low
Preview:	2021/07/20-07:19:35.100 958 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/20-07:19:35.105 958 Recovering log #3.2021/07/20-07:19:35.111 958 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\031e396cb6831fa7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8312
Entropy (8bit):	5.646290790109634
Encrypted:	false
SSDEEP:	192:Sb7ZvJ81zESVOyIaoranAvEKHZLG05lKTz+R:2RJ8xEyargAtlkE
MD5:	B3F4B71431DC27084A553A7FA68CF56C
SHA1:	2F1EFCAC7788B5E915A652C7F4F2AA0E14FF9A7D
SHA-256:	9CBDE24830DCA188E41C4B08950C176BA5E5F05635AF83439EB57281E7D71502
SHA-512:	D6A1A213C068C430F07A9D899B658A52A671F55330789D865A9C8F17B89B82242B75B9296D4C34561E7B76DBA1B3B68EDFE7A210DC1A52EE4CFA22BDBE43000 C
Malicious:	false
Reputation:	low
Preview:	0\r..m......X...9.ZV...._keyhttps://www.cloudflare.com/8eaff4a1-b7a7207301c7b03b97d8.js .https://cloudflare.com/.$..%&/.....................'.d&]...p..}t.<?...j..O_>^.....A..Eo......V&by.........A..Eo..............................'..:....O........._xK..........................t................(S.l..`.....$L`......Qc.j.J....window...(Q..........__LOADABLE_LOADED_CHUNKS__....Qb...m....push.....`......L`.......`......Ma........`........a..........Qb........ac1MC.(S.......Pd........push.ac1M...ab....9...........qs........1.2..@.2.3..@.3.4..@.4.4..@.5.5..@.6.6..@.6.7..@.7.7..@.8.8..@.9.:..@.:.:..@.:.:..@.;.<..@.<.=..@.=.=..@.=.=..@.>.?..@.?.@..@.@.A..@.A.A..@.B.B..@.C.C..@.D.D..@.D.D..@.E.E..@.F.G..@.G.G..@.G.G..@.H.I..@.I.J..@.J.J..@.K.K..@.K.L..@.L.M..@.M.N..@.N.N..@.O.O..@.P.Q..@.Q.Q..@.Q.Q..@.R.S..@.S.T..@.T.T..@.T.U..@.U.V..@.V.W..@.W.X..@.X.X..@.Y.Y..@.Z.Z..@.[.[..@.[.[..@.\.\..@.].^..@.^.^..@.^.^..@._.`..@.`.a..@.a.a..@.b.b..@.c.c..@.d.d..@.d.e..@.e.e..@.f.f..@.g.h..@.h.h..@.h

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\09d0a59a0de48c50_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.733523194047859
Encrypted:	false
SSDEEP:	12:F1TYl5W4k6oP1TYu4W4kIrP1TYJW4kUl:z0up/90ulpU90YpUl
MD5:	FBA39A6699CB63758A157A9DDB3FE6CD
SHA1:	6F7F98D708DA163CBF4A7D1319AD04D211B70FBE
SHA-256:	F84AED245C6755EEC6AC2B02131678D0CE00696B2603E46C21E26EABD4EAACFB
SHA-512:	E06DC7383622E54D8BE6B2D227202162098F38189EF55A6C4CE8B99A913E2356E30EA217D1A8071C8512136DED9A82B3364D71821DAE2704602E83AF8612BBB5
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...P.m...._keyhttps://assets.www.cloudflare.com/js/chunk-5f991135348b5b16cb1b.js .https://cloudflare.com/....%&/.....+..F...nx..MV....[*.....9D.K.A. .Eo.....y4+.....A..Eo.....0\r..m....._...P.m...._keyhttps://assets.www.cloudflare.com/js/chunk-5f991135348b5b16cb1b.js .https://cloudflare.com/....%&/..... ....C.....+..F...nx..MV....[*.....9D.K.A..Eo.....!.j.....A..Eo.....0\r..m....._...P.m...._keyhttps://assets.www.cloudflare.com/js/chunk-5f991135348b5b16cb1b.js .https://cloudflare.com/-K..%&/.....z'.....+..F...nx..MV....[*.....9D.K.A..Eo.....H&.J.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\09fb8741326e0b46_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.735246909613906
Encrypted:	false
SSDEEP:	12:xuDAoCFL3zuDAbsb4zuDA5LyzuDAF/jcx1zuDAmBVXpSpzuDAHhi7:4U1FL3qUg4qUdyqUFLC1qUabKqUHhi
MD5:	FBB18011F60B0A835B09B277FEE9DE18
SHA1:	DCEC82E043D72FFBA37A6A443FA6A9CED5FF221A
SHA-256:	430C3B99958C7166A44B747A646F73329A3E04E86E8BD7B7BE05AF800FE359EA
SHA-512:	55AB95BA7BD5E3CC182AA51766D20FD9DBA50A79AC2E8A6133160C0203C781545E21844065D677359B1B7033F3F0E24CFF51AD0FC41DF7877388F971EBDF227
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://www.googleoptimize.com/optimize.js?id=GTM-N4JSZJ8 .https://cloudflare.com/...%&/.....X.....G.....}\....J.5.\.|vS..C3{..A..Eo.....v. .....A..Eo.....0\r..m.....V....._keyhttps://www.googleoptimize.com/optimize.js?id=GTM-N4JSZJ8 .https://cloudflare.com/...%&/.....G.....}\....J.5.\.| vS..C3{..A..Eo.....R.....A..Eo.....0\r..m.....V....._keyhttps://www.googleoptimize.com/optimize.js?id=GTM-N4JSZJ8 .https://cloudflare.com/5. .%&/..... .....G.....}\....J.5.\.|vS..C3{..A..Eo.....?.....A..Eo.....0\r..m.....V....._keyhttps://www.googleoptimize.com/optimize.js?id=GTM-N4JSZJ8 .https://cloudflare.com/Q;d.%&/.....`.....G.....}\....J.5.\.|vS..C3{..A..Eo..... .....A..Eo.....0\r..m.....V....._keyhttps://www.googleoptimize.com/optimize.js?id=GTM-N4JSZJ8 .https://cloudflare.com/.f..%&/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a5bddda536af763_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	687
Entropy (8bit):	5.627870909713855
Encrypted:	false
SSDEEP:	6:mLYcvSOIYeiMY1+HgVd3UqZCr44DK6tWLYcvSOIYeiMxgPvUqZCr4yRK6tWLYcvm:7ntw+wd3UqZKBntmUqZUrBntiX3UqZ0
MD5:	43C3FA0353F23B6BEDE62010433E6F1F
SHA1:	5657B4D7F143ACED821810023A1968B800751E85
SHA-256:	443FAEEDEC014B43184DF499A4B41D4CB54DC2159CB7BC3CB46E24F87D516A33
SHA-512:	3AAE5860CC95F536324D62E33C34A3D50F0C8A73A53206884F7C700AA9BFED20E753A1E92A40D0345721BD1019D7BD08E89053D2897A4C397E65FD37DA7F9A0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a...*M&\...._keyhttps://assets.www.cloudflare.com/js/runtime-6a16446847617098e330.js .https://cloudflare.com/.M..%&/.....0.....Z*.....c..?9...m.Q...Dz'....< .A..Eo..... .....A..Eo.....0\r..m.....a...*M&\...._keyhttps://assets.www.cloudflare.com/js/runtime-6a16446847617098e330.js .https://cloudflare.com/.]..%&/.....t .....Z*.....c..?9...m.Q...Dz'....<.A..Eo.....'.\.....A..Eo.....0\r..m.....a...*M&\...._keyhttps://assets.www.cloudflare.com/js/runtime-6a16446847617098e330.js .https://cloudflare.com/*...%&/.....%.....Z*.....c..?9...m.Q...Dz'....<.A..Eo.....oTw.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0c84bc0ecf0dee96_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.688855964454208
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0c84bc0ecf0dee96_0	
SSDEEP:	12:FsmRLMKCLBPsmRLMVCLEONPsmRLMcHyCLz:6mtMKCLBUmtMVCLbUmtMQyCLz
MD5:	65B4544B83F168D728710DD2C2938B8B
SHA1:	F27C4CF6D1F3742F84BEA981699589F0FA9D74C1
SHA-256:	CC716FDADB8E9CFE06D4CD9A304978A990FBF0D293195726D4919638EC09B2DE
SHA-512:	6A25CCFEFC6817CB1F6C9C16820511DD5148F20EEA521B9C31353BDC0EC44137D6491D1A3E0061B349187F88EED3B058DC13BB320F27D150FA2CC36C813947
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....._keyhttps://assets.www.cloudflare.com/js/chunk-962e1864decb73b3a75a.js .https://cloudflare.com/....%&/.....>h..~.O....:.i.....B.@.A ..Eo.....;Q.....A..Eo.....0\r..m....._....._keyhttps://assets.www.cloudflare.com/js/chunk-962e1864decb73b3a75a.js .https://cloudflare.com/....%&/.....:.... .....>h..~.O....:.i.....B.@.A..Eo.....A..Eo.....0\r..m....._....._keyhttps://assets.www.cloudflare.com/js/chunk-962e1864decb73b3a75a.js .https://clo udflare.com/\G..%&/.....u'.....>h..~.O....:.i.....B.@.A..Eo.....Awq.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\132f44c2689e2c96_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	195080
Entropy (8bit):	6.039395530575337
Encrypted:	false
SSDEEP:	1536:RmA0q4WDQG9AAyG1o++hT5nmfo+v5nmfxtmVU8ydRZQKbgNxo3rT9kBTzUikwamp:R29WH1hUZZQVNmTi3tDLX
MD5:	48F46AD2D4EFE424CBA73B4BD1C3DFB6
SHA1:	9DA585A0473D052C6E0A892A5D5993EF4BB4CABD
SHA-256:	C5B409B7963EFA1A4E8E7E0FBA8E9B1A8DA94097CBB32AE6230911EAD9C54508
SHA-512:	F04291DE2706AC947FE071554718815ADCEB38C6AC3E7F12F564186EDD39B3F4227A4E3A9B59CBFC1D16BD84D397002E19BD2B67B163D2C124A0AC320D465A 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...5/.....632CCF83066B6D902D093E184EA7E6298731C01624806D6B2314CA305C5FBC86.....'..0....O-.....:_u.....85..... .....8.....D...\.....4.....(S.0..`.....L`.....(S...95.`.j.....L`.....Rcp.....0.....Qbn.....o.....Qb>P.)....r.....M...R. ...Qb.=\.....p.....Qb.tB.....t.....Qbz.%C....c.....Qb..C.....n.....QbV.|.....s.....S...Qb2..s...l.....QbJ).....d.....Qb"P.....k.....Qb.b33....h.....Qb..j....y.....Qb.F.....f.....Qb.....C.. ...Qb>>. ....w.....Qb.....A.....Qb..=L....S....Qb.L.....x.....Qb..d....j.....Qbn..b....B.....Qb..~....G.....QbZ?.!....H.....Qb._.1....O.....Qb&*.....M.....QbZE.$....q.....Qbr.....z.....Qbf.. x....W.....Qb..a.....K.....Qb.....Y.....Qb&.....J.....Qb.b\|.....Q.....QbJ.....Z.....Qb..`.....X.....Qb..%.....ee....Qb.$N....te....Qbnl.B....oe....Qb..?.....ne....Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\18b97f4ce89cc052_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.715234538645875
Encrypted:	false
SSDEEP:	12:Fkn7UXRtthrZ41Pkn7U1hrZT7Pkn7UoUhrZ92:a4B1K184/J84o0D2
MD5:	FEF35E7D1E1748561988F2D24C1C05EE
SHA1:	6572A9FCDB3B18F0CDD57DCF275BB5E5AF58E78F
SHA-256:	B80BF6A5C80ADADBEE2881FCDE57A421A35A6756EC45BCCDB2B47D5662954996
SHA-512:	E2848D73116822614BD51C93EF5023AF5D1AA2F165AB30BC562FFCB47BDF70D45FDCBEA09002051DB6B0527C42043FB50CE8088C1AF52795E3149292D15B779
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....._keyhttps://assets.www.cloudflare.com/js/chunk-232ffa51e57f882f0534.js .https://cloudflare.com/_...%&/.....2.....i.H{..F...S..H...qW.....(.i.A..Eo..... A.....A..Eo.....0\r..m....._....._keyhttps://assets.www.cloudflare.com/js/chunk-232ffa51e57f882f0534.js .https://cloudflare.com/.U..%&/.....v.....i.H{..F. ..S..H...qW.....(.i.A..Eo.....A..Eo.....0\r..m....._....._keyhttps://assets.www.cloudflare.com/js/chunk-232ffa51e57f882f0534.js .https://cloudflare.com/Z... %&/.....%.....i.H{..F...S..H...qW.....(.i.A..Eo.....3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\20208095690143df_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2640
Entropy (8bit):	5.744257542109046
Encrypted:	false
SSDEEP:	48:3ku+tN5WQIS3C5EcKdeCFOQ/3lr93vnduRCWS/hQHXIaxMh5t/sEl5xTzfeB:ryN+BucKdeCFOQ3lrdnduyh4XX+5t/fk
MD5:	902C3B46D6C1296845D85B5E8389858B
SHA1:	2399951C383AEB89E6044569D3C71541703E0BBE
SHA-256:	FE4E067DB8A4ED0836A618116B951FBEC4838A6000C9F5147F63D5090DC00A8E
SHA-512:	FF426938DADEFE3E384824BE5E8D329AAB197A5C37819FEFE1D52715E176000C5DB0020B2B791AFC7ECF5A215F20D1D77BA8CBCCC420E688638EA3A6AA366F A9
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\20208095690143df_0	
Reputation:	low
Preview:	0\r..m.....x...z....._keyhttps://www.cloudflare.com/1c5e1e1e37532e5d3e12606c412d346b1e41bfcd-93c6d6b82e344fb29469.js .https://cloudflare.com/rp..%&/..... ..*..z.J.;.....v.....7.!^.....2.A..Eo.....6t.?.....A..Eo.....rp..%&/.....'..=....O.....A.A.....<.....(S....`.....lL`2.....Qc.j.J....window...(Q....._L OADABLE_LOADED_CHUNKS__....Qb...m....push.....`.....L`.....`.....Ma.....`.....\..a*.....Qb...P....1HU7C..Qb.;.....2wa6C..QbR{.....HMs9C..QbN1+a....PTkmC..Qb. Wg.....SeimC..Qb...W....Z1EpC..Qb..3Y....tDjCC..Qb*$.....tvXGC..QbZq.-....uUxyC..Qb.M.j....wFXmC.(S.....Pd.....push.1HU7...ad.....E.@.-....hP.....[...https:/ /www.cloudflare.com/1c5e1e1e37532e5d3e12606c412d346b1e41bfcd-93c6d6b82e344fb29469.js.a.....D`....D`&...D`.....Y....`....&...&.....D&.(S.....Pd.....push.2wa6...a.... 4.....E..Q.d.....@.....D&.(S.....Pd.....push.HMs9...aB....!.....{g.....@.....@

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\26ce44646e1a1769_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	5.523837681271579
Encrypted:	false
SSDEEP:	12:BPRUscGzLPRUGpi7GklNLPRUZKdGY7LPRUgKD3GB1:BpUspLpUG8HlNLpUEp7LpUgKDE
MD5:	F7D99939914F19A635187DFAFA282E56
SHA1:	AF87E8510D41024FF12CB95E82E23CFDAA218D8B
SHA-256:	C6FB226C512AA057240F12773AE52D4950D83F0BC85EE5CC735F29D5FBAFC332
SHA-512:	B99945850C4D1AED2B42EC6064684D3A32A19373ED94AD6EF49E6715964FFAD65FB3884A9C202F806D00FAE37C1964234640FD0E37736F4E36CC62BC3E1AE92
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....%6....._keyhttps://info.cloudflare.com/js/forms2/js/forms2.min.js .https://cloudflare.com/....%&/.....[.....%....4...<.....e.Yd...A..Eo.....M.H..... .A..Eo.....0\r..m.....S....%6....._keyhttps://info.cloudflare.com/js/forms2/js/forms2.min.js .https://cloudflare.com/.,..%&/.....p.....[.....%....4...<.....e.Yd...A..Eo.... ...1.....A..Eo.....0\r..m.....S....%6....._keyhttps://info.cloudflare.com/js/forms2/js/forms2.min.js .https://cloudflare.com/....%&/.....B'.....[.....%....4...<.....e.Y d...A..Eo.....A..Eo.....0\r..m.....S....%6....._keyhttps://info.cloudflare.com/js/forms2/js/forms2.min.js .https://cloudflare.com/...,%&/.....3,.....[.....%....4... <.....e.Yd...A..Eo.....c.R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2f37f2b08fea58ef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	287
Entropy (8bit):	5.517186700601419
Encrypted:	false
SSDEEP:	6:mE0gEYGL1yMWglgQBrlQBhtwVUmygenjN92Em4YXK6t:Z0KBgVB+BhWFgyEmnZ
MD5:	E99A5B6DC513853790B6AF3A7267641C
SHA1:	BDBE36666CD04FF334BAD8D7A79ACE292BC831FA
SHA-256:	9C42858DC070979B2F59BA97C1919F80E90B19BD7E6064B6FEC3BFCE44B930A0
SHA-512:	AF07DB6CFB973E5C6A02758ACC0169437543053496BB99C257B176125CD9FA785CBB5A0DC0BAE29875224F381F7021D6DF6923EBDA54A8E3AF23FA5B6F036A7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K?....._keyhttps://www.cloudflare.com/component---src-components-case-studies-templates-case-studies-template-tsx-9d44ecbafad4b038b911.js .http s://cloudflare.com/..c.%&/.....'.....C"XVe.T...."F../$.j.x51#.w~Fi...A..Eo.....z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\30624e5df392084a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	363
Entropy (8bit):	5.932249050344734
Encrypted:	false
SSDEEP:	6:msY2AKbHYVg3NRR3zBTfm+X/R1MmVFLygH1HK1N7YiK6t:eKbD4OD/HO7f
MD5:	223DC38E16A28ABC6697E15FD79A884A
SHA1:	B164586A1FBEA5F579E20705AA97DF5DCD2F3E77
SHA-256:	89A9730FC4793C8C85FDE1A71408FB76EA1D20CADA35ED0918E088AACECBEE70
SHA-512:	F5DBE4F0DEF7A8B94E293F4661C3A010B10E45013031CDB87C2234CA10E80D4ABC474FDBEA94B87027FEF0F7F2861D842C628581ABA167AEDA82F45CFAA41F 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://info.cloudflare.com/index.php/form/getForm?munchkinId=713-XSC-918&form=1649&url=https%3A%2F%2Fwww.cloudflare.com%2 Ftrademark%2F&callback=jQuery112406433527933138605_1626790814124&_=1626790814125 .https://cloudflare.com/@.$.%&/.....(.....qJ.*..=..s..G..... !...A..Eo.....*.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\31910c091738eab4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	52120
Entropy (8bit):	5.832905568486988
Encrypted:	false
SSDEEP:	768:hrq3G1253y4oKkm8jCjsJ3sSfQiTfGr2kLWrhdkLITVsjyJ1NinC:A3G125i5k8v3sS4iar8OLkVPYC
MD5:	81103F3F9218DC3DEB6A1FB31C3F4060
SHA1:	D585E3E702D32172166C15C49F04192240B59E20
SHA-256:	279C97C48A0BE640E57C3E09077D2339EBB366D0254F867B499A68058E309CB8
SHA-512:	B9B3722E2ECB9ED1413968BEED5AE625F81483AD12E4FEB4DEC903124B39B739FF61151566EFDB48A999AD9F8D3750F6507DB40ED7A915E9C1956587E11DED9D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x....nCC...._keyhttps://www.cloudflare.com/5e009dc030717571c643fcc1a1f8adeaa5c9aea9-d7bacc3e33dea420a560.js .https://cloudflare.com/....%&/..... ...~G3c.a6..I=#HY....%.<.T.H~(.w...A..Eo.....i?TF.....A..Eo.....'.....O.....S.1..... .....(S.]...`t.....].L`. .....Qc.j.J....window...(Q.....__LOADABLE_LOADED_CHUNKS__....Qb...m....push.....`.....L`.....`.....Ma.....`.....M...a.....Qb.R?y....+5j6C..Qb.h.2....+6jIC..Qb... K....+HlWC..QbR.....+NPkC..Qb.OV.....+OJBC..Qb.>.....+Pz5C..Qb.d.....+dcqC..Qbz.m.....+gcAC..Qb..OA....+v9gC..Qb...../+k/C..Qb...../UbjC..Qb..S..../W8uC..Qb..... ./apbC..Qb.{...../qNpC..Qb.HrD....0+iTC..Qb..;o....03A+C..Qb.P.....0BRoC..Qbr.....0KeIC..Qb.....0RbXC..Qb&.e.....0aKPC..Qb.d1.....0h9/C..Qb.....0mGVC..QbrV.4....12LyC..QbN.....1VtTC..Qb.6<....1mpwC..QbJ.X....1s4dC..Qb..P.....20u5C.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\321b4bc5e1cc0bf2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.642433143543354
Encrypted:	false
SSDEEP:	12:FYLrkEjqF9jzrPYLPtejqFCPYLyijqFST:uL9jojPwLVejVwLZjB
MD5:	7705B112D4B2F152672F95B5255C1BB9
SHA1:	E654743FEF0E9F67FCCF2D96A66BD612003F3940
SHA-256:	5A6DBCD23F5698093AB0430ABBED620F79FF34D7D0892B9B3204E1CE7B9F84A7
SHA-512:	1B5566039E855EA58E668AB5CE09339E3F547437EED75182F0A2E35DA058F95651765B9B3BCF2C65A747736D263A26867729345D0BAADD173DF8E9BECBF97855
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...I./...._keyhttps://assets.www.cloudflare.com/js/chunk-1560bda32b9d6d231e95.js .https://cloudflare.com/....%&/.....z.....(P...7.}.. 1i.....f..)9$.L.A. .Eo.....SFP.....A..Eo.....0\r..m....._...I./...._keyhttps://assets.www.cloudflare.com/js/chunk-1560bda32b9d6d231e95.js .https://cloudflare.com/=a..%&/..... .....(P...7.}.. 1i.....f..)9$.L.A..Eo.....o.....A..Eo.....0\r..m....._...I./...._keyhttps://assets.www.cloudflare.com/js/chunk-1560bda32b9d6d231e95.js .https://cloudflare.com/....%&/.....L&.....(P...7.}.. 1i.....f..)9$.L.A..Eo.....r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\33a8355209af0d89_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.645709722025089
Encrypted:	false
SSDEEP:	6:mYjQXYcvG3vcDOADugfMTgrQK6tWYjQXYcvG3vcDmtngbBMTgrUEbK6tWYjQXYc+:FRKO5TJPRKMTzENPRK52Tn
MD5:	28D70B9FF2DED046214D694512376246
SHA1:	842C7F723CCF6D7A9D66B44C8A47316C5B0BAB4E
SHA-256:	EE40B90A97BEB5B14169EA8200569E807CEEF71F48303B77B1D615C4F3B65429
SHA-512:	5607D08A6BCDE815921D3E67598C51F63591A389CA878C6A8EB092996065E859AE54C94609585EE33E4F609B170319063F98715C283EBB6CD6D85C26175BD2CE
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....n.u...._keyhttps://assets.www.cloudflare.com/js/chunk-55d37f7935d3778f0709.js .https://cloudflare.com/....%&/.....:...../.....R...(.....A..Eo..... .....A..Eo.....0\r..m....._....n.u...._keyhttps://assets.www.cloudflare.com/js/chunk-55d37f7935d3778f0709.js .https://cloudflare.com/....%&/.....>.....:..... ./.....R...(.....A..Eo.....\.....A..Eo.....0\r..m....._....n.u...._keyhttps://assets.www.cloudflare.com/js/chunk-55d37f7935d3778f0709.js .https://cloudflare.com/jW..%&/.....y'.....:...../.....R...(.....A..Eo.....".P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\36436e71f619b2fa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6753
Entropy (8bit):	6.24811951036848
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\36436e71f619b2fa_0

SSDEEP:	192:/31OGwnLw87xqin7mMIgasLFtKoM+EhAoCkoCyC3v:/5c5t7mBgfFtVMvCkoCjf
MD5:	E20119539CC7A7E959E06EFCFA0893A0
SHA1:	05395C36E30EE5CACF3F8DF17FB55307F6FB6D75
SHA-256:	BE3F2C38F9FF720EB58608E3AC83FE62C7B4BF7DEE4973041504710450A52D9E
SHA-512:	2E9BC5E03530FA69646019D9A22EA42985FE4F318231195FC5D9116503BD0F95E6D8946616AAEB30B68F0337195459B0B1415BE56309EB53121FF6E7D6CAAE3C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y.....e...._keyhttps://www.cloudflare.com/framework-a37fee216cd2ef2ee260.js .https://cloudflare.com/...%&/.....aX.v....f.G.8h.!..-.....4._.A..Eo.....z.....A..Eo.....'.....O.....(S....`.....dL`.....Qc.j.J....window...(Q.....__LOADABLE_LOADED_CHUNKS__....Qb...m....push.....`..L`.....`.....Ma....F...`.....T..a&.....Qb..k.....+wdcC..QbF!.....16AlC..Qb.f.....17x9C..Qb...y....QCnbC..Qb...:....WbBGC..Qb..g....i8i4C..Qbvx.8....q1tlC..Qb.....viR OC..Qb..\y....yl30C.(S.....Pd.....push.+wdc...a.....@. .#..@.#.$..@.$.%..@...~...*.....d.....$.%..@.(.....1.E.@.-....HP.....<...https://www.cloudflare.com/framework-a37fe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\368dad393f6af4f0_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.6301008667348045
Encrypted:	false
SSDEEP:	12:FZXG8LDxOhzePZXG8UxOhzbGPZXG8s+2vxOhz/7:TtROIhtWOJGhtxyOF7
MD5:	E215B2A35ED1C11A096B5335722AF355
SHA1:	F9FD218E5FDA40D8870DDE275B29739B9825E069
SHA-256:	54A45135737AB939117EB8DE01BF8B58607C621E86890586C543EE03B04225F2
SHA-512:	9D7163859922073B19828BB949E04FAA8FE39706699BE92F3BA5459EA6F5E98B6DED0C235D377D8CF37F5E0F47D45685F6C051BF1F53DDF63CE09A984E3249BD
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....`._keyhttps://assets.www.cloudflare.com/js/chunk-5d677ef1b4eeb74635d3.js .https://cloudflare.com/A...%&/.....=.....L..E+c..t.H.M{3.t.u.....u....A..Eo.....M.....A..Eo.....0\r..m....._.....`._keyhttps://assets.www.cloudflare.com/js/chunk-5d677ef1b4eeb74635d3.js .https://cloudflare.com/....%&/.....E.....L..E+c..t.H.M{3.t.u.....u....A..Eo...../|;.....A..Eo.....0\r..m....._.....`._keyhttps://assets.www.cloudflare.com/js/chunk-5d677ef1b4eeb74635d3.js .https://cloudflare.com/....%&/.....}'.....L..E+c..t.H.M{3.t.u.....u....A..Eo.....!.W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\40c2219e5f5a1e88_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.947424348348431
Encrypted:	false
SSDEEP:	6:mMqVYGL1KQGFgsA6piJhUx4QnK6tNAVN0LRm67jy6piJhUx4K/:XnJ1pAhUxT/QNZ67jjpAhUxF
MD5:	80B6DD9B166D0B919B9B323A5F3AA6A5
SHA1:	84F309C9DC56BA2EFDF08AA3DB2AD15938504197
SHA-256:	F85568AAF8BC674B4A1049684A20FE4F495CC39D8093FD16440E14AE99C34CBC
SHA-512:	86E4B344BA81A8F7E7911C107B70F5C557FAEBAD08FA2DED79DC8675151F0315F28C05B1C28185BFE24D9B1E88DA0625597C33DB8EFC6F0E0677126EB101F58E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q.....]...._keyhttps://www.cloudflare.com/compiledNav/navigation.js .https://cloudflare.com/U...%&/.....x[..o..m".,..&..K&Ro..F^...n.w./.A..Eo.....4.....A..Eo.....U...%&/.@X..3FD3A4C060587D5FE840F9E315E2B068D55241F215CA375C2B4FD2AE396E9267x[..o..m".,..&..K&Ro..F^...n.w./.A..Eo.....K.}'L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\462ff694af2c9745_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1837
Entropy (8bit):	5.526946386809577
Encrypted:	false
SSDEEP:	24:c7G8xFlpylJuV7UBerdddZ6OVef9qQ4ZFCyPaYGLdw8W/7WnNG3g2rxUddKB8fux:bKF/yiUBNqQ4ZF5gdWyJdKB8fToQF+
MD5:	0CD27397BA42A897A6516F1BC36700D9
SHA1:	0F3D8DB34633A639A59A4CEE841CA0D9279CB710
SHA-256:	4916B39023FF8DF206E80833B187E51AC9DBD68C02B164992052574676991818
SHA-512:	A1AF8E61BA7354CCEAF961976DFD8060856024F68DE4F6C30CA4A4C96A6308C069D5ABEB10ABD02335E3F40CFE903ABCD92692D44013802920378947 3DB7BF1A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\462ff694af2c9745_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E....v.:...._keyhttps://munchkin.marketo.net/munchkin.js .https://cloudflare.com/L...%&/.....L.....4...8.5h.....0..<..K".y...*..A..Eo.....|e.y.....A..Eo.....L...%&/. .....'.....O.....0.....(S.4..`$....L`.....(S...`.....@L`.....pRc4.....O…Qbz'.....c.....Qb.....e.....Qb..tk....k.....Qb.:.$....l.....Qb..{.....m.....Qb.....n.....Qb.q.@....h...h$.....I`....Da.....Q.@.u.....Munchkin..Qc...W....document....a.....y...Qb.....160..(S.....a=.....@.-....4P.....(...https://munchkin.marketo.net/munchkin.jsa.....D`....D`....D`.....(...`....&...&....&....&.(S.....a.....d.....d.....D&.(S.....Pc.....h.init..a:...N.....QbB VJ<....init..d.....&.(S.D..`@.....L`.....4Rc.....O.`$.....Qb.r.....p...`.....q.a.....(S.....Pd.....h.<computed>ar.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4c76748133762fdf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2832
Entropy (8bit):	5.497736012566581
Encrypted:	false
SSDEEP:	48:v7sdrtT/r6+nStVjGihH8FFGMwBvk+ht4BNJJ2fjQEVo/sEl5xngMEJo:v7cxTJnSqY8+MwBMatWJ9/ffSo
MD5:	4B6D6436B006D823BCD49CADA6655605
SHA1:	E8809D8F6FAF3E28675A7A45BBF1206F0A482726
SHA-256:	7338D4C4A83882FA246BD287AD13059DD67E2B871666F58DDD59A832E3E1E4BB
SHA-512:	697BAA5DBC5E7DE31EEF5605E81738E3E2D0C8B8F2AA7A70847B40D96E91711710FCED8A516FE64902CA625D34E39EC87CE8EA28F32B7F74F4A334AD60050B0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x....uJ....._keyhttps://www.cloudflare.com/afce47c9ba5426869dbc5a926461a546e054f2e1-f00f87555f2a2eb1ac9a.js .https://cloudflare.com/.}..%&/.....g. [.%..(7....Yw.f.....?...A..Eo.....U~~.....A..Eo.....}..%&/.....'.tW....O.....(S...`N.....L`>.....Qc.j.J....window...(Q.....__LOADABLE_LOADED_CHUNKS__....Qb...m....push.....`.....L`.....`.....Ma.....`.....t..a6.....Qb.r.....4vICC..QbF.2.....88oqC..Qb.....JRpuC..Qb^T0A....MEMKC..Qb~70;....QIyFC..QbnC.....TO8rC..Qb.I~.....Xx1rC..Qb2.....bFg/C..Qb..,.....eCMqC..Qb.g.!....iJ1OC..Qb..W....jXQHC..Qb.....sEfCC..QbB.L.....tLB3C.(S.....Pd.....push .4vIC…ad...*.....E.@.-....hP.....[...https://www.cloudflare.com/afce47c9ba5426869dbc5a926461a546e054f2e1-f00f87555f2a2eb1ac9a.js.a.....D`....D`$...D`.....`. ...&...&.....D&.(S.....Pd.....push.88oq...a:...C.....E..1.d.....&.(S.....Pd.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4e292f0da84a8806_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5552
Entropy (8bit):	5.608925415765911
Encrypted:	false
SSDEEP:	96:upAKXNVb2PBTtL8ItRlep9M/S6iFuEjb++ukDnyLh1Uxwjn/ftxCL6:kdvbYpV8Itj4eajbty+wjnt8G
MD5:	8886D9D9D692AF6EF5DA005AA93E3997
SHA1:	28E63C363DFD8363D543D49297087D98F204DB4E
SHA-256:	1F9B009FF7E165548E13DC8A1F021DDDB098E7A905363826059CBAAAE47C42F9
SHA-512:	B0F236B66935C75553641D07D877B7E45E4F7DC490350E6D18DB03288C8ED8FE4806A05AC54B8AE82805454986444FD143179A7B483CC6C92CB36C94934448D4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x.....K...._keyhttps://www.cloudflare.com/ac9eeed4e6d0e0162060928fa2fbb56350368406-996346b0d397c6efbf45.js .https://cloudflare.com/....%&/.....^wY...4`A.....bdc.w...?...2s..A..Eo.....!-.....A..Eo.....'.....O.....(.....(S.-...`.....L`n.....Qc.j.J....window...(Q.....__LOADABLE_LOADED_CHUNKS__....Qb...m....push.....`.....L`.....`.....Ma.....`.....af.....Qb.h.....10d8C..Qb.....1CCGC..Qbz..+....6DAAC..Qb.@.....CXhCC..Qb.....FQCyC..Qb~cfb....LZbMC..Qb6$\L....RJeWC..Qb.....SjEeC..Qb..q....Us+FC..Qb63&"....VGX7C..Qb>2.....WA8BC..Qb..O.....a2DFC..QbFF!M....cPJVC..Qb..WO. ...csjhC..Qb:.C.....fupuC..Qb..''6....gfz1C..Qb.....iWRJC..Qbf.;.....iowuC..Qb*.....kOWhC..QbJ+.....mwIZC..Qb..M.....pLeSC..Qb..Q.....pzWdC..Qb..L.....tMf1C..Qb...'... .x84WC..QbF.,.....yNUOC.(S.....Pd.....push.10d8...ad.....Q.....@.....@.....@.....@.....@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\509801de2644843d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.5489734383842935
Encrypted:	false
SSDEEP:	12:F2t1VycPXCzP2t1V2hPXCu71P2t1V3QPXCY:Et1VycYOt1VEz71Ot1VAr
MD5:	DD0DCF3974823B2097F710966CDF7311
SHA1:	8118E3CB5F07EF003AABB0CB508718FD1E710D75
SHA-256:	81431C8E0CC7FA95E90853BFF0CFBC2A5412AA15ACD896CE0397043DBC83ED2E
SHA-512:	D27B2A1D991909B0D4BB4D4E46B6CA072F9C64AC9CF1C5BF91B406232974BDFEC66B46317023CA58F27DA993611F6BC58AC4A8547C0D22CD8E76D9DD2CA1BF7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\509801de2644843d_0	
Preview:	0\r..m....._...b..Y...._keyhttps://assets.www.cloudflare.com/js/chunk-e50bafad0559f7d0a0f0.js .https://cloudflare.com/}...%&/.....%"....B..p.w....7V.....3.....A ..Eo.....i.....A..Eo.....0\r..m....._...b..Y...._keyhttps://assets.www.cloudflare.com/js/chunk-e50bafad0559f7d0a0f0.js .https://cloudflare.com/....%&/.....;.... ...%"....B..p.w....7V.....3.....A..Eo.....y.....A..Eo.....0\r..m....._...b..Y...._keyhttps://assets.www.cloudflare.com/js/chunk-e50bafad0559f7d0a0f0.js .https://clo udflare.com/.Z..%&/.....w'.....%"....B..p.w....7V.....3.....A..Eo.....V..i.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\58b307e504086606_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6745
Entropy (8bit):	5.75534079444132
Encrypted:	false
SSDEEP:	192:z8S1YlDmLETdKTVUl4eDI0BjxJ+2KMugtwEBHV:QS1Ylegd4VPe80h+stjtV
MD5:	206884008672F99E5FEE759C34D4861C
SHA1:	39175B64A19921A26334DBA4D30CD436D522931C
SHA-256:	78E0A919A2E231A7F6923C826B58443D85897B8D4E9045F580549BA2C3EEAE32
SHA-512:	04F7BA1CD1607F2BF0143A67C8EA4DE73ACBE8AB529D1E39EBE4F9F4604B15B8782DFE50FE11E66C69995370FF56A6609ADB4B5C78E8C25AD6167C47E31F00I 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...9|....._keyhttps://munchkin.marketo.net/160/munchkin.js .https://cloudflare.com/;..%&/.....t..lEW...0j}..7...'T..o.6.C_..A..Eo.....9g.....A..Eo.... .....'.f+....O.....(S.4..`$.....L`.....(S.Y..`j.....L`x....q.Rc.....R.....Qb.q.@....h.....Qb.:.$....l.....QbJ.\....q.....Qb.<.(....D.....Qb.w.E.. ..A.....R....Qb^:.....t.....Qb..e.....E.....Qbj.o.....x.....Qb.....F.....Qb.....v.....Qb.v.C....V.....Qbnn.....f.....Qb.....G.....Qb>.G.....W.....Qb:V.2....r.....Qb.f&=....H.....Qb..M.....I... ..Qb.....J.....Qbz..V....K.....QbJ0."....L.....Qb..O....y.....Qb.....e.....Qb..{.....m.....Qb.r.....p.....Qb.6.....X.....QbV.....B.....Qb.S.....C.....Qb.@9.....M.....Qb..pZ....Y.....Qb.13.... .Q.....Qb>.H.....Z.....Qb..jg....R.....Qb^.....w.....Qb.-.....S.....Qb.....z.....Qb.....T.....Qb..s....N.....Qb.....U.....Qb.e.<....O.....$.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6527596934c8107b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5312
Entropy (8bit):	5.305267777071977
Encrypted:	false
SSDEEP:	96:dqsoOTJsVWKDcreXBEwdYapfh7zkYDmf/fSMVlh:dqsoONsVWKDcQndpVzgNlh
MD5:	AA81042B8C2C5FD2AB5A581F15D0B071
SHA1:	386A915E9953B562636DF27ED8AE4C1A0D17F373
SHA-256:	E58C5ABF02B65CD68B75D6A6CAA45EE9AE1F269468FD5E24C73827E8DBFC9D0D
SHA-512:	098605C2336C0502986819AECBA036AB049A4E179079F792A28BD2E11999A6DD9598CD529C374900DFACF87675BD96DE43C2CF1BDBA6AEC94BB5ABEED5B5C3 88
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...d....._keyhttps://www.cloudflare.com/0d625897b26b36d368c45fce14325a7ae0ab1d92-a57847f1d12b4b9c26be.js .https://cloudflare.com/$...%&/..... .....p/Q...."....G..H..L.P.H...A..Eo.....w.....A..Eo.....'.....O.... ...&;.....d.....(S.u...`.....-.L`.....Qc.j.J....window...(Q.....__LO ADABLE_LOADED_CHUNKS__....Qb...m....push.....`.....L`.....`.....Ma.....`.....a.....Qb.....+6XXC..Qb...h..../9aaC..Qb.@t....44DsC..Qb".#.....4kukC..Qb.X B....4uTwC..QbR.....9NapC..Qb&}V>....9ggGC..Qb.^~.....EpBkC..Qb..e.....GNiMC..QbN.....H8j4C..QbV.A}....HvziC..Qbr.....I01JC..Qb.a.....JHgLC..Qb..k.....JS QUC..Qb.w.....KMkdC..Qb.1.....QkVEC..Qb.YU(....SfRMC..Qbr.....Xi7eC..Qb.7.....YESwC..QbZS.....Z8oCC..Qb...W....ZWtOC..Qb~.U.....adU4C..Qb~.fp....dt0zC..Qbv. .....e4NcC..Qb.F.....eUghC..Qbzm.....ekgIC..Qbn.....fGT3C..QbB.....k+1rC..Qbb.....ljhNC..Qbb."....pSRYC..Qb..+$..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\723e13dfdf85457a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.864044905885746
Encrypted:	false
SSDEEP:	6:muNYGLHKiWPURmILV6qWtgEMGKJD4uRK6tZjVwOfH0V0o+MGKJD4Tll:bxK5PUR/wqWMGKJDBrTGOfHs0o+MGKJD
MD5:	A93CB8A07CCDF6E3082CA03858EC02EE
SHA1:	A6E65FF54A31A4FD82B830FCD06701CCB3E83E03
SHA-256:	E15162B53B7D480D5D5DEABE61869B77E07682A811B8641F54E3692AABE2C4CE
SHA-512:	0D0BB18D53867FC873D46680F10697CAAEEA0A87E5C10A951F3F121ED2D579879EFD443D9C4756FD889A0D8CAB1E537E38EA1727C00D0874E183F61159781DD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...#6....._keyhttps://www.cloudflare.com/vendor/onetrust/scripttemplates/6.8.0/otBannerSdk.js .https://cloudflare.com/....%&/.....g.>...P;..hC+pW.W.B8. {e(...2..A..Eo.....k.....A..Eo.....%&/.`...632CCF83066B6D902D093E184EA7E6298731C01624806D6B2314CA305C5FBC86..g.>...P;..hC+pW.W.B8.{e(...2..A..Eo.....m.VL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73fffadacae25d8a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.594449159220719
Encrypted:	false
SSDEEP:	12:F/PTNNtOmuP/PTNRptOm//7P/PTNJltOL:hRNtNuHRRpt/7HRJltS
MD5:	5083E6A07CB4AA7AF326D8DBD868CFD1
SHA1:	8BDAF1712C1FE39254F34053DCE37AEA14C8EB89
SHA-256:	3428431E7437FD302C8AEC4DC771EF876C844BF743B8E7267C269A99B7E72D59
SHA-512:	8414194699E5C4253C7E85B273629F5614BBC78398C21960DCA110B88B61E6FAD560F54B71B132C0B97EB725180FE6B2E3FA5DEC28511ACDDE3FA1C3246746A
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....\.s...._keyhttps://assets.www.cloudflare.com/js/chunk-01f71c423e068664057e.js .https://cloudflare.com/j...%&/.....s.....e}.C8..f..C1...Mk.c..t....^.A..Eo.....v.....A..Eo.....0\r..m....._....\.s...._keyhttps://assets.www.cloudflare.com/js/chunk-01f71c423e068664057e.js .https://cloudflare.com/.\..%&/.....e}.C8..f..C1...Mk.c..t....^.A..Eo.....A..Eo.....0\r..m....._....\.s...._keyhttps://assets.www.cloudflare.com/js/chunk-01f71c423e068664057e.js .https://cloudflare.com/U...%&/.....G&.....e}.C8..f..C1...Mk.c..t....^.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\74e8f9a2a1a9c3e1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	364
Entropy (8bit):	5.906961389323838
Encrypted:	false
SSDEEP:	6:m+uXY2AKbHYVg3NRR3zfVm+XxyHBigZ0Cym0qUpr9hK6t:UQKbD0EyHBvj0qOx7
MD5:	AB70C9766CCE40835CE9A5DAF4A6CA37
SHA1:	F1F3A12309B58B95EA1A57B250E14AF8371BC529
SHA-256:	8068AE39722DB0413CDBDF7109B14CFEC41C82F87484B921FC623FA916C67F75
SHA-512:	0475B28D75684F62FC2A1091276870094E610F4CC369A341692C8B68DDEC6B599B424EB3905FB8400B9309248DD2DCFBF2B986A3414713E920E7B611718FB196
Malicious:	false
Reputation:	low
Preview:	0\r..m.....#...._keyhttps://info.cloudflare.com/index.php/form/getForm?munchkinId=713-XSC-918&form=1649&url=https%3A%2F%2Fwww.cloudflare.com%2Fdisclosure%2F&callback=jQuery112408671637525847358_1626790809680&_=1626790809681 .https://cloudflare.com/.m..%&/.....1..C.....PB.S.Q.:.p.....A..Eo.....\1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\77bae649a8ae54c2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.63001123054348
Encrypted:	false
SSDEEP:	12:Fsd0pjluq7mk8qPsd0yAQq7mk8Tn1Psd0eq7mk8Ar:qd0pjlBf8q0d0TXf8L10d0xf8Ar
MD5:	3225C3AF7D58A539D62ADD8F9531C9A4
SHA1:	A5E2478282F1C3950EA68951A886C51B6D9EC04F
SHA-256:	DDC1B21D17BEA0ECDC3C1B425699247FFC25B3A4C03EE4A0059A2B108C8E86A2
SHA-512:	F1C61940E2FF105AC022DA6339B90E941EB5C5526FBE4EE556B481FF388930981F4F3697769463AF992D82CE5F4A10192BD0B1C897544CA43995301FB1D4D98C
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...{.F....._keyhttps://assets.www.cloudflare.com/js/chunk-cd8895b507ee9e702e17.js .https://cloudflare.com/....%&/.....`.....U.....d..1q./y..u.w....%.....A..Eo.....L.....A..Eo.....0\r..m....._...{.F....._keyhttps://assets.www.cloudflare.com/js/chunk-cd8895b507ee9e702e17.js .https://cloudflare.com/._..%&/.....U.....d..1q./y..u.w....%.....A..Eo....."".....A..Eo.....0\r..m....._...{.F....._keyhttps://assets.www.cloudflare.com/js/chunk-cd8895b507ee9e702e17.js .https://cloudflare.com/-...%&/.....*&.....U.....d..1q./y..u.w....%.....A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d34d7942ee0ee97_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16648
Entropy (8bit):	5.753986195598043
Encrypted:	false
SSDEEP:	384:yAXIqTl0Rs6yl1iJga6Qn3v9hoW0sHYBuLt2EXv0qoPwTCEEki+:yQIqTl0+JaWQnkiH1t9Tsi
MD5:	237C60B511C63372D0DF10B1369FFC6D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d34d7942ee0ee97_0	
SHA1:	95259832E3C27F1B958636C173DE3A5B0D231D0D
SHA-256:	ED7B28A80471878C1DB9653CBB853314D2F20705433AA135DEFAEB17282EC071
SHA-512:	BADEC05B22B5B4F19347B11B7EDABE531CB4681AD30D02321D45D751FB8B65BD183BF2FC4C369925FC57D5789C76BEA2E0DD2E50BA52187A9A1486BD0CA7A9C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P.....Y...._keyhttps://static.cloudflareinsights.com/beacon.min.js .https://cloudflare.com/.-..%&/.....c.....".....!..Ne....--g.d..../.9..A..Eo.....+.....A..Eo.....'..5....O.....?...`.{.....D.....(S....`....,L`....(S...`....<L`.....@Rc.....Qb.....e.....Qb.tB.....t.....Qb..C.....n...b$.....I`....Da.....(S..`.....L`.....Qc..H.....exports..$..a.....S.C..Qb2..s....I...H..A....a.....Qb.Q.....call..!...K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da....&.....A.....e..... P.....@....@.-....@P.....3...https://static.cloudflareinsights.com/beacon.min.js.a.....D`....D`D...D`.....`....&...&....&....&.(S.....Pb.....t.d.a.....I.....d.....&.(S.....Pb.....t.n.a....v.....e..... I..A..d...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\856d1204b1f6e469_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9080
Entropy (8bit):	5.321209889840036
Encrypted:	false
SSDEEP:	192:QSvGSSZYqBtBJyWG61GmIFk8jL29nKHHkVcTxBWdZyr:QycZrXry3m+jSkBTWdZq
MD5:	59601ADAF6A85ADDD19956D21F05179B
SHA1:	E197172187675891B218719F5297B3D0E9340654
SHA-256:	F327174D20307872006902580CA811A94B81D6AEF95A6060ECEB81D3B2425989
SHA-512:	C8D9C3E2D0561CA374C74D717FB429B410B8CCA04895ABA6DF553055DD56EEA267E9493435EFB1D3A67B4F9FB3CEC08AB7A682DFA8D5162A523FE97EC18BA28
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x....I....._keyhttps://www.cloudflare.com/4b2a42a93029629026b3b5bf51209ba1171ffdfd-1f5b96576ed0703e6889.js .https://cloudflare.com/5...%&/.....NhQ.._B...i)...V$.1..Z.....A..Eo.....~.1.....A..Eo.....'..B....O....!.....+.....(S.]...`n.....L`.....Qc.j.J....window...(Q.....__LOADABLE_LOADED_CHUNKS__....Qb...m....push.....`.....L`.....`.....Ma.....`.....a.....Qb.....+K+bC..Qb..#.....+iFOC..Qb..[H....0Cz8C..Qb.....0ycAC..Qbv.8~....1+5iC..Qb.]R.....1VvMC..Qb..).....4Oe1C..Qb...5....5Tg0C..Qb.}.+....77ZsC..Qb...3....7GkXC..Qb.T.....7Ix3C..Qb.....88GuC..Qb.....Dw+GC..QbBO.....EEGqC..Qb6.....G6z8C..Qb.....Gi0AC..Qbj.....IoaoC..Qb.b.)....JHRdC..QbB.p.....KxBFC..Qb&.G.....L8xAC..Qbr t.....LXxWC..Qb6.....LcsWC..Qbb..<....MrPdC..QbB.....MvSzC..Qbj.....O0oSC..Qb.=.....OBhPC..Qb.....PuqeC..Qb6.e@....Q1l4C..Qb.E.....QcOeC..Qb~8|.....RBanC..Qb.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86ef09a943d02485_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.672280026789836
Encrypted:	false
SSDEEP:	6:mYYYcvGTNRVrMpgRJ1sPnH4N9K6tWYYYcvGTNRVrWtmugF1sPnH4z5lDK6tWYYY1:FxVrPwPHiPxVrWnPHi1PxVrS6IPH8
MD5:	AC94B65CE6117562E5497CA66894E1CE
SHA1:	9C4A1CC32A7629D86540205FB0F64E4507D0D457
SHA-256:	1EC24FE5FF4000EE7144545CFE4CBE6DCF494938E212AEF9453AE40FAFC2195F
SHA-512:	48D42A1E755900EE86847FF4C23D1CFDF3CB60BA959A6FC1C05E792A7E56F720664E171F964BAF6D2BEBB0199C08D417F193E06DB20581EA7500BE0B893AE6F8
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...8;...._keyhttps://assets.www.cloudflare.com/js/chunk-3125ea56e87c986b133e.js .https://cloudflare.com/....%&/.....7.^..g.L*._.b=9..D_...f.."....A..Eo.....#.....A..Eo.....0\r..m....._...8;...._keyhttps://assets.www.cloudflare.com/js/chunk-3125ea56e87c986b133e.js .https://cloudflare.com/...%&/.....7.^..g.L*._.b=9..D_...f.."....A..Eo.....U.....A..Eo.....0\r..m....._...8;...._keyhttps://assets.www.cloudflare.com/js/chunk-3125ea56e87c986b133e.js .https://cloudflare.com/....%&/.....'.....7.^..g.L*._.b=9..D_...f.."....A..Eo.....E.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3dbefcef26296d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78744
Entropy (8bit):	5.573600066121333
Encrypted:	false
SSDEEP:	1536:Wml5Nvg9/QgNeROcX8gNGO54Vs3/18uc0T0e6WyUQi:V+LkM1OSiilEyUJ
MD5:	0CD652198C2F1B78FA4DA36FFF6E3487
SHA1:	7B5D2C6732F0BDCD2E90F1B3A4CC116A8E895FCD
SHA-256:	B1B1A4CBEE074F14E8E887E871B7E54D7908C4DD588F7799F507B753F51624C2
SHA-512:	17F2F07C449F59739CBC837793DC5A53731637C18419A1982263971F0ED2C237464B8DF9A2028F765C7E585AD2C96533E0F87207DA82D1FB21A98C5FB9ECD7A6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3dbefcef26296d_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....CX....907AE4693EF1998A704E747DE82824C24765F4C91459C149949B6937A907302C.....'./.....O....X2.....T.....$.....T...D#.....(S....`.....L`N.....Qc.j.J....window...(Q.....__LOADABLE_LOADED_CHUNKS__....Qb...m....push.....`.....L`.....`.....Ma.....`.....aF.....Qbj.....05SNC..Qb.da*....1F66C..Qb..W.....3V46C..QbJ.%`....5WrjC..Qb.....8NNaC..Qb.....BOyCC..Qb2.X.....NmYnC..QbB.....QSxFC..Qb.....T+oqC..Qb.nRA....W4OWC..Qb.^.....WfpQC..Qb.....ZFRsC..Qbn..|....bT6jC..Qb.....dfCWC..Qbn..g....vDUPC..QbB.....vrmYC..Qbb8=.....x/+mC.(S.T.``.... L`.....e...Qdf|.....__esModule.....a.....G.a..(S.....Qb.Tou....r...a.....q.\.@.-....hP.....[...https://www.cloudflare.com/78ea267daafe81328bdca4e600e3c86b21c254f4-565aff763e8d9fd664bd.js.a.....D`....D`....D`.....`....&...&..q.&....D&.(S...9...`&.....L`L.....RcL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f460b3eded3029f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.562499539963143
Encrypted:	false
SSDEEP:	3:m+lS16lldA8RzYrSL64BLbUEKfQUsL7PLBDNm/lHCmkltRiWZ5nszNDXhm5m61xB:mo9YGL1B/7lrLDagmklthsz9Rm4aK6t
MD5:	E3323D8DD3A0F7BC5F76BDBE32E74054
SHA1:	C6A373CCDCAB043F678091F73CE3CB04A63AF9D7
SHA-256:	6C46FD88D9CB13B6DADA43FE5A68C462F580930A54AC61BE6B6F71F6D373F47B
SHA-512:	8F1A483ED8E7B5A639FC8E144F4BA1E02AD94FEEC60F0F0C2B7A0CA1043E6F6BCE44F39127DB60BDDEA7F7E63E7674BBFFDCFFED5A4D83822AFEE02A7C5D8DA0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://www.cloudflare.com/cdn-cgi/bm/cv/669835187/api.js .https://cloudflare.com/d...%&/.....Q{G'p|9lb.d..l..1.....D.....0.A..Eo.....;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99e650ddc603eeab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19652
Entropy (8bit):	6.146477633305951
Encrypted:	false
SSDEEP:	384:WgFu5E6BwlS6aJpmVij32jB04Zjmcx9LqSWyfn+:rFup7pURp5f+M/+
MD5:	5BB3476220878E1E4A6AD8949FA96BB5
SHA1:	4AD9F77532EE70D81B8BA5CE063F7E5B6BEE06A0
SHA-256:	D6C3C56BE2818A6677995AF037B9623DF75BE064863FDF9A8E4B9EE56B0ECC32
SHA-512:	0B90E8018F27B09520C7735FDE72093A468EE89DB07A517995DCCC2C14A633C7AFE262135C1B1C203A19F87DEC48A0F3D21290A6ADC0792FE4BBFB896C4175CA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....8L....._keyhttps://www.cloudflare.com/vendor/onetrust/scripttemplates/otSDKStub.js .https://cloudflare.com/....%&/.....h.....Ved...ha.I..U.q..W.....&S..mN.A..Eo.....m.....A..Eo.....'..C....O....(K..P.X.....(S.@..`<....L`.....L`.....Qd. .....OneTrustStub.(S....`:.....L`J....@Rc.....Qb..%.....ee....Qb.$N....te....Qbnl.B....oe..b.....I`....Da2.....(S...`.....L`B....8Rc.....Qbz.%C....c...a.....Qbn.....ae..`....DaXa..\|.....(..QcB..N....iabType...Qd.0.Q....iabTypeAdded..Qd.qs.....crossOrigin...Qc.....isAmp...I..Qc..AG....domainId..Qc.=+(....isReset...Qd>.....isPreview.....Qd2:.....geoFromUrl...(S..... Qff4.2....addBannerSDKScript..ak1...7.....d.....i.j..@..@..I...0.@.-....TP.A.....G...https://www.cloudflare.com/vendor/onetrust/scripttemplates/otSDKStub.js.a.....D`....D`$...D`.....`v...&...&....&.(S....`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9f6eb263354d9328_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.45536360090909
Encrypted:	false
SSDEEP:	3:m+lQ9pl08RzoKTAyGXdB/UEKfQUsL7mdKTAyGXCD+1t/lHClXPlvN9vRmg1XXlpD:m/xXkdT/7lrLaIkdNg3vAwTK6t
MD5:	66434BE7F3D3B76BFF8847CD999ADD56
SHA1:	EA4F7AAC948549E921AEFBD216796EAD5007E569
SHA-256:	E73FFDE291DE15FE3FA56AC65B9702B2DC0B8CFDF4C39D6188CF20A76401C2ED
SHA-512:	7D30939A0640362EB18AB61C8239A8240A6D2F61D122A1569014E10BF02E6E9201620DFFB62AE3CADDB6797ED0EDB7DAE278E44021C3E246E18AC453A9CDFC5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....._keyhttp://covid-19.in.th/cdn-cgi/bm/cv/669835187/api.js .http://covid-19.in.th/....%&/.....|....._....r.\...]/i%..W$oo .ja'+.[..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a156729f543b6d56_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1421
Entropy (8bit):	5.60232703212801
Encrypted:	false
SSDEEP:	24:TRyvTZRyXC+ZRyIa5ZRyfcZRyiEQPZRyCLXQ/NZRy8w:TR8TZRh+ZR5a5ZR8cZRJPZRjQ1ZRHw
MD5:	C1FBE56D21EACA6B8494F782D2334A11
SHA1:	8AA5626E3A3BB522294B91DF365F7DF1C80C8024
SHA-256:	8464A221A62F471FD5DA6D8C684759A98C521421BC04101D92634B956B9F5B1D
SHA-512:	878C35ED53CA915F5179211252D0600F8E5EA140E0AA45684E1AA816BD0AEFC72541C67E2AFF76E6BAD3D784266FAE63BF46E99437A5AE65CD94A3BEC9C5182B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G...8."....._keyhttps://tr.www.cloudflare.com/analytics.js .https://cloudflare.com/M.F.%&/.....V.....XI..M-H..:.K..'b..=.A..Eo.....hK.v.....A..Eo..... .0\r..m.....G...8."....._keyhttps://tr.www.cloudflare.com/analytics.js .https://cloudflare.com/.I..%&/.....F.....XI..M-H..:.K..'b..=.A..Eo.....bh.....A..Eo..... ..0\r..m.....G...8."....._keyhttps://tr.www.cloudflare.com/analytics.js .https://cloudflare.com/.V..%&/.....XI..M-H..:.K..'b..=.A..Eo.....*.....A..Eo..... ..0\r..m.....G...8."....._keyhttps://tr.www.cloudflare.com/analytics.js .https://cloudflare.com/..9.%&/.....XI..M-H..:.K..'b..=.A..Eo.....7.....A..Eo..... ...0\r..m.....G...8."....._keyhttps://tr.www.cloudflare.com/analytics.js .https://cloudflare.com/mju.%&/.....XI..M-H..:.K..'b..=.A..Eo.....S.....A..Eo...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a92f690aa7e5682e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.587615679218894
Encrypted:	false
SSDEEP:	12:FGgcBMaZ6KwPGgcBMMtMKnrPGgcBMOTKG:dhxnM6qrnOTb
MD5:	4702EB7615DEF13B0C7C8E5C8522EBFA
SHA1:	BF17D1BA915B436EC7052582DA1023A1E0CDB318
SHA-256:	1897F35339D6A89A3B6176A39A4509173CD32888CFCDD77BBBA5244E2055DB84
SHA-512:	4F497D4FAE4FA935670DE6EE362658814FEAFFDEB787BD15CD9999FD7387415E116A6A3946C7F87A73204C78EAC357360A5767FEF5EAAA445B08BBF9188B92ED
Malicious:	false
Reputation:	low
Preview:	0\r..m....._..........._keyhttps://assets.www.cloudflare.com/js/chunk-e06d79a8c06c0d46865a.js .https://cloudflare.com/....%&/.....3.....rt\j.-f.....H....MQ..f...OSf.A.. Eo.....A..Eo.....0\r..m....._..........._keyhttps://assets.www.cloudflare.com/js/chunk-e06d79a8c06c0d46865a.js .https://cloudflare.com/.S..%&/.....y..... .rt\j.-f.....H....MQ..f...OSf.A..Eo.....m.,.....A..Eo.....0\r..m....._..........._keyhttps://assets.www.cloudflare.com/js/chunk-e06d79a8c06c0d46865a.js .https://cloudflare.com/4...%&/.....%.....rt\j.-f.....H....MQ..f...OSf.A..Eo.....O&\.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a9a61d9a8445425f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4175
Entropy (8bit):	5.711028665990787
Encrypted:	false
SSDEEP:	96:T8B+M2cRxBGuzqJlneIqJ9mprNy0PU7nj:IBh2Ovz0eJ9mpZs7j
MD5:	72ACF07319346619EB81CFC78E7D8478
SHA1:	ADDBFE732276ACB484F6848E9386EDCBB3E437AF
SHA-256:	3B1977294F060E5543B96A1F9A07D9961E0318B59DA3CDB1FF936D29E9D8427B
SHA-512:	44677BDA89A9291B1E4788722EAA56309EB4709BC7BF6D1A26416C89B64E4909BDD35F61224C37F9C2F637F14CFA0006FC475490239B244E65DD1D6B37121FD0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q.?.....A..Eo.....b...%&/.(.....'.. ....O.....XL.....(S.4..`$.....L`.....(S.1..`.....L`<....hRc0.....Qb..L.....e.....Qbn.....c.. ...Qbjb.|....n.....Qb.....o.....M...QbB.....s.....Qb.Tou....r.....O.g$.....I`....Da....\A...(S.M..`P....(L`.....M.....Qe.....hasOwnProperty....Qb.....call..Qb ...m....push..QcZ..L....shift.....K`....D...x.....*..&...*..&...*..&..&.|.&.(...i...e%.*..&....&.(...&.(...&.(...&...&.Z.....).&.%.*....(...&...&.%.*..&..*..&.Y.....&..0.. %.L"&..i.%..Q w.....#.&...B....#.4&....&.(...&.(..$&.(..&&.Z....(....&.%.*.*&.0..,%..&..B.....&.]...(..0..(..2&.X..4&.\.6.....&.(..8&.(..:&...&.%...|<&.Z....=..&.\.?....,Rc.....Qb~.....t...`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aca5ffcd3b597dad_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.668097929909775

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aca5ffcd3b597dad_0	
Encrypted:	false
SSDEEP:	6:mYaVYcvGrC2Rr8mHgJkbvP4rsRK6tWYaVYcvGrC2RrKFg0MkbvP4cYK6tWYaVYcE:Fyo8SP/rPyoKRPyPyoLzJP7
MD5:	B60EECF6FCF5C2C8F5E442BF72A0D822
SHA1:	76910314CC1FD7B61BFEB1079E42CEE1EDCDA1AD
SHA-256:	E964FE5797CEFDF53C5A71A962DC4D206D210966AF164DE9614B64F94ADA551D
SHA-512:	B0964C9F68C5445BA68FCAF478CD0B194BC5EDCFF1D6D8C7010FF80647813107A9F21EC47EE68C33FB54EF64AB0A08EE5C43871B3B251C4CB5E32545044E606 5
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....._keyhttps://assets.www.cloudflare.com/js/chunk-06380521ff19239efe05.js .https://cloudflare.com/....%&/....._.....Lq....U{....~0..G.....A..Eo.....A..Eo.....0\r..m....._....._keyhttps://assets.www.cloudflare.com/js/chunk-06380521ff19239efe05.js .https://cloudflare.com/.^..%&/.....Lq....U{....~0..G.....A..Eo.....8{.g.....A..Eo.....0\r..m....._....._keyhttps://assets.www.cloudflare.com/js/chunk-06380521ff19239efe05.js .https://cloudflare.com/....%&/.....(&.....Lq....U{....~0..G.....A..Eo.....x.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ad4da03ad6699463_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1272
Entropy (8bit):	5.688531060131349
Encrypted:	false
SSDEEP:	24:DbYAzl7RbYpRbYGKAxRbY8rRbYARbYZD5:DbvRbeRb7xRbbrRbfRbc5
MD5:	D94AF6CB1CE28613297B76D09B109915
SHA1:	CC888F83F4CD290E8C6301FE1FDE4B134716CBED
SHA-256:	9FBE1D8AF926F8A6183333D8EB8665A71644674D7AC9647CDE655832EB482E24
SHA-512:	B4946844B3C3B6857CC8A7267FD6C93CE4CE0960DAD4DB20B4AEAA008F049FC0135ADE2CC787CB78D08FDD4B063BFB624AC6C91617A7ECE9D1F55221D584F A8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...-@3....._keyhttps://tr.www.cloudflare.com/gtm.js?id=GTM-PKQFGQB .https://cloudflare.com/.GB.%&/.....y.....XN.{...-?..cB&.".8|"z..U..Z\....A..Eo.....S#K. .....A..Eo.....0\r..m.....P...-@3....._keyhttps://tr.www.cloudflare.com/gtm.js?id=GTM-PKQFGQB .https://cloudflare.com/.u..%&/.....XN.{...-?..cB&.".8 |"z..U..Z\....A..Eo.....{.....A..Eo.....0\r..m.....P...-@3....._keyhttps://tr.www.cloudflare.com/gtm.js?id=GTM-PKQFGQB .https://cloudflare.com/Y...%&/..... ...XN.{...-?..cB&.".8|"z..U..Z\....A..Eo.....s7jU.....A..Eo.....0\r..m.....P...-@3....._keyhttps://tr.www.cloudflare.com/gtm.js?id=GTM-PKQFGQB .https://cloudflar e.com/.M1.%&/.....J.....XN.{...-?..cB&.".8|"z..U..Z\....A..Eo.....Gb#m.....A..Eo.....0\r..m.....P...-@3....._keyhttps://tr.www.cloudflare.com/gtm.js?id=GTM- PKQFGQB .https://cloudflare.com/..q.%&/.....%.....XN.{...-?..cB&.".8|

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aee831ff5029c966_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	415976
Entropy (8bit):	6.0335443429469855
Encrypted:	false
SSDEEP:	6144:LCkKTv+jA4T2n3HHytp8id8lyQuQbjJyzbYbG1pjQzV:LCkKTv+jOmqid8IdhJGsG/oV
MD5:	0B3F8C21F1089A3E119D2F639B08517F
SHA1:	02E6AE6A4B48727AB4DB1FA067BC0E035DD4519D
SHA-256:	5C0EB44857AB8B59CE97D6912D1D674AEE99745FB55560576ED2C0E86DB6EF31
SHA-512:	08ED8B7E0C38AAF230EFCA4E9366E4F9CA2233A31EABC3970331387D9AF305C7446409CE00DDAB87A1180483026077090D9AB6317C20D457AF1B111B4EEE4CF 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....*&t....3FD3A4C060587D5FE840F9E315E2B068D55241F215CA375C2B4FD2AE396E9267.....'.f.....Ox...8V.....u.....+..... .....|...\.....$.....t...D..... ...l0.....(..... .....@....P.....`...H.....`.....p.....<.....(S....`.....L`.....(S...`.....LL`'....@Rc.....Qb..... e.....Qb^:.....t.....Qb.....n...b$.....l`....Da.....(S...`.....L`.....Qc..:....exports..$..a.....S.C..Qb.:.$....l...H..a'...a.....Qb.....call..A(..K`....D}8.....&.%.*.... ..&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&..'..W.....-...(.....,Rc.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bb472feda361e78e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.661236738588302
Encrypted:	false
SSDEEP:	12:FG4O3K7mcFITPG4Jr3K7mII7PG4KnVL3K7mF1:A4f1IT+4JidN+4Ksc1
MD5:	09E3E71965277E103C7740B2A24709BE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bb472feda361e78e_0	
SHA1:	D59962004EEAE5E5570F882BEBDECA5D3E70BA32
SHA-256:	0E199EDDB2300AD01EC55AEFD468A86F7F2D4388BC1251399D6EBAA3496A3C47
SHA-512:	2C347E0B1FCBB3E1E3C9B0C1057BAF97C303BEC6F751D50DE1815C666BA2FF54C66E58A8BA5377E46327D6A8A3F2FBF289E56A4E80AAE6084C4495A97CE217A5
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...,.B...._keyhttps://assets.www.cloudflare.com/js/chunk-e6a0177c9a8b595a3dd2.js .https://cloudflare.com/._..%&/.....-..).....NsD..-..k..E..(..?o|.1.A..Eo.....o.|.....A..Eo.....0\r..m....._...,.B...._keyhttps://assets.www.cloudflare.com/js/chunk-e6a0177c9a8b595a3dd2.js .https://cloudflare.com/\...%&/.....-..).....NsD..-..k..E..(..?o|.1.A..Eo.....O.....A..Eo.....0\r..m....._...,.B...._keyhttps://assets.www.cloudflare.com/js/chunk-e6a0177c9a8b595a3dd2.js .https://cloudflare.com/....%&/.....'.....-..).....NsD..-..k..E..(..?o|.1.A..Eo.....7.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c2ffe14a07d86383_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.6652225172518715
Encrypted:	false
SSDEEP:	12:FLgYqMSNolANPLgYqHNol37PLgYqe5NolzN:JgYqMSMANDgYqHM37DgYqcMp
MD5:	3000DFDA232CF7E232374553B9F3D677
SHA1:	CA59D0D17357FD2626C68B24D5E7DD926BC9332D
SHA-256:	2F91F3268CF4AA9AE4F1070833E523F880F1A4FBFAD63D5DE10857A8AC3A6847
SHA-512:	499CA5A9FCC9D07E0185C34D0578C4728A9091913E3E86EF198971085E2E167C27E5A5536DC6D93D1F414D5071D0ED200A1D9FB6991E88C1852D5A8517237460
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....H...._keyhttps://assets.www.cloudflare.com/js/chunk-27eef9fa207b28718df2.js .https://cloudflare.com/....%&/.....8......"~;.f...!..,...z.=.I.....86...A..Eo.....7.....A..Eo.....0\r..m....._....H...._keyhttps://assets.www.cloudflare.com/js/chunk-27eef9fa207b28718df2.js .https://cloudflare.com/.Z..%&/.....{....."~;.f..!..,...z.=.I.....86...A..Eo.....d..y.....A..Eo.....0\r..m....._....H...._keyhttps://assets.www.cloudflare.com/js/chunk-27eef9fa207b28718df2.js .https://cloudflare.com/...%&/.....%....."~;.f...!..,...z.=.I.....86...A..Eo.....n..$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c720d3196762a96b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6609
Entropy (8bit):	5.765464928275716
Encrypted:	false
SSDEEP:	192:XClDMQnf4R9niSQYOw4DSlt3zlD3HzX6tUR:Xe3f4P37RDzl2A
MD5:	7507E1E14906EBCF666DD3A2DA41459F
SHA1:	686EEABBE1B0444E8A3E8DC98E080C896FDD97E3
SHA-256:	C2429AA024B3128548667008C18253BDAFB0A85403F016EE2F2A9B88C29C3FC4
SHA-512:	A1C043444D5D87E45340B5AB5A7A602B35F57EBD6B8F44EBE49808791D79961A15B16507390A8D005AED04F20E357ABFC4D261BE8FBE153F728CC802F8ADB67
Malicious:	false
Reputation:	low
Preview:	0\r..m.....10.&...._keyhttps://www.cloudflare.com/component---src-components-page-page-template-tsx-d90133272e40419501a8.js .https://cloudflare.com/.}..%&/.....T5`#..M.....|u.B...31...M.....uC.A..Eo.....A..Eo.....'..i....O....(...Pt.Y.....(S.-...`.....L`n.....Qc.j.J....window...(Q.....__LOADABLE_LOADED_CHUNKS__....Qb...m....push.....`.....L`.....`.....Ma.....`.....af.....Qb..:.....571MC..Qb.T.:....9b73C..Qb...c....BWBAC..Qb.^.Z....Eqd8C..Qb..Fqy6C..Qb&.T.....GsyWC..Qb.....JGcrC..Qb..R.....Mv6/C..QbZY.?....PXPiC..QbN. .....R8uDC..Qb"E.....TgIWC..QbR.z.....cAaeC..QbR.pj....cqNIC..Qb.....ew1GC..Qb.z.....fTf9C..Qb..)z....foeLC..Qb.....gutMC..Qb..RW....h7XDC..Qb.@.....iuYDC..Qb~.e.....k0b1C..Qb.K.-....oAnnC..Qb.....t94IC..Qb..2.....vbKGC..Qb.....w0vjC.QbV.1g....zB2iC.(S.....Pd.....push.571M...ae...o.....1.E.@.-....pP.....d...https://www.cloudflar

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d3c83df3d6e4942e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.580852833627088
Encrypted:	false
SSDEEP:	12:FkAKVzxrRsPkAKV1D+xrR65rPkAKVkv2xrRb:+AQzNRscAQh+NRycAQkONRb
MD5:	3EDE17A3E4570F873323FBDD28392534
SHA1:	9E68DD5434AD6EEAB3D704D9FCC24A720373B8E2
SHA-256:	3AF6CEF5A135F5D204C462EC648B7276BAD36E11333397655249016FBA148854
SHA-512:	7E8895B007C449088E1A518DB0975B1446D40B15363779B47EBB992862CDE7E046EFEAD56B6050557662AF62B75313712DD87E161174F6607D4C14E427F27F83
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d3c83df3d6e4942e_0	
Preview:	0\r..m....._...@2....._keyhttps://assets.www.cloudflare.com/js/chunk-cc3c9c6363f24544e951.js .https://cloudflare.com/....%&/.....m)....X.\.0.....&}.4.@E.f.2..A..Eo.....A..Eo.....0\r..m....._...@2....._keyhttps://assets.www.cloudflare.com/js/chunk-cc3c9c6363f24544e951.js .https://cloudflare.com/....%&/.....<.....m)....X.\.0.....&}.4.@E.f.2..A..Eo.....p.n.....A..Eo.....0\r..m....._...@2....._keyhttps://assets.www.cloudflare.com/js/chunk-cc3c9c6363f24544e951.js .https://cloudflare.com/...%&/.....x'.....m)....X.\.0.....&}.4.@E.f.2..A..Eo.....5.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dddb8d98c3534241_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	473
Entropy (8bit):	5.519769938864785
Encrypted:	false
SSDEEP:	12:mZKouAFV93+21Jg/bTH+21JglH+21Jg2j/v+21Jgx/:9cfzObTHfzIfzx3fz
MD5:	1D5A059DEA0AE0CF40986130D2588C43
SHA1:	AD6DF950119D9F8740BB1833C31361EF93D8955D
SHA-256:	1B4E4220A95F83CD2898819D7C32923E7BAB1D1E95D2D7FBEBF50BDBD94B2429
SHA-512:	8F0F85C9452233FB80B9CA93B52EEC461ACEDB13CA75D26C7E83F6036848412461E61B3A435837974030672457F62E38BAA413FD0AC5A9791FA2EF1E65776CF8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y....2.~...._keyhttps://embed.videodelivery.net/embed/4.ef69d404.chunk.js .https://videodelivery.net/]...%&/.....@..../...sys..C..O]#P.....A..Eo.....(.V`.....A..Eo.....%&/.....@..../...sys..C..O]#P.....A..Eo.....%&/.....@..../...sys..C..O]#P.....A..Eo.....(.@>.....A*..%&/.....(.....@..../...sys..C..O]#P.....A..Eo.....r..p.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dffa7aed83798cac_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.543747306497807
Encrypted:	false
SSDEEP:	3:m+lPxta8RzYrSL64KIHHnzW9ZEHFVRPLBDZ9lH/lHCBsMTLsoWsOGhzmqhltpK5M:m29YGL1Lnz+EHnV1lHg1HsLsqqzbK6t
MD5:	849CE53B047696760A054FB15BADA1BC
SHA1:	81A84CFDC8C415789BBB9006240069DCC8E6AF59
SHA-256:	3812DD8BB084EA51F4D92D46211E4178C9D2ADD8770AA55EF602C108AEC1F56C
SHA-512:	0D32A5E90E0FB574273AA9599DA6FB8C8EAF2F3CE459F7AA8FC6967F6CEAA2BC3D9FB9531F7122D69F223F2985BFC5C9A8361DBF4A20D958004B3DCB163024 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://www.cloudflare.com/commons-6269fe301a1aa3b81ea1.js .https://cloudflare.com/....%&/.....J-.8F+,.s.#....J.s.w.6.....A..Eo.....x.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dfff23a80e98adeb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.594933144643277
Encrypted:	false
SSDEEP:	12:FpkkIaWYRRUl1PpkkIORRdPpkkI4WaRRM:rkkIaWISl1BkkI2TBkkI8i
MD5:	9514E4D7A996F1A5F0EA997C5024A62F
SHA1:	882B8E9A1830AC0CDA6A850BE401FE35EC22EC9B
SHA-256:	EBB2BF68E22C161196237A56D75CBC62C4078A1A41AAF8C972BFB4C4AA7031FA
SHA-512:	6189CC49B63681882D7FC9D4E73775FAFE12149E3CE4E42F693601FF8C7F50B1E685052CA33C5CA4D7DFB2BE7920E04F60456C533C9F48CE079366432051AFF5
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....keyhttps://assets.www.cloudflare.com/js/chunk-5c6ec7c6f9d0b6f9dd57.js .https://cloudflare.com/....%&/.....>.....zQ.j.]%X;:.c...v.....i.%&..7...A..Eo.....nL7.....A..Eo.....0\r..m....._.....keyhttps://assets.www.cloudflare.com/js/chunk-5c6ec7c6f9d0b6f9dd57.js .https://cloudflare.com/....%&/.....E.....zQ.j.]%X;:.c...v.....i.%&..7...A..Eo.....~cK.....A..Eo.....0\r..m....._.....keyhttps://assets.www.cloudflare.com/js/chunk-5c6ec7c6f9d0b6f9dd57.js .https://cloudflare.com/....%&/.....~'.....zQ.j.]%X;:.c...v.....i.%&..7...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e0288702def24326_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e0288702def24326_0	
Size (bytes):	11867
Entropy (8bit):	5.707900317742041
Encrypted:	false
SSDEEP:	192:0WJv2XekFzHipdY3cxTizfZ4m32zdUYvhgDyE/OqDK8r4dvRaGD/:0NXPDi7wEi6umgDnONndvRau
MD5:	F65B2015EA7B2871595B35E040F7682B
SHA1:	910B99BA48A0ADBEE1D4C6586634D47980064B7B
SHA-256:	48624EE26DA7C1A5C7947CC6F4E9C5BD40DD871BE748F92DBE98F4B3F72FE696
SHA-512:	AC317EA7777AF99A46DCE63468244C03DDD436E0C7465FACE57D1F26D9CBBB9DD61F0E48E8F9F4C475A779254708F6CD9C935F3A91204CEAFAB4893944255C3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....&....._keyhttps://www.cloudflare.com/app-0b1250e637689a34706c.js .https://cloudflare.com/...%&/.....*.....c. .o..u.....!.h^,L.H.A..Eo.....y.b.....A..Eo.....'..#....O....,.....h.....(S.=...`.....L`.....Qc.j.J....window...(Q.....__LOADABLE_LOADED_CHUNKS__....Qb...m....push.....`.....L`.....`.....Ma.... ...`.....`.....L`.....`.....M`.....Qb^.P?....UxWsb.....F.....a.....Qb.....+ZDrC..Qb...../hTdC..Qb.g.....1wtQC..Qb...~....284hC..Qb..2....2mqlC..Qb.Y.....30RFC..Qbr.e/....33yfC..QbJ]C.....3uz+C..Qb..b.....5yr3C..QbJ..&....7hJ6C..Qb.....8OQSC..Qb:.....8oxBC..QbF.>....94VIC..Qb*.2.....9Xx/C..Qb..6n....D/D5C..Qb.....EnzkC..Qb>.k.....GddBC..Qb>.....IOVJC..Qb...{....InJvC..Qb.zV9....JX7qC..Qb.E.....JeVIC..Qb&X.....KQm4C..Qb:.....LYrOC..Qb^E.....LeKBC..Qb..L....MKeSC..Qb.....MMVsC..QbjU.L....NAsvC..Qbf.v.....NSX3C..Qb.@ .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e039148fbae90272_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	473
Entropy (8bit):	5.444758900161907
Encrypted:	false
SSDEEP:	12:ow/BZ/ASAJHmS45SDam45SZS45Swlxni45Svh:9QZ65SDaB5SZd5SwJ5S
MD5:	EBECC5B954DF4547199CEFB4AC368DF5
SHA1:	C334E4BDA4ADEFE449B6F27676CE1F44776718B9
SHA-256:	05BB4C3A107B271BA4B9048A2EC52E04DD510B5A393A86CDC753683128342347
SHA-512:	111297BEC7DE53BACD8C4E96C7F9BD953AE15D55DC89785E2CD5B8A81BCF86D91F6440E251D45BC967B16705EDFD638B89B90B5127BEFBD33B9EDAB68C30695
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y.....!....._keyhttps://embed.videodelivery.net/embed/5.068adc7c.chunk.js .https://videodelivery.net/Q..%&/.....L.&.E....x.R..ih.....h.|.....A..Eo.....lY]....A..Eo.....D..%&/.....L.&.E....x.R..ih.....h.|.....A..Eo.....!.E.....r...%&/.....L.&.E....x.R..ih.....h.|.....A..Eo.....a.0.....%&/.....L.&.E....x.R..ih.....h.|.....A..Eo.....dx.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e218b56339a9333c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.668960893012526
Encrypted:	false
SSDEEP:	6:mYMPYcvGNU8tJAygX3t0d8/YhebZK6tWYMPYcvGNU8tCEtgLEd8/Yh77DK6tWYMJ:FDtGtF3TPDtCEg1opPDtdoft
MD5:	85834E9457D05BA46F13D49A030DFF5D
SHA1:	8889900F338B93D0AED02A82C51C85D4D9461625
SHA-256:	7537B17EBEE830F869428706C0FE3FFB8636DD2E52694C6FE11534A88F27D8B2
SHA-512:	CFBB54CFE53B30B5953874081FE48CCB16D80BB7157AB14AF0BAFD18DFD38A911DE649CB9A8D6AE0EBF8E7F752803E8F253075447F61DF312516777939D4C72
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....-...._keyhttps://assets.www.cloudflare.com/js/chunk-55ad6e1817237ece29a0.js .https://cloudflare.com/....%&/.....2.....s.{.`.a5...Fj...Y#.y.R..4....e.A..Eo.....A..Eo.....0\r..m....._.....-..._keyhttps://assets.www.cloudflare.com/js/chunk-55ad6e1817237ece29a0.js .https://cloudflare.com/.U..%&/.....x.....s.{.`.a5...Fj...Y#.y.R..4....e.A..Eo.....C.....A..Eo.....0\r..m....._.....-..._keyhttps://assets.www.cloudflare.com/js/chunk-55ad6e1817237ece29a0.js .https://cloudflare.com/....%&/.....%.....s.{.`.a5...Fj...Y#.y.R..4....e.A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e7fd65a93a982fcf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.42084576234455
Encrypted:	false
SSDEEP:	3:m+lQilta8RzYPkAvBAQzLAgW7sNRPLBDo+v//lHCKyAW7TB4mqS7l//pK5kt:mUnYMQBAQzUd7sVyuglbhpJhK6t
MD5:	BDD2BE878BE89BEA80F94659D8A7F4DF
SHA1:	5F7F89E428DE73FC555BF646D1EF1E1172E95809

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e7fd65a93a982fcf_0	
SHA-256:	830887C0BDD60034284CE0E34CF36850F98DB07C616C8A89B14B5E09C15C02E2
SHA-512:	56077FAF35CC89E2575193F2B3A9EFE651241D6C46EF4C161C4317BFF75FBB0D0930278E0703DB8F5109B8E6B881989E835374236403EC7674383C61A76C3724
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P..._r....._keyhttps://embed.videodelivery.net/embed/sdk.latest.js .https://cloudflare.com/TNt.%&/.....E.....hr."3...;.'..y...6..ku..A..Eo.....Q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f0640f7148c6300d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	5.868462097845651
Encrypted:	false
SSDEEP:	6:maYGLL5B1XrQ1kZIngAkR7eVk49C0hK6tn8qVrmXqk5Br7eVk4x0l/:RBxZYkMVkYh8q5gq0AVkV
MD5:	A4FB318AAC4DB62E4D0410BE5B45D91D
SHA1:	7CCD8C6A8F527D7FCA58A3D36841841A5A6FE00B
SHA-256:	4B817D0E55553200CEE55C7497BC4DAB5C216EA2B91F83D92D3526CDF51CA0C5
SHA-512:	7453FEAF445E56A90B94070C1D6198631F86CA015E15B5D7E3D9A4797CCF51BD93F664EAD451134F6009E14B9CF47B6A547D30D618073821DEE2B5A502B9351E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x....._keyhttps://www.cloudflare.com/78ea267daafe81328bdca4e600e3c86b21c254f4-565aff763e8d9fd664bd.js .https://cloudflare.com/.]..%&/.....[..`W.C.t.....c.jj..3.`...A..Eo.....].....A..Eo.....].%&/..2..907AE4693EF1998A704E747DE82824C24765F4C91459C149949B6937A907302C[..`W.C.t.....c.jj..3.`...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f665d1821da95ab9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	407
Entropy (8bit):	5.535313191851701
Encrypted:	false
SSDEEP:	6:mURYMQBAQzUMw9cC7sAQzoYQKlHgAs1lrqqkYcnK6t8tFgWl1lrqqkYbwKFgal/r:pTZTM3CwArYfls7rq5pCz5rqRg/jrq
MD5:	0CC86185627003DD715841C2750BD4CD
SHA1:	6D647BEAC9941D3AE5E53CF49F9AD74FF30926E6
SHA-256:	4F99D0488E9590FB43B1623E6D31BD9FF5561601320CD985B0D83CB899EF90B9
SHA-512:	6D7D44B0CA6F7B8A282D3055F9D46B311BE4B7F83C7D4453AB4A6E70E611F2C3256BC34176BB9866971DCA226777EA702F5BCF742165D6BB7B8095386406B182
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...1.HA...._keyhttps://embed.videodelivery.net/embed/sdk-iframe-integration.fla9.latest.js .https://videodelivery.net/.*}.%&/.....\..U5.y.....,.....r..A..Eo.....A..Eo.....x..%&/.....\..U5.y.....,.....r..A..Eo.....7.....r..%&/.....=.....\..U5.y.....,.....r..A..Eo.....4.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f81ec822cd6c4871_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	263
Entropy (8bit):	5.605478353155192
Encrypted:	false
SSDEEP:	6:mcF6EYGL1yMWgf8c/43FgxCsSvjmvhK6t:xF6pB5c/4SCn67
MD5:	DCE980F27E263DE2538E089F925F9080
SHA1:	A3DF0435F47D115B7067B615703D53C3120E602F
SHA-256:	7AC2CF99612B0E3BCB87A28E2C8C2F1868AAB290C47CBE9AC254ED58688F5807
SHA-512:	7F65C513F890244E99501926A6B4DAAAFB130C8E3FE65DDACAED0C84E77A5739E4AC46B85D7D5E8A3FB7BB482F70B98C11082219463073FCF6961FF267371E4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....-....._keyhttps://www.cloudflare.com/component---src-components-plans-plans-template-tsx-810ea8962b1a98c105bb.js .https://cloudflare.com/.R .%&/.....s#A..h.....q.....A..Eo.....i.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Size (bytes):	1536
Entropy (8bit):	5.439723531272372
Encrypted:	false
SSDEEP:	24:GnLQwOE4k7lNKHbSzy+vYqRYUzY+AARrmKhvHFxM/l/jc/mbZy/llmLpMNhfCK:Y0w0FUznhvl+1jchIRbfr
MD5:	CB8B559FA83ED53BBF9E8A8D326883B3
SHA1:	2BFEC670B66C904EABFB755A39C9226F0EADE71E
SHA-256:	CBD15B1BCCBE4CDF4D9B6691876E01599410A9B928496B8FC01C6D5301389B9C
SHA-512:	17469998D858B3B76E19C9C527EA2583FBA7853CBAC285B939BF77D552416AD6387081F1E2BA4A761C8C2650354891C954B60ED32BCAE5690C31F8C567DB9FD
Malicious:	false
Reputation:	low
Preview:	.....@9.oy retne....>.....l.....Vm;T.rV..%-.%&/.....i..ndD.&.%-.%&/.....c.i.:.M..%-.%&/.....J...]Nb0....%&/.....f.)P.1....%&/..Z.....$.C.....%&/.....a../G.....%&/.....#.....%&/.....j?9..6....%&/.....P.....%&/.....R5.3....%&/.....=.....%&/.....=.D&...P....%&/.....%&/.....F.n2A...@...%&/.....K.2@...%&/...].....s@...%&/.....T..I.w@...%&/.....}Y;....@...%&/.....c..J...@...%&/.....h..i/.@...%&/.....<3.9c...@...%&/.....c.jS..[.@...%&/.....f.....X.%-.%&/.....E.,../F....%&/.....t....%&/.....Z_.!.@....%&/.....r...9..M..%&/.....ABS.....M..%&/.....Z....e...v.%&/...../.:.e...f.%&/.....X..7/..f.%&/.....qHl."...@}..%&/....m)&...=.@.W.%&/..5.....,.h.D/.....%&/.....4}@...%&/..B.....J../)N@}..%&/.....k.bg.. .@}..%&/.....0.Hq.d.@k..%&/.....{..4iY'e@}..%&/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	2.9690217581551317
Encrypted:	false
SSDEEP:	96:dNwy1s9D1xFjPxVOyTqbMwNwsE11LB4CfGUEHUyFxkNoxJMcipqMQ:duyWD9ZqbMwusu1LPOUTWSNmJS4MQ
MD5:	3AD07C9CC831DD2B484A6D8A3EA26483
SHA1:	AD64C5B1B19B74D150E8F1A91F0D308E53132CD0
SHA-256:	3B827D304D169BD4F268CE1D445E77687DB847FFCC635530461DB50CBF381D97
SHA-512:	EA16BD4A8212B98E9CDE2644790827FAB08B68A304319ABC3400351F22B723BB7CB753E53998B5E07C8E3FF7F6A342359CD32DE72805197C85FC76AF238192F2
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.8315478349939258
Encrypted:	false
SSDEEP:	48:L8NOZtRq5LLOpEO5J/Kn7Us8bMKOgmKdus9660tBOwiFjNeg5ZZbM8rD7HhpdNOU:wOfcNwtbM/1s9D1xFjPxVOyTUMNwg
MD5:	B0F9F198D1D88B182ED8C3C4081E409A
SHA1:	A78636CBDB7B8CC176848F8470C665DF111537F0
SHA-256:	1762B66167EA423A2D6F5B893AFF703F19AB8D009E3191572122FA1430F061E1
SHA-512:	AC83AAF476578C0F69B1CCD2B1A269A3907E8F1FC93398B0BC1EBD5B5E7AA734B82E69EBCD240F7B60939B7ADA55277A138DC66B994FB9D995F8CEE9116E9D 03
Malicious:	false
Reputation:	low
Preview:	.....X..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	74835
Entropy (8bit):	2.799718406809575
Encrypted:	false
SSDEEP:	384:70tp5ntRnq5j3+C9Rwe1AlK30wWwGg5sCY7zVqjhq6mEF8d:Sk31UkH4gddo
MD5:	38D3F817627C06F62FE130E5674DD248
SHA1:	129C38AAB57D0C660C1CF6061CBA2F62189A4026

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
SHA-256:	EC317D8DCFB63B39B4BE4E9DC6A1FC3DB16A711A0D742B8127A559F923AA5FEC
SHA-512:	B0C3C1D96CE2C8FFAB5B6CD5254EA3BF2DF8A8D619DB8338908894F3D4D805D2EE85B6CE432A70A832887A8A78A23EDF93F451578297D0B4BA8007E9649A07 0
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...8a645d74_403b_44fc_9986_00a18f5862f6.....h}..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....http://covid-19.in.th/.....\|...x.....p.....h.....`..... .....4.....h.t.t.p.:././.c.o.v.i.d.-.1.9...i.n...t.h./.....8.....0.....8..... ....http://covid-19.in.th/.....~.%&/.....! .....1.,.....$...

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.206596123379137
Encrypted:	false
SSDEEP:	6:mJ9N9+q2PWXp+N23iKKdK8aPrqIFUtp41mWZmwP41NVkwOWXp+N23iKKdK8amLJ:o9N9+va5KkL3FUtp41mW/P41NV5f5Kkc
MD5:	03163296E6B4D392496ADA4AF3A132F4
SHA1:	1359994D5C832DDF3B34B03D344AEE34608CB406
SHA-256:	D49CE82265E74BDA1E7B153971C7CD1546C7A75EF0A9F0FFA7BD54E8C51C73F7
SHA-512:	9E82CCB7150EE2399775C04B56EDFEE51ECE4F92B6533BEE6BDA00489F0061272CAF7711263808AF843516F8E5E761617A9B52771240A9825FA7B33628CB347B
Malicious:	false
Reputation:	low
Preview:	2021/07/20-07:19:27.373 c5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/20-07 :19:27.375 c5c Recovering log #3.2021/07/20-07:19:27.375 c5c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Category:	dropped
Size (bytes):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB C
Malicious:	false
Reputation:	low
Preview:	.f.5..................f.5................f.5................f.5................f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.2149558198787735
Encrypted:	false
SSDEEP:	6:mkF39+q2PWXp+N23iKKdK8NIFUtpgJZmwPJL9VkwOWXp+N23iKKdK8+eLJ:VF34va5KkpFUtpgJ/PJLD5f5KkqJ
MD5:	C6F5C129F28C44E83C4B4BC36B3451D9
SHA1:	E3EE76B268620573DF76013D1898F3E1357E587E
SHA-256:	F0EF6F27ABDCB9622FB01320307724E73B163CFDEB811F8D6CFEFA8207E0F247
SHA-512:	D4A5A3A3ED3B5C687944E896975E76A5E46F43E492F9A67C292C426CABA593DEF4B2AAE7DD700AD60FFBD8E2E2AECF6584EB84EEDA48B66CE4BC7A7224AC CE3F
Malicious:	false
Reputation:	low
Preview:	2021/07/20-07:19:29.706 1368 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/20-07:19:29.707 1368 Recovering log #3.2021/07/20-07:19:29.708 1368 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	34816
Entropy (8bit):	1.410116105518542
Encrypted:	false
SSDEEP:	48:yBmw6fU1illMNZUucotG+TpNJn9P72YXYk4P+IYS7ju:yBC/lCZUjotlpbljyj
MD5:	C0CF1F9361D23C23B436ACA843BD7107
SHA1:	ABD5281E06D9E0E4A94A378915047A90A5B7E354
SHA-256:	4F5D6F0936488BF887D18FC77E81D0A4DCF532DFAF2BEBD8493225106793FF00
SHA-512:	3E3AD2F22BFA1DF7FCDB44E4A63D3824FD4F49DF597A9E797ED28E1A1AC1CDCD50E1C1CFABBFB406954BA5D57BDF949E42E22047A286441621EA4C0B4A5F659D
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	37048
Entropy (8bit):	0.8217548959850852

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Encrypted:	false
SSDEEP:	48:CVKMbK0sNfdBmw6fUq3nS+Xq186mPtgYXY78:CVKMbK0sNfdBC16enlmw
MD5:	3AED0C83E2052DB48D7718F6EF2CEAB5
SHA1:	32835824B04E8171D360DC7A0667E0EF543F059F
SHA-256:	B05CB4913BFA55073D4313110DF35AB896BA61355ECA17CD46322DA9A4CD9512
SHA-512:	4551697A941AA64DBA6E935D7553B28165B572293BAF9D5BC7BC97A645015AC910E08B52DB0B8829C97D2DB055D517C2462BE4ADCBCE6E9368843A679DF5E6E A
Malicious:	false
Reputation:	low
Preview:	.....c..5..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.281704893300454
Encrypted:	false
SSDEEP:	6:munt+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpH3JZmwPPEVkwOWXp+N23iKKdK25N:5ova5KkTXfchI3FUtpH3J/PPE5f5KkTM
MD5:	0B78C1E3D58B3FF562031CDD3ED920B8
SHA1:	C5E635DA88DD00222B324EF53133424B394B2A17
SHA-256:	B74F04CEB1BBA186490574188DF2CBF9A7B92757A77E28D5D55DD7F5DFFBA340
SHA-512:	D6C02B47EBBF0F7F03B1B0E1601C1C266E62A35373A0CFD499306D7D8E335A69AD8FD3D046BF1EE1AAED63953C1B20673CA0AAB1EEE53D1F2B1165E9E1E897 37
Malicious:	false
Reputation:	low
Preview:	2021/07/20-07:19:35.011 958 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/20-07:19:35.040 958 Recovering log #3.2021/07/20-07:19:35.041 958 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.257796824543672
Encrypted:	false
SSDEEP:	6:mTcW9+q2PWXp+N23iKKdK25+XuoIFUtpycMhH3JZmwPycjVkwOWXp+N23iKKdK28:/1va5KkTXYFUtpPSXJ/PPp5f5KkTXHJ
MD5:	7954C05F9DBB558009E38871E314583D
SHA1:	E157D7C5D561556BE942D7DEA048AFB2CB29AD52
SHA-256:	1B30709E7C2CC3DFF3DEE3F57C889A2A9F2FB171BAF7A14610976F78520D7C0B
SHA-512:	DF97F8029BE9B66E30D0A15F540862B1D378F9FF6118ECF5AD453CF4C7C6DE0D0B8BB8BCC68CD8948DEC3DA0D6116DD2F4564479C08B3290C5304FEF59CD0 A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Preview:	2021/07/20-07:19:34.985 958 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/20-07:19:34.990 958 Recovering log #3.2021/07/20-07:19:34.991 958 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	327
Entropy (8bit):	5.281991810915725
Encrypted:	false
SSDEEP:	6:mTcN3+q2PWXp+N23iKKdKWT5g1IdqIFUtpyc3JZmwPycvEVkwOWXp+N23iKKdKW4:/NOva5Kkg5gSRFUtpP3J/PPvE5f5Kkgk
MD5:	D0220F80375CA8C82F16CF9FB72E396F
SHA1:	B31513B7B152434C918B9B6AC2FCFA88C5D23358
SHA-256:	0828DF1E133BBB68625F787B29E8F7241E83265494A0F453F5990D89533470F4
SHA-512:	255C4B58EEE49E59E8F101B3D5821989305AB3A4EE5C4DABE90D0B3AD5A0BC70566F9C6510B3D85860059461AF94A0B792D5FCED9528AFBEF8D16092B5A8214B
Malicious:	false
Reputation:	low
Preview:	2021/07/20-07:19:34.908 958 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/20-07:19:34.922 958 Recovering log #3.2021/07/20-07:19:34.923 958 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.5095524948419067
Encrypted:	false
SSDEEP:	96:kC8KZ6WXCWxZq4atguXCaeIdxZVEb5atguXC36IdxZozFq:V8KZ6faZqNIaeIXZVEb2I36IXZQFq
MD5:	4B56F2D789B689FF81413419B6F98F9B
SHA1:	3CFEBB9FCEB6C657E57D535377E9A36C5405E988
SHA-256:	6D6BE61342C52C7796799D604AD8D901E45A421AF237AFB303BB4214404DC121
SHA-512:	784014A5025857EB67B482BC0BFF941C881AC582561800AAF4F4B3068C9EAA68137DBF685DA4854CC6F585F536307BFB7DAF244B63DC6AF7C0398CEBDB80DDF3
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	129832
Entropy (8bit):	0.3459341045371616
Encrypted:	false
SSDEEP:	48:2RqX3QxCYalKZ70w/W1xCwSEROxZTtg48DZAoatgu1xCsnQt7ykPMo/IH9xZNl6x:2RZC3KZrWXC4IxZTLoatguXCE7eIdxZ4
MD5:	45BA32A330238E84332FEB3F09CFC346
SHA1:	A87CF6F232EF0A753D3A55174B4A5CDD9DF376FB
SHA-256:	AB277BF2F8BCAE549BA6D0B2F9B41A9F2AC3270ABD358E0BD0FC5F6059F43A8E
SHA-512:	591E104D46E3CC1ECA6C1B85EB96945F65563186979F615460DAB9E0397E1DBE99C9BCD02E82F0D47BB8CF860EA60AD5B6F18C9803DC33331C9C8CF8039564
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Category:	dropped
Size (bytes):	3543
Entropy (8bit):	5.601814615433376
Encrypted:	false
SSDEEP:	48:Ctj5BmoGhTa7gMO8dbN1AVBbQSefgG+WNrS0U9RdiN94/8qEtjMIG:La7gMldbN1AVBbQ5fgG+KrS0I
MD5:	C5A9F65BD769D5F27CCC34F79F8CCFCF
SHA1:	6F1A328C79BC93852B22E5980F6DCF86AE09BE2A
SHA-256:	67A21D4CB26E03E678393B63FEAF882FC382CD5D9C079B6823331E0985D1D92B
SHA-512:	BA6BD1DF2D8A4EF9B5874DA9899AC45A4812DCC51053E26E059FC09ED111A04B28DB85F0873A5F58985D87A17FC18D71D313E3ED81B6601559A5DCEDAA18FE AA
Malicious:	false
Reputation:	low
Preview:	../#...*.....META:https://www.cloudflare.com.3_https://www.cloudflare.com..__cf_test1626790779837.&_https://www.cloudflare.com..modernizr7.n...-.....8META: chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoverySe rvice;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGener ator..657786000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-20 07:19:36.38][INFO][mr.Init] MR instance ID: dd114c0b-8b65-4687-ba53-04b3704bbb57\n","[2021-07-20 07:19:36.38][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-20 07:19:36.38][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-07-20 07:19:36.38][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-20 07:19:36.38][INFO][mr.PersistentDataManager] initialize: 163 chars u

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 20, 2021 07:19:30.727902889 CEST	192.168.2.3	8.8.8.8	0x4956	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:30.731309891 CEST	192.168.2.3	8.8.8.8	0xd5ca	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:30.739947081 CEST	192.168.2.3	8.8.8.8	0x3a1	Standard query (0)	covid-19.in.th	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:31.463699102 CEST	192.168.2.3	8.8.8.8	0xbeb	Standard query (0)	www.cloudflare.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:35.600621939 CEST	192.168.2.3	8.8.8.8	0x63ae	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:40.454061031 CEST	192.168.2.3	8.8.8.8	0xefcb	Standard query (0)	assets.www.cloudflare.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:42.791862965 CEST	192.168.2.3	8.8.8.8	0x4567	Standard query (0)	tr.www.cloudflare.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.000561953 CEST	192.168.2.3	8.8.8.8	0xb09e	Standard query (0)	d.adroll.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.207166910 CEST	192.168.2.3	8.8.8.8	0x25b7	Standard query (0)	www.cloudflare.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.316482067 CEST	192.168.2.3	8.8.8.8	0xe254	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.579478979 CEST	192.168.2.3	8.8.8.8	0xf723	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.879256010 CEST	192.168.2.3	8.8.8.8	0xec50	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:50.212624073 CEST	192.168.2.3	8.8.8.8	0xda86	Standard query (0)	www.googleoptimize.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 20, 2021 07:19:50.539026022 CEST	192.168.2.3	8.8.8.8	0x3f51	Standard query (0)	static.cloudflareinsights.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:51.439277887 CEST	192.168.2.3	8.8.8.8	0xb1a	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:51.842248917 CEST	192.168.2.3	8.8.8.8	0x72c5	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:52.169291973 CEST	192.168.2.3	8.8.8.8	0x6a36	Standard query (0)	adservice.google.ch	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:52.884561062 CEST	192.168.2.3	8.8.8.8	0x7cfe	Standard query (0)	d.adroll.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:54.356939077 CEST	192.168.2.3	8.8.8.8	0xaf26	Standard query (0)	images.ctfassets.net	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:57.281620979 CEST	192.168.2.3	8.8.8.8	0x6943	Standard query (0)	images.ctfassets.net	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:00.017173052 CEST	192.168.2.3	8.8.8.8	0xbfcf	Standard query (0)	9309168.fls.doubleclick.net	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:03.446542978 CEST	192.168.2.3	8.8.8.8	0xa82e	Standard query (0)	embed.videodelivery.net	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:03.902865887 CEST	192.168.2.3	8.8.8.8	0x1eb9	Standard query (0)	iframe.videodelivery.net	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:04.897219896 CEST	192.168.2.3	8.8.8.8	0x15fe	Standard query (0)	videodelivery.net	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:10.280477047 CEST	192.168.2.3	8.8.8.8	0xb208	Standard query (0)	info.cloudflare.com	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:11.542335033 CEST	192.168.2.3	8.8.8.8	0xdeae	Standard query (0)	munchkin.marketo.net	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:11.826172113 CEST	192.168.2.3	8.8.8.8	0xfcb9	Standard query (0)	713-xsc-918.mktoresp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 07:19:30.777003050 CEST	8.8.8.8	192.168.2.3	0x4956	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:19:30.777003050 CEST	8.8.8.8	192.168.2.3	0x4956	No error (0)	clients.l.google.com		142.250.185.238	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:30.794296026 CEST	8.8.8.8	192.168.2.3	0xd5ca	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:30.811065912 CEST	8.8.8.8	192.168.2.3	0x3a1	No error (0)	covid-19.in.th		172.67.159.246	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:30.811065912 CEST	8.8.8.8	192.168.2.3	0x3a1	No error (0)	covid-19.in.th		104.21.41.46	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:31.524976969 CEST	8.8.8.8	192.168.2.3	0xbeb	No error (0)	www.cloudflare.com		104.16.124.96	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:31.524976969 CEST	8.8.8.8	192.168.2.3	0xbeb	No error (0)	www.cloudflare.com		104.16.123.96	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:35.668451071 CEST	8.8.8.8	192.168.2.3	0x63ae	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:19:35.668451071 CEST	8.8.8.8	192.168.2.3	0x63ae	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:40.518538952 CEST	8.8.8.8	192.168.2.3	0xefcb	No error (0)	assets.www.cloudflare.com		104.16.123.96	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:40.518538952 CEST	8.8.8.8	192.168.2.3	0xefcb	No error (0)	assets.www.cloudflare.com		104.16.124.96	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:42.857541084 CEST	8.8.8.8	192.168.2.3	0x4567	No error (0)	tr.www.cloudflare.com		104.16.123.96	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:42.857541084 CEST	8.8.8.8	192.168.2.3	0x4567	No error (0)	tr.www.cloudflare.com		104.16.124.96	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.050978899 CEST	8.8.8.8	192.168.2.3	0xb09e	No error (0)	d.adroll.com	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 07:19:44.050978899 CEST	8.8.8.8	192.168.2.3	0xb09e	No error (0)	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com		52.31.250.1	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.050978899 CEST	8.8.8.8	192.168.2.3	0xb09e	No error (0)	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com		54.78.251.22	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.270587921 CEST	8.8.8.8	192.168.2.3	0x25b7	No error (0)	www.cloudflare.com		104.16.123.96	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.270587921 CEST	8.8.8.8	192.168.2.3	0x25b7	No error (0)	www.cloudflare.com		104.16.124.96	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.366097927 CEST	8.8.8.8	192.168.2.3	0xe254	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:19:44.366097927 CEST	8.8.8.8	192.168.2.3	0xe254	No error (0)	stats.l.doubleclick.net		74.125.133.155	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.366097927 CEST	8.8.8.8	192.168.2.3	0xe254	No error (0)	stats.l.doubleclick.net		74.125.133.157	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.366097927 CEST	8.8.8.8	192.168.2.3	0xe254	No error (0)	stats.l.doubleclick.net		74.125.133.154	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.366097927 CEST	8.8.8.8	192.168.2.3	0xe254	No error (0)	stats.l.doubleclick.net		74.125.133.156	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.639431000 CEST	8.8.8.8	192.168.2.3	0xf723	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:44.937407970 CEST	8.8.8.8	192.168.2.3	0xec50	No error (0)	www.google.ch		172.217.168.35	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:50.280241966 CEST	8.8.8.8	192.168.2.3	0xda86	No error (0)	www.googleoptimize.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:50.601639986 CEST	8.8.8.8	192.168.2.3	0x3f51	No error (0)	static.cloudflareinsights.com		104.16.94.65	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:50.601639986 CEST	8.8.8.8	192.168.2.3	0x3f51	No error (0)	static.cloudflareinsights.com		104.16.95.65	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:51.491234064 CEST	8.8.8.8	192.168.2.3	0xb1a	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:19:51.491234064 CEST	8.8.8.8	192.168.2.3	0xb1a	No error (0)	dart.l.doubleclick.net		142.250.186.134	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:51.907417059 CEST	8.8.8.8	192.168.2.3	0x72c5	No error (0)	adservice.google.com		172.217.168.66	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:52.229389906 CEST	8.8.8.8	192.168.2.3	0x6a36	No error (0)	adservice.google.ch	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:19:52.229389906 CEST	8.8.8.8	192.168.2.3	0x6a36	No error (0)	pagead46.l.doubleclick.net		172.217.168.34	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:52.944534063 CEST	8.8.8.8	192.168.2.3	0x7cfe	No error (0)	d.adroll.com	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:19:52.944534063 CEST	8.8.8.8	192.168.2.3	0x7cfe	No error (0)	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com		52.31.250.1	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:52.944534063 CEST	8.8.8.8	192.168.2.3	0x7cfe	No error (0)	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com		54.78.251.22	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 07:19:54.422343969 CEST	8.8.8.8	192.168.2.3	0xaf26	No error (0)	images.ctfassets.net	ctfassets-images.contentful.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:19:54.422343969 CEST	8.8.8.8	192.168.2.3	0xaf26	No error (0)	ctfassets-images.contentful.net	d3orhvfyxudxxq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:19:54.422343969 CEST	8.8.8.8	192.168.2.3	0xaf26	No error (0)	d3orhvfyxudxxq.cloudfront.net		13.224.99.49	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:54.422343969 CEST	8.8.8.8	192.168.2.3	0xaf26	No error (0)	d3orhvfyxudxxq.cloudfront.net		13.224.99.124	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:54.422343969 CEST	8.8.8.8	192.168.2.3	0xaf26	No error (0)	d3orhvfyxudxxq.cloudfront.net		13.224.99.91	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:54.422343969 CEST	8.8.8.8	192.168.2.3	0xaf26	No error (0)	d3orhvfyxudxxq.cloudfront.net		13.224.99.59	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:57.338551044 CEST	8.8.8.8	192.168.2.3	0x6943	No error (0)	images.ctfassets.net	ctfassets-images.contentful.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:19:57.338551044 CEST	8.8.8.8	192.168.2.3	0x6943	No error (0)	ctfassets-images.contentful.net	d3orhvfyxudxxq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:19:57.338551044 CEST	8.8.8.8	192.168.2.3	0x6943	No error (0)	d3orhvfyxudxxq.cloudfront.net		13.224.99.49	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:57.338551044 CEST	8.8.8.8	192.168.2.3	0x6943	No error (0)	d3orhvfyxudxxq.cloudfront.net		13.224.99.124	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:57.338551044 CEST	8.8.8.8	192.168.2.3	0x6943	No error (0)	d3orhvfyxudxxq.cloudfront.net		13.224.99.91	A (IP address)	IN (0x0001)
Jul 20, 2021 07:19:57.338551044 CEST	8.8.8.8	192.168.2.3	0x6943	No error (0)	d3orhvfyxudxxq.cloudfront.net		13.224.99.59	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:00.082663059 CEST	8.8.8.8	192.168.2.3	0xbfcf	No error (0)	9309168.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:20:00.082663059 CEST	8.8.8.8	192.168.2.3	0xbfcf	No error (0)	dart.l.doubleclick.net		142.250.203.102	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:03.510596991 CEST	8.8.8.8	192.168.2.3	0xa82e	No error (0)	embed.videodelivery.net		104.17.23.75	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:03.510596991 CEST	8.8.8.8	192.168.2.3	0xa82e	No error (0)	embed.videodelivery.net		104.17.22.75	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:03.965787888 CEST	8.8.8.8	192.168.2.3	0x1eb9	No error (0)	iframe.videodelivery.net		104.17.22.75	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:03.965787888 CEST	8.8.8.8	192.168.2.3	0x1eb9	No error (0)	iframe.videodelivery.net		104.17.23.75	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:04.961347103 CEST	8.8.8.8	192.168.2.3	0x15fe	No error (0)	videodelivery.net		104.17.23.75	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:04.961347103 CEST	8.8.8.8	192.168.2.3	0x15fe	No error (0)	videodelivery.net		104.17.22.75	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:10.346087933 CEST	8.8.8.8	192.168.2.3	0xb208	No error (0)	info.cloudflare.com	cloudflare.mktoweb.com		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:20:10.346087933 CEST	8.8.8.8	192.168.2.3	0xb208	No error (0)	cloudflare.mktoweb.com	ab13.mktossl.com		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:20:10.346087933 CEST	8.8.8.8	192.168.2.3	0xb208	No error (0)	ab13.mktossl.com		104.17.74.206	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:10.346087933 CEST	8.8.8.8	192.168.2.3	0xb208	No error (0)	ab13.mktossl.com		104.17.72.206	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:10.346087933 CEST	8.8.8.8	192.168.2.3	0xb208	No error (0)	ab13.mktossl.com		104.17.73.206	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:10.346087933 CEST	8.8.8.8	192.168.2.3	0xb208	No error (0)	ab13.mktossl.com		104.17.71.206	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 07:20:10.346087933 CEST	8.8.8.8	192.168.2.3	0xb208	No error (0)	ab13.mktossl.com		104.17.70.206	A (IP address)	IN (0x0001)
Jul 20, 2021 07:20:11.602878094 CEST	8.8.8.8	192.168.2.3	0xdeae	No error (0)	munchkin.marketo.net	wildcard.marketo.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 07:20:11.971836090 CEST	8.8.8.8	192.168.2.3	0xfcb9	No error (0)	713-xsc-918.mktoresp.com		192.28.144.124	A (IP address)	IN (0x0001)

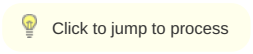
HTTP Request Dependency Graph

- covid-19.in.th

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 3096 Parent PID: 4220

General

Start time:	07:19:26
Start date:	20/07/2021
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://covid-19.in.th'
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: 5232 Parent PID: 3096

General

Start time:	07:19:27
Start date:	20/07/2021
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=1544,17804831982283933720,7344052518000277292,131072 --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: 7088 Parent PID: 3096

General

Start time:	07:20:05
Start date:	20/07/2021
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=1544,17804831982283933720,7344052518000277292,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=3720 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly