ID: 453275
Cookbook: browseurl.jbs
Time: 17:23:06
Date: 23/07/2021
Version: 33.0.0 White Diamond

Table of Contents

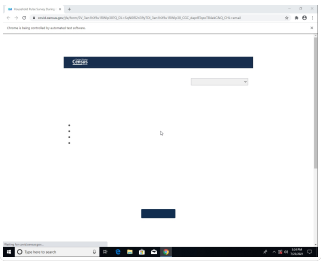
Windows Analysis Report https://covid.census.gov/jfe/f…

Overview

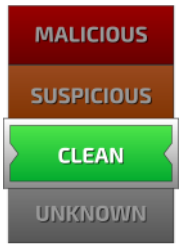
General Information

Sample URL:	http://https://covid.census.gov/jfe/form/SV_3en1hX9u1RWIp38?Q_DL=SqN0lR2ri39yTOI_3en1hX9u1RWIp38_CGC_daprBTqzoTB4ekC&Q_CHL=email
Analysis ID:	453275
Infos:	

Most interesting Screenshot:



Detection

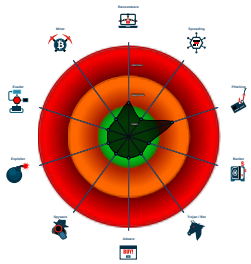


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Form action URLs do not match mai…
- Found iframes
- HTML title does not match URL
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5496 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://covid.census.gov/jfe/form/SV_3en1hX9u1RWIp38?Q_DL=SqN0lR2ri39yTOI_3en1hX9u1RWIp38_CGC_daprBTqzoTB4ekC&Q_CHL=email' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3504 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,18278074203958404562,976415347008169297,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3420 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1564,18278074203958404562,976415347008169297,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=4612 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4952 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1564,18278074203958404562,976415347008169297,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=4644 /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

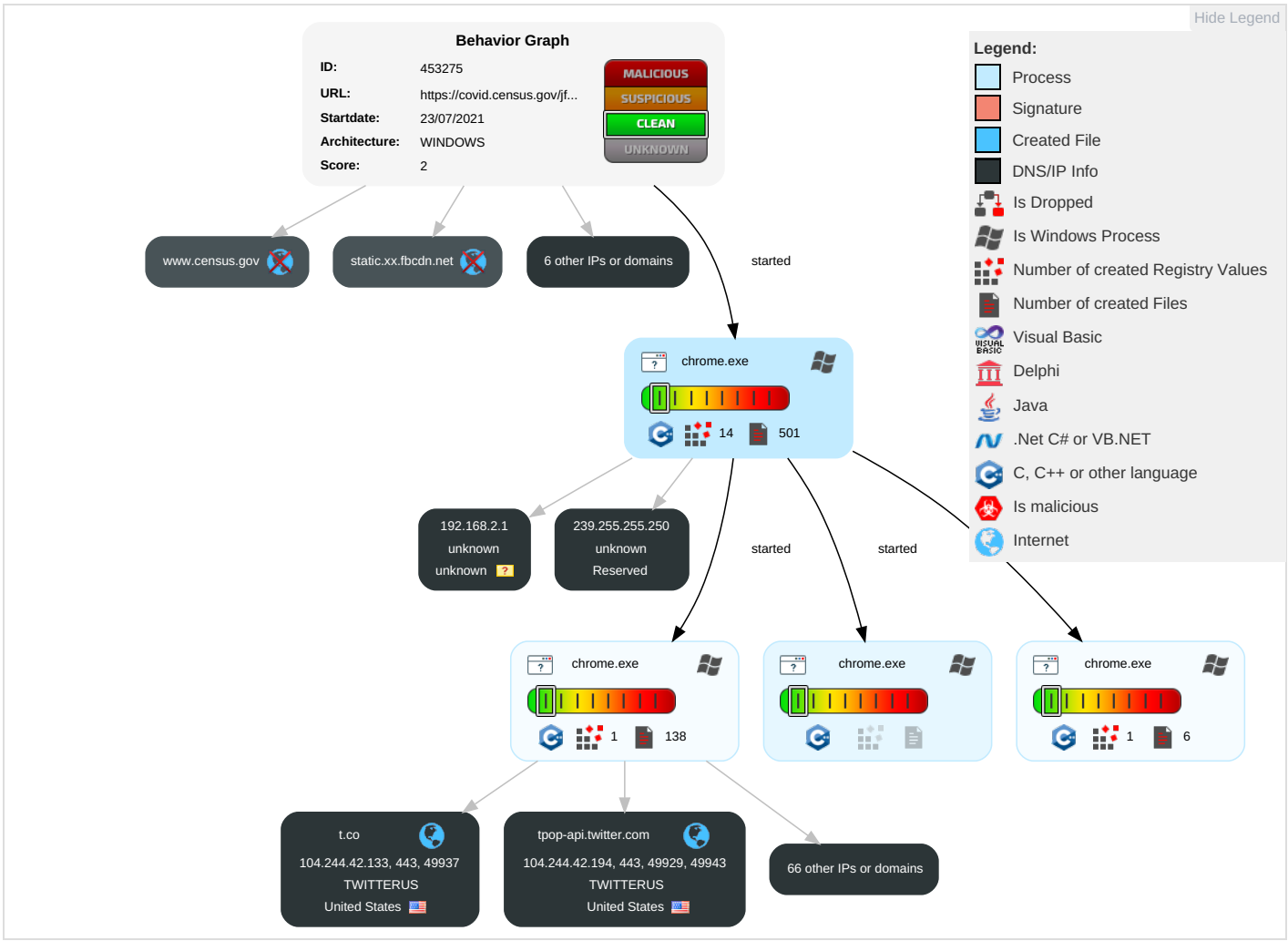
Click to jump to signature section

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

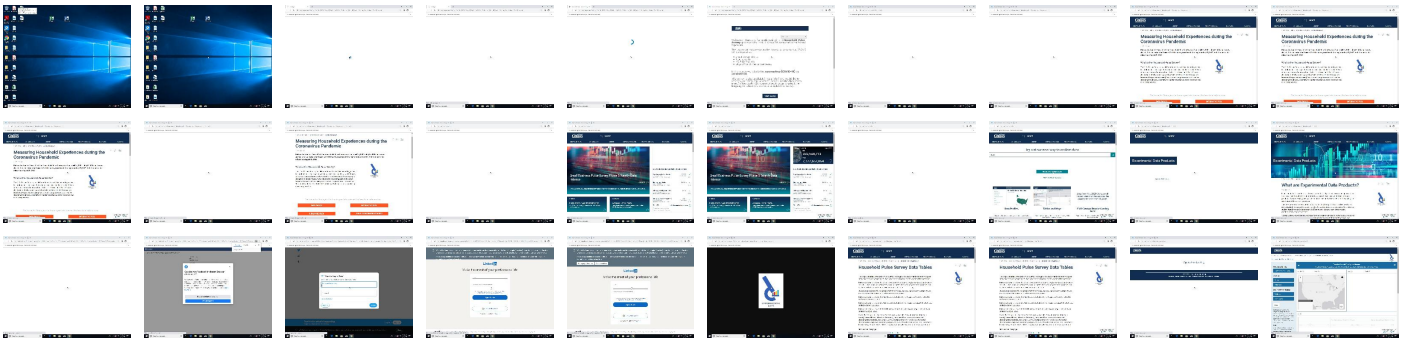
Behavior Graph

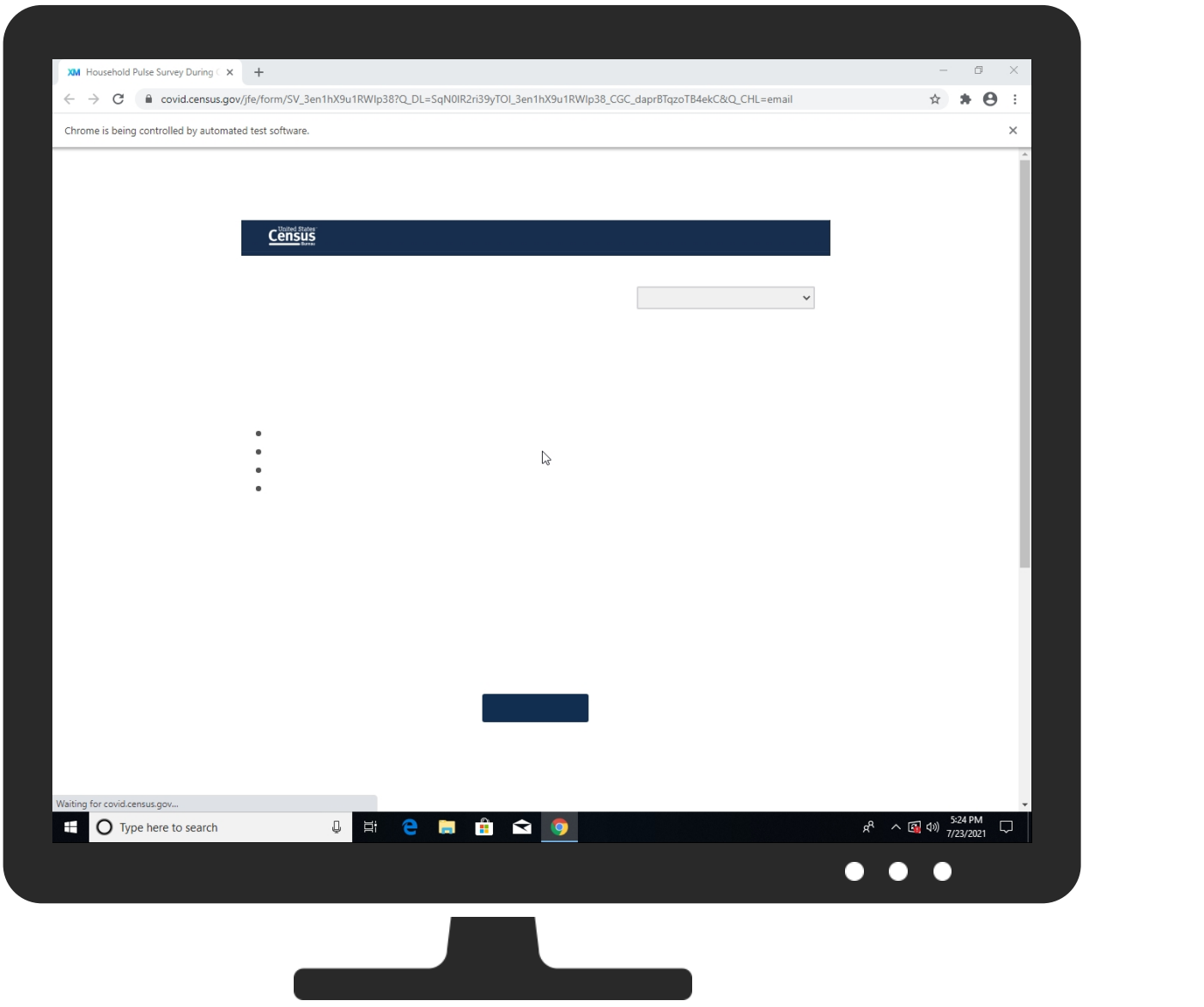


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://covid.census.gov/jfe/form/SV_3en1hX9u1RWIp38?Q_DL=SqN0lR2ri39yTOI_3en1hX9u1RWIp38_CGC_daprBTqzoTB4ekC&Q_CHL=email	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://s.go-mpulse.net/boomerang/N5F9F-5SXNV-TJA4F-B6CEM-65LXH	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.3	true	false		high
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
cs531.wpc.edgecastcdn.net	192.229.220.133	true	false		high
twitter.com	104.244.42.65	true	false		high
accounts.google.com	172.217.168.45	true	false		high
www-google-analytics.l.google.com	216.58.215.238	true	false		high
d27f3qgc9anoq2.cloudfront.net	52.222.174.63	true	false		high
cdn.digicertcdn.com	104.18.11.39	true	false		unknown
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	63.32.159.255	true	false		high
censusbureau.d1.sc.omtrdc.net	15.236.176.210	true	false		unknown
censusbureau.tt.omtrdc.net	52.213.168.74	true	false		unknown
tpop-api.twitter.com	104.244.42.194	true	false		high
scontent.xx.fbcdn.net	157.240.15.13	true	false		high
t.co	104.244.42.133	true	false		high
cs672.wac.edgecastcdn.net	192.229.233.50	true	false		high
www.google.com	172.217.168.68	true	false		high
cs1404.wpc.epsiloncdn.net	152.199.21.118	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
gis.geo.census.gov	148.129.75.137	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
cs510.wpc.edgecastcdn.net	152.199.21.141	true	false		high
uscensusbureau.demdex.net	unknown	unknown	false		high
kqiticdijx3nayh234wq-f-a6f6e7152-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
abs.twimg.com	unknown	unknown	false		high
s.go-mpulse.net	unknown	unknown	false		unknown
dap.digitalgov.gov	unknown	unknown	false		high
data.census.gov	unknown	unknown	false		high
6852bd0c.akstat.io	unknown	unknown	false		unknown
kqiticdijx3nayh235jq-f-4b8ecdb08-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
cm.everesttech.net	unknown	unknown	false		high
api.twitter.com	unknown	unknown	false		high
www.census.gov	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
kqiticdijx3nayh2345q-f-ac8018cd7-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
video.twimg.com	unknown	unknown	false		high
uscensusbureaucovid.gov1.qualtrics.com	unknown	unknown	false		high
platform.linkedin.com	unknown	unknown	false		high
dpm.demdex.net	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kqiticdijx3nayh234yq-f-fe811546c-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
gov1.qualtrics.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
assets.adobedtm.com	unknown	unknown	false		high
pbs.twimg.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
covid.census.gov	unknown	unknown	false		high
static-exp1.licdn.com	unknown	unknown	false		high
static.xx.fbcdn.net	unknown	unknown	false		high
kqiticdijx3nayh2344q-f-5302de751-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
c.go-mpulse.net	unknown	unknown	false		unknown
server.arcgisonline.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.census.gov/populationwidget/populationwidget.php	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.199.21.118	cs1404.wpc.epsiloncdn.net	United States		15133	EDGECASTUS	false
52.213.168.74	censusbureau.tt.omtrdc.net	United States		16509	AMAZON-02US	false
216.58.215.238	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	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
157.240.15.13	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
172.217.168.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
152.199.21.141	cs510.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
148.129.75.137	gis.geo.census.gov	United States		7764	CENSUSBUREAUUS	false
104.244.42.65	twitter.com	United States		13414	TWITTERUS	false
192.229.220.133	cs531.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
104.244.42.133	t.co	United States		13414	TWITTERUS	false
192.229.233.50	cs672.wac.edgecastcdn.net	United States		15133	EDGECASTUS	false
104.244.42.194	tpop-api.twitter.com	United States		13414	TWITTERUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
63.32.159.255	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
52.222.174.63	d27f3qgc9anoq2.cloudfront.net	United States		16509	AMAZON-02US	false
15.236.176.210	censusbureau.d1.sc.omtrdc.net	United States		16509	AMAZON-02US	false
18.200.233.208	unknown	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
192.168.2.3
192.168.2.6
192.168.2.5

IP
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	453275
Start date:	23.07.2021
Start time:	17:23:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://covid.census.gov/jfe/form/SV_3en1hX9u1RWIp38?Q_DL=SqN0lR2ri39yTOI_3en1hX9u1RWIp38_CGC_daprBTqzoTB4ekC&Q_CHL=email
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.win@47/558@42/27
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.census.gov/householdpulsedata • Browse: https://www.census.gov/data/experimental-data-products/household-pulse-survey.html#content • Browse: https://www.census.gov/en.html • Browse: https://www.census.gov/data • Browse: https://www.census.gov/data/experimental-data-products.html • Browse: https://www.facebook.com/sharer/sharer.php?quote=The+new+Household+Pulse+Survey+is+designed+to+deploy+quickly%2C+and+efficiently+collect+data+on+how+people%E2%80%99s+lives+have+been+impacted+by+the+Coronavirus+pandemic.&u=https://www.census.gov/householdpulsedata • Browse: https://twitter.com/intent/tweet?url=https://www.census.gov/householdpulsedata&text=The+new+Household+Pulse+Survey+is+designed+to+deploy+quickly%2C+and+efficiently+collect+data+on+how+people%E2%80%99s+lives+have+been+impacted+by+the+Coronavirus+pandemic. • Browse: https://www.linkedin.com/sharing/share-offsite/?url=https://www.census.gov/householdpulsedata&title=Measuring+Household+Experiences+during+the+Coronavirus+Pandemic&text=The+new+Household+Pulse+Survey+is+designed+to+deploy+quickly%2C+and+efficiently+collect+data+on+how+people%E2%80%99s+lives+have+been+impacted+by+the+Coronavirus+pandemic.&source=U.S.+Census+Bureau • Browse: https://www.census.gov/content/dam/Census/data/experimental-data-products/data-products.jpg • Browse: https://www.census.gov/programs-surveys/household-pulse-survey/data.html • Browse: https://www.census.gov/data/data-tools/household-pulse-data-tool.html
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:25:09	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC7594B0C90F3F2256C46D2FDBA24D95	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1262
Entropy (8bit):	7.22485770722756
Encrypted:	false
SSDEEP:	24:7ShGlGv46u7sBHRS6Vb3lhU+pjJguEAVGX95rs56d5CdUinUfkuhgy042X:7kJvOsTSu7IjJghAVm0ueUMuhgyj2X
MD5:	B64852C81713421B7E47E4302F97658A
SHA1:	6938FD4D98BAB03FAADB97B34396831E3780AEA1
SHA-256:	25768713D3B459F9382D2A594F85F34709FD2A8930731542A4146FFB246BEC69
SHA-512:	6A6F6DA5D47D88757F16853723198D5AD55F4A041E1EAA5200AF7F1054800CD4A9EA734AF8763DF1209A8CE2273DC0DBBFC766731DB5117BFC66D44DB2B7009
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC7594B0C90F3F2256C46D2FDBA24D95	
Preview:	0...0.....5..\)+.}..e....0...*.H.....0a1.0...U....US1.0...U....DigiCert Inc1.0...U....www.digicert.com1 0...U....DigiCert Global Root CA0...2009240000000Z..3009232 35959Z0O1.0...U....US1.0...U....DigiCert Inc1)0'..U... DigiCert TLS RSA SHA256 2020 CA10.."0...*.H.....0.....K.eGp..OX....f..1.T.JfF.,..d..... .....z.....V...X.Q.,4. ...V..y_....%.{.RAf.`OW.I..7g....KgL"Q.....WQt&.}..b....#.%So.4X.....XI"{.....|..Q...7.6..Kb.I...g..>....^D.qB}X.....2...'.'.+t....d...S.V.x..I.)..IO.....\.Wmky.+.' ...=@.!0.....0...0...U.....k....y.....v..0...U.#..0.....P5V.L.f.....=.U0...U.....0...U.%..0...+.....+.....0...U.....0.....0v..+.....j0h0$..+.....0...http://ocsp.digicert.com0@..+.....0..4http://cacerts.digicert.com/DigiCertGlobalRootCA.crt0{..U...t0r07.5.3.1http://crl3.digicert.com/DigiCertGlobalRootCA.crl07.5.3.1http://crl4.digicert.com/DigiCertGlobalRootCA.crl00..U. .)0'0...g....0...g.....0...g.....0...g.....0...*.H.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC7594B0C90F3F2256C46D2FDBA24D95	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	3.098219488358403
Encrypted:	false
SSDEEP:	3:kkFklWRtfllXlE/NtoGr/vhDvcalXl+RAIdA31y+NW0y1CSkNm/flgGNl5lq3b3/:kKtUtBcalgRAOAUSW0tXNQ3OiW/n
MD5:	776AA946D60195AC4D0417DEFB6D1F46
SHA1:	0AD79A00A928F41CB11F595F3103F8331A6FE105
SHA-256:	4E3A893C2C8249BA50516FE8B47FB1E59C7BA3D1172AF6DD68CBFDC23BD38CB5
SHA-512:	67A94AA1EFE83832523220F00DF76656D4AADDA8BF7D535F4F85EF0139119360D71D25902F6CB3903FA63CDF1A66B63E7A7C3573AF8EDF8F1A45227BE838752C
Malicious:	false
Reputation:	low
Preview:	p..... ....x.....["...(..... .....A.....u.....h.t.t.p.:././.c.a.c.e.r.t.s...d.i.g.i.c.e.r.t...c.o.m./.D.i.g.i.C.e.r.t.T.L.S.R.S.A.S.H.A.2.5.6.2.0.2.0.C .A.1...c.r.t..".5.f.6.d.4.4.1.0.-.4.e.e."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\1a3d923d-c92a-450b-a525-6240c399b863.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):	166208
Entropy (8bit):	6.04919883427251
Encrypted:	false
SSDEEP:	3072:QOayzVlexlBLiktL4AbbFF1CfLIWfFcbXafIB0u1GOJmA3iuRE:ilBLBtL/F1CfVtaqfIlUOoSiuRE
MD5:	20FDF88F2D5D5EE37EBB05E7231B1AB5
SHA1:	1AA567837A0A3FF6C13B76AB6C32154CF1103DD2
SHA-256:	71D4F7BC15E80B187E018E5BAC13C1D3804A3B08A58D34A12F7D41FB6F7976B1
SHA-512:	72CB32F03290ED5C7EFC437B39058258E00C665B0FC02DBA38418D33921D0788B2D8221F9827BC048E771FF3DC14813C8ADD0FA45486093B76046E790682CA36
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":1.627086243558919e+12,"network":1.627053845e+12,"ticks":5794559845.0,"uncertainty":4370503.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016582099"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\1ec1b88b-ebb0-47c2-bb16-22502ba811fb.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):	174673
Entropy (8bit):	6.078915097873806
Encrypted:	false
SSDEEP:	3072:WsGOayzVlexlBLiktL4AbbFF1CfLIWfFcbXafIB0u1GOJmA3iuRE:hglBLBtL/F1CfVtaqfIlUOoSiuRE
MD5:	9EA63511E0E9D5B6DAFCDE52EECABC4F
SHA1:	9E313A4297576EAC1EB2A21CB6DD82381F61720C
SHA-256:	819397EB0FEB6BC9C3A9078051B03CA53464BCD1BEAD2D06395384887447F920
SHA-512:	62346D33BB55BB4D2D9D7BE35E6B1ADC8C397E7C250047CDC5B34CDBCF4E605A697CB905F4A8EC4B0EF91E47DCEE7A147CD000055591A4B7FC138D6F66321F2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\1ec1b88b-ebb0-47c2-bb16-22502ba811fb.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":1.627086243558919e+12,"network":1.627053845e+12,"ticks":5794559845.0,"uncertainty":4370503.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016582099"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\3ddfe3e4-a6ad-4432-b03a-3015c3c3e6ff.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	103360
Entropy (8bit):	3.7501578329031746
Encrypted:	false
SSDEEP:	384:XbonXNqwF2xNV2criNDrYvf13wPhwHpsG0zr+ZXvxohNtsr2bmGSsaFbH7QOhBfK:vSKVVqNs4UeocuxEnbOFKrFHh1
MD5:	C5264B59EB3F881F77E819ACA31F73B6
SHA1:	ED1E11CACC58C18CE828FD8D33DE1CD114613FB5
SHA-256:	D48294721AF80FCF5B9D9DD87FC83583AE6BDE32AD046EF24421E7BAB1B0F549
SHA-512:	4118EB3A3F43842C52BC99DC5238BFA414B8AE6CF43DDA93FC6D58B3A9F99C877D44971FCA01CD04A4CC03CFCFB7E56A7126B9E6800896C9AB1C93D607A614EB
Malicious:	false
Reputation:	low
Preview:	.....*...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\47888741-95ab-49a8-a719-941aba46f1ec.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):	174673
Entropy (8bit):	6.0789138377265415
Encrypted:	false
SSDEEP:	3072:W9sOayzVlexlBLiktL4AbbFF1CfLIWfFcbXafIB0u1GOJmA3iuRE:Q2lBLBtL/F1CfVtaqfIlUOoSiuRE
MD5:	D44709DAB76D430543F576D5EE2DB116
SHA1:	F20D9A4DDC79EFCE102B1449924F66BD55E9751F
SHA-256:	D225BE08370003658E759FAB2E60E11EE99E892C50EC42F214D9CD2DFDA6FE02
SHA-512:	DB78E42237DEBE40BBC0B60EAEDD270F1101EC4E2432C2C8101FBE671F0C0088270778863B3AD50F3A6C6964078CA2BA1F3405B1297F9B7A477228869B05136E
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":1.627086243558919e+12,"network":1.627053845e+12,"ticks":5794559845.0,"uncertainty":4370503.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016582099"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\49190660-bfcc-4064-b21a-3c7422eb8b4c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.750714104219658
Encrypted:	false
SSDEEP:	384:DbonXNqwxx2riNDrYvf13wPhwHpsG0zr+ZXvxohNtsr2bmGRaFbH7QOhBfN+1TqY:gKVVqNw4UejD9xUnbOFKrFHhC
MD5:	6F1957AA2A94578F974707539C12306F
SHA1:	6F69BAB16FBA9F652EA94E88E167E6281C6945B4
SHA-256:	3A84A5A92337119F8D64F8EF75CCE97D42C0475994B5884BCE97ABAA3DFF3F71
SHA-512:	1F1898777FE8E8B871862F5E43E672553F61DF80689E6A1DD3808E8059B1F87C2A15D33824C0D0976250571DC51B9BAA090D4B435B0014BA61F7F611DB1675D9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\49190660-bfcc-4064-b21a-3c7422eb8b4c.tmp	
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\4da0bf35-bc54-40a9-b279-0dc8df3f41ef.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):	174673
Entropy (8bit):	6.0789130046311595
Encrypted:	false
SSDEEP:	3072:CH8OayzVlexlBLiktL4AbbFF1CfLIWfFcbXafIB0u1GOJmA3iuRE:+mlBLBtL/F1CfVtaqfllUOoSiuRE
MD5:	A167DF83C37A6C71A43F66667D9EFBD7
SHA1:	70EE4BA843AE6E51D9389100873CE819A9B65D68
SHA-256:	E5F05C6B124BDA41BE6E70EA6EFF331E9456591D36AFF8D6285E766DD7FE02A0
SHA-512:	075F73CD5555354773E2C44300C6F946C0550E4032F2BB0EF2D23BEC1B7FF90152EC62F411883B3EA9C9737685EBDFAA46D8FECF5C3E4FDE37B08C5742441F6
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":1.627086243558919e+12,"network":1.627053845e+12,"ticks":5794559845.0,"uncertainty":4370503.0}},"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\5e5b78b5-76f4-4161-af8f-e08d37e91e44.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.751155142079015
Encrypted:	false
SSDEEP:	384:tbonXNqwF2xNV2criNDrYvf13wPhwHpsG0zr+ZXvxohNtsr2bmGRaFbH7QOhBfNk:5SKVVqNw4UejD9xUnbOFKrFHhc
MD5:	B028F9D2815C7783164173AA80FAD0FC
SHA1:	240F19DFFA7FE5DE1324D0B325595F0F651B89F4
SHA-256:	B67ACC05A0E8C3A0F4ECE0ACEB647BAA8E2C9930405C07B06DD2B9C3CAD23EB8
SHA-512:	7A0D092DE65A1A73326DBBF2A7D22C25D1A8F04671BFBB7E41560BAE647C573BB038ADD4A341B4B3C989989CE4BBA7EC60F375752953E441B3FC9B7DC3B47455
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\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\070b0d14-ddf9-443a-8b0a-d64bd564ac30.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):	4438
Entropy (8bit):	4.863446523418582
Encrypted:	false
SSDEEP:	96:JOXGDHzAEKnccx7fiGqGdlj46f0N/KlK6J0i+fHZTna1DhwhH:JOXGDHzAEKccxjiGqcj46f0ReK6J0i+t
MD5:	CD1F8D45791531BBFE5207B9B1D129CA
SHA1:	6C35B4CF4B271FEA33A4A304C7CBD9B1882695E9
SHA-256:	06B7DDDFC02C39335C184436B4CDB3697A086FEE1B9A2ED8FE467463CD2AAF65
SHA-512:	39F6B2F8BC7E079EE96C5B12D0182A29256A1609036203C8846694A1E5171830C69A74E3F9CAA5C630D9BA831A8CC4862D9EA035099DEFB86BA6F43BD044752€
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274151843269631","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274151843413868","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13274151843413872","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r2---sn-h0jeln7e.gvt1.com"},{"isolation":[],"server":"https://uscensusbureaucovid.gov1.qualtrics.com","supports_spdy":true},{"isolation":[],"server":"ht

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\28f5cc1d-af65-48bb-a95c-eb4c17464947.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):	22595
Entropy (8bit):	5.535826563745343
Encrypted:	false
SSDEEP:	384:KHDttLl1vXV1kXqKf/pUZNCgVLH2HfDtrUIHGlnTG6Xm0W4Q:0LltV1kXqKf/pUZNCgVLH2HfJrU8GlnU
MD5:	07606786A6E24BA7BC41C1F0B3CA81AC
SHA1:	0D9A541E56F21FDA960E6CE3C47A6460F2B94FCA
SHA-256:	009E2FAA5CC5011928E2217D2E18B5C573EB46906D9287A8D9486135F4F03D24
SHA-512:	9A112E205198BBE94C6676CBAE53515ACEA07AE427F251F3A2FADE1A51C6C81CC9A3E9CBB2C5EBA6B26B9EBB5C761BF30A459F8FD6461A9F996BE8CD0AB08 444
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":"13271559838587274","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\2c3fd3c9-4477-43a0-a940-b0554aa22dfd.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):	5105
Entropy (8bit):	4.982871548000931
Encrypted:	false
SSDEEP:	96:nYCzoXMpcKIZok0JCKL83k11MbOTQVuwn:nYCCMpc24KEk1E
MD5:	62CFBF8F74320D2F75D629D3A7E73DBA
SHA1:	169DE42EC013E4E159D7875454EE892E86242D73
SHA-256:	C2051773DDAF7AB4A8C55C00D97790CFAAC3615FF6CDAFE1EAEE2E2C2280F738
SHA-512:	4F47ED50DE3957B0BC373F180CFF6581E3A7D99604B2605F2A76B4844CA9E606D124CB886FE4D13D34A342A9C21CD590BC08F8CC9A341F7AA90C119B731EEA(B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271559838968582","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\4e0d3d99-1386-46fa-9e57-2222e1f1fcad.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4e0d3d99-1386-46fa-9e57-2222e1f1fcad.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\52502a42-9e75-41e6-ac7f-a918b6e93ebf.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):	3048
Entropy (8bit):	5.608258220984387
Encrypted:	false
SSDEEP:	48:YUFUqw1LUb6UUhFEUyUCKUQ/jUI8yUzUzKUpI4q5lUa7omBsmU7yUTqPeUer2UeN:dU/LU+UUQUyUCKU0U9yUzUzKUabUtmFz
MD5:	F75F9982A4E11CD2BCA65253B7CC98E5
SHA1:	83DD0CD798E1E8249B752312533A156CABBC69FE
SHA-256:	6AD8C14DC2863FA463B560883905B86E4CF2F8AD3486558F811060C0D3C05830
SHA-512:	946EC17C73A5B12AB91273D2279053663437CBB64F3E984E3DE95C6F6B9CA2C1D25FDEF404974E1A52DF24F9412057BA4ABD5416297FEAD610F4089D4D897C0
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658622309.202274,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086309.202278},{"expiry":1658622294.192047,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086294.192053},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1642638300.994522,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o74YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086300.994526},{"expiry":1658622245.104889,"host":"TbNXujyuKYzExGI5EVjLCj66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086245.104896},{"expiry":1658622251.250057,"host":"UXkwKK50RSIe0pxRNE8AV4z71mmitHDrvDfp8QzFpcE=","mode":"force-https","sts_include_subdomains":true,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\61fa8bd1-eaa4-4578-8991-a015510a7880.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):	3048
Entropy (8bit):	5.607083453688251
Encrypted:	false
SSDEEP:	48:YuFUp1LUb6UUhQEUmUCKUQ/jUI8yUzUWDKU7q5lUa7omBsmU7yUTqPeUer2UefWU:vUvLU+UULUmUCKU0U9yUzU0KUoUtmFUo
MD5:	4CA63D976527CCA8DDA56BE483BDFD91
SHA1:	B5361EBC9C2BD07387CE1D5165799C421F0AF98F
SHA-256:	BC1967CABC54F1E170EC6F094C64CD07542C9973AFCE5F6C6782279EACCF5598
SHA-512:	ED78DF8A07199EA847D1A14E1D6691EA784DE890378F728127BC8E6380172948B13444298BDC5069AE83AE20D6D5B5E7F0250748F14F49CF170642AE6EB7023D
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658622300.016782,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086300.016788},{"expiry":1658622294.192047,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086294.192053},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1642638291.733488,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o74YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086291.733492},{"expiry":1658622245.104889,"host":"TbNXujyuKYzExGI5EVjLCj66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086245.104896},{"expiry":1658622251.250057,"host":"UXkwKK50RSIe0pxRNE8AV4z71mmitHDrvDfp8QzFpcE=","mode":"force-https","sts_include_subdomains":true,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6de3d020-8551-4252-ade0-5fa4b3d769d1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6de3d020-8551-4252-ade0-5fa4b3d769d1.tmp	
Size (bytes):	2210
Entropy (8bit):	5.614929600040242
Encrypted:	false
SSDEEP:	48:YI6UUhHEURCUCKUQ/jUyUWDKUuUTqPeUer2UefWpwU22UOUenw:GUUKURCUCKU0UyU0KUuUmPeU9UEWqU2T
MD5:	7202676261C098234E033FC896F0E15E
SHA1:	F38E6346F238E028C32B0A0267D27A5EFFD1BD17
SHA-256:	0288B0C063A129653AEA6851440719BBEF7F70829E423DF5ABD879D8B7D15C18
SHA-512:	47B68A28EEBB91AB0089D206405B113FA2096140F79AE93F063C2A9DBA15FA8ECC1E7CE64D11DB5B163B990B89B5DCA217B3301713774CA2A578806ADEC1D3 1
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1642638288.020978,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086288.020985},{"expiry":1658622245.104889,"host":"TbNXujyuKYzExGI5EVjLCj66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086245.104896},{"expiry":1658622251.250057,"host":"UXkwKK50RSIe0pxRNE8AV4z71mmitHDrvDfp8QzFpcE=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086251.250062},{"expiry":1658622251.396867,"host":"YHSMTQnYC85xpfxQXKcYuC0wBIhWAWiCTB+UjCnXwn0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086251.396872},{"expiry":1637972655.841281,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7285dc9c-bf58-4018-b2d2-6d07238e892a.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):	1874
Entropy (8bit):	5.609423000312037
Encrypted:	false
SSDEEP:	48:YI6UUhqUCKUQ/jUtseKUeUUTqPeUer2UefWpwUEv2UoUenw:GUU4UCKU0Ut3KUZUmPeU9UEWqUEv2Uo2
MD5:	73FCBECE5766CC628FDB3E374B35495B
SHA1:	70F602E3D27361D5DA4157538C381B4F3FF630F7
SHA-256:	36B290BA4349B0456818B302EF511B6F4A65980C17EBDCFF73E5B1740AF23E05
SHA-512:	3CD28C42164AF5786983AD7D3FD288C840E16069917CE8B9BFD13F6842A30AD32C55B4242F8533BB8379F018FAB898D8E6D15DAFC31F6983460F40FC07801CC
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658622245.104889,"host":"TbNXujyuKYzExGI5EVjLCj66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086245.104896},{"expiry":1658622251.250057,"host":"UXkwKK50RSIe0pxRNE8AV4z71mmitHDrvDfp8QzFpcE=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086251.250062},{"expiry":1658622251.396867,"host":"YHSMTQnYC85xpfxQXKcYuC0wBIhWAWiCTB+UjCnXwn0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086251.396872},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1658622245.954931,"host":"wPBGK7SV+UX5bqJcu0I1WRTpTkGu+94cCkvBBYprdTY=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\82b13cc1-0c82-4abf-8fcf-4e57bee9797d.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):	5.53587613531401
Encrypted:	false
SSDEEP:	384:KHDttLl1vXV1kXqKf/pUZNCgVLH2HfDtrUIHGmnTG6XmeW4r:0LltV1kXqKf/pUZNCgVLH2HfJrU8Gmn5
MD5:	5C1C8818BF6E63B74E31B7B420E44C5E
SHA1:	D9AA4735D4B45A810CA1307A23EDCC2DC60596B9
SHA-256:	A1ED40476308CA8D167ED5CB4121554F8FAC7C31454888AC65874A34E31DBE45
SHA-512:	D09EFCC8B17BA0D3A9549374A2AB0C1B62DB1626846DBC8F9710AA371EA6CE1216A839E1F002E66C73AA2E4F5B102F09CB4D7DC9FE2A082791C1DDE1A82F03 D6
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":"13271559838587274","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8742d8b7-fb34-48b1-a078-91d677ecc594.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8742d8b7-fb34-48b1-a078-91d677ecc594.tmp	
Size (bytes):	2043
Entropy (8bit):	5.611792226832913
Encrypted:	false
SSDEEP:	48:YI6UUhqUCKUQ/jUyUWDKUuUTqPeUer2UefWpwUj2U9xUenw:GUU4UCKU0UyU0KUuUmPeU9UEWqUj2U9A
MD5:	6336A2E562AB65E707A82B063A320586
SHA1:	41AE34BA08DFE4C381456AB0DA4B8A8FA669CC27
SHA-256:	FA6D7DF6699B5ACD4D48E91CB15A1AA888B4EBA89B969AFD6624052248DB7B21
SHA-512:	F818F883EF484F2F31289A6AC0955A4DED8D3CB689A80116318E309081FFEE6235231AFD5AA4B684291C3905BC7C2626A67761297490291EF20E77EBC44D2CA2
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658622245.104889,"host":"TbNXujyuKYzExGI5EVjLCj66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086245.104896},{"expiry":1658622251.250057,"host":"UXkwKK50RSIe0pxRNE8AV4z71mmitHDrvDfp8QzFpcE=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086251.250062},{"expiry":1658622251.396867,"host":"YHSMTQnYC85xpfxQXKcYuC0wBIhWAWiCTB+UjCnXwn0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086251.396872},{"expiry":1637972655.841281,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086255.841287},{"expiry":1658622275.183043,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\89abc0d1-b7cb-46be-84bb-dda05927ad0c.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):	2041
Entropy (8bit):	5.611477040169513
Encrypted:	false
SSDEEP:	48:YI6UUhqUCKUQ/jUyUaseKUeUUTqPeUer2UefWpwUEv2UoUenw:GUU4UCKU0UyUa3KUZUmPeU9UEWqUEv2I
MD5:	D737149FA76EE40BA80F4F2B7277D620
SHA1:	ED0D3860874F43FBDF427F9D527D490A679159BE
SHA-256:	6110B4BAA2564088839940DD13F13635CC5005FC6AC92E0CCE8C525DF9E23852
SHA-512:	E823A63C64E16C7FC299E9BA54132042FECBE029534D45F2E8222E09498AB74735107F6B5478EA60B65192A54EC7E952187890031589A43902714E3E7B9AFE9D
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658622245.104889,"host":"TbNXujyuKYzExGI5EVjLCj66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086245.104896},{"expiry":1658622251.250057,"host":"UXkwKK50RSIe0pxRNE8AV4z71mmitHDrvDfp8QzFpcE=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086251.250062},{"expiry":1658622251.396867,"host":"YHSMTQnYC85xpfxQXKcYuC0wBIhWAWiCTB+UjCnXwn0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086251.396872},{"expiry":1637972655.841281,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086255.841287},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.30042494758006
Encrypted:	false
SSDEEP:	6:mf3q2PWXp+N23iKKdK9RXXTZIFUtpOsZmwPOZkwOWXp+N23iKKdK9RXX5LJ:2va5Kk7XT2FUtpR/P25f5Kk7XVJ
MD5:	0E2A1AC3AF1D6DE604B5A8D3D75EFC80
SHA1:	43ACABBAC5CE0F4CC215E8520552EAFE10151FA5
SHA-256:	494AEB33B1569DC3416EC9BB1591B8609997FA96E63F787A16DE79B85A243FB5
SHA-512:	772165C272720240B140E1E122F3EE24A2C48DC176077DEC453EA8809A04A5374FEE13781211D11106BCF143395BC7E95E0421F961D2B9B8E9ACF2E535DD5923
Malicious:	false
Reputation:	low
Preview:	2021/07/23-17:24:16.969 18b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/23-17:24:16.992 18b4 Recovering log #3.2021/07/23-17:24:16.993 18b4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.278838304758079
Encrypted:	false
SSDEEP:	6:mfPq2PWXp+N23iKKdKyDZIFUtpOGOZmwPOGikwOWXp+N23iKKdKyJLJ:uva5Kk02FUtpzO/Pzi5f5KkWJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
MD5:	D67DDDC83D49F86C1830571C7714F930
SHA1:	390528F0BDFDCBD3876F90579727CE2D7415D293
SHA-256:	DCAAD6EEB2C34AAA26BDCF0E198D29A6CE4F5494813A01236528DF639CBB0F74
SHA-512:	1008009C5BDD6E787CEFD84F173C68AF9DB0A4A4CCB38641BF2C3FA4E116FCC505F221B98A120917F23F578716AC0D0373E5D7226EC2A345BFC84EDAD375E19
Malicious:	false
Reputation:	low
Preview:	2021/07/23-17:24:16.961 18b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/23-17:24:16.962 18b4 Recovering log #3.2021/07/23-17:24:16.962 18b4 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\0a295f2daec3ddae_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	196
Entropy (8bit):	5.347077209015406
Encrypted:	false
SSDEEP:	3:m+lyTggOA8RzYrSLbGtGE36J/ViLXWGer9l/lHCgZl/yvjCTQG6SJp9PeXmpOz/X:myVYGLKcNJ902Hgqy+Qem2pOzbK6t
MD5:	23374D5C8371E54D6223E4D804D8D689
SHA1:	EFB1BB955B198D8FBAFA6303A309E62E7214FA8F
SHA-256:	46FA09F25EDAA34A3831DDE64EC77DA30D165AAE5235E859D89573D7E58FED90
SHA-512:	2355515D23F70BE857DD67486154E41BDFA848C5F2C6880B3050E9B1343CEB52372F046801C67CECAB29638A1B3069A3EB1B8315D7C4E4C656960666BFEC8212
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...Rb....._keyhttps://www.census.gov/akam/11/2260023c .https://census.gov/.%..i&/...../t.)1...4g6u.s.6.s.!...E..zu.A..Eo.....E.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a69c121d2aba1b8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22949
Entropy (8bit):	5.717014481761511
Encrypted:	false
SSDEEP:	384:tKE76Zqm5etOF2ZcXT1M6gU4uumjkBbY6atw58DNrfZHB32JGAdd:tL2qL5sL4z+kBJQVJrfZhGDd
MD5:	A28AA9356605FC834B60022DCF63902B
SHA1:	F6383E92AF692FDC9282970CC9F228173FD13C8C
SHA-256:	D109D5C3F513ED2B2CCDE015FED1076D14ABA085DD08FD8EA0E74A96608D6C1B
SHA-512:	83A8C142A74C545F39E3066D7FD51667FA2896102B074E1C9E0EA533A095EDB203CED31D6F48F9E89B2E596372EA8B493DB2C02166D10F0A28E24AD55C383453
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....._keyhttps://www.census.gov/etc.clientlibs/census/clientlibs/bootstrap.js .https://census.gov/....i&/.....6.....jBX.B...o....(V.k.@[...a.A..Eo..... .[.....A..Eo.....'.....O.....X..Z.....$.....(S.....`.....HL` .....Q.@.5nv....jQuery.....4Qk.#".&...Bootstrap's JavaScript requires jQuery...(S...`.....$L`.....Qbn.....fn....Qc.....jquery....Qc.....split.....K.....LQq.'W.>...Bootstrap's JavaScript requires jQuery version 1.9.1 or higher....K`....D.q.(.....(...&.(...&...&.Y....&..*..&.(...&...&.Y....&..*..&...i.....*..&...i...+.*..&...g.../..*..&...g...!..*..&...i.....&...&.%.e.....(Rc.....l`....Da2...L....$..g!.....P.. P.. ..."..."....@.-....PP.1....D...https://www.census.gov/etc.clientlibs/census/clientlibs/bootstrap.jsa.....D`....D`....D`.....`|...&...&..Q.&.(S.T..`b.... L`.....8Rc.....Qe.6l.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0b77f43b78f08ef2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.535954040426491
Encrypted:	false
SSDEEP:	6:mSlPYsyZcDA3RdZSfgbdf69QZ5P4khK6t:NlsdH8q/T7
MD5:	D99109E11AF150BCBDB47375491F826A
SHA1:	0DE8BAA8405D04BA23163FD1F51D0D63BAC5ECF0
SHA-256:	1F23047FF783477007F36D685A62CD8F3B57BCBCB7829D7E8EEF3BA4202555E6
SHA-512:	33A00223D4978C626E37F7B21DEB15B9F119F4C1ADA6EDACE7FFDC188EF433B72D6CFFF8F6E1C6EC87D94AB820F659F7B02F414B40353A86D4C3325F22CAA71
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...S\0...._keyhttps://covid.census.gov/jfe/static/dist/jfe.f5270bb8374885d2b2ea.js .https://census.gov/.H..i&/.....OC..wzg}.....0B=.].....BD...A..Eo.....E.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0cc355b46b6d9532_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	69008
Entropy (8bit):	5.750517396871957
Encrypted:	false
SSDEEP:	1536:OS//sEtMlXePcg3TFMfUgdPiySoi6WAdeT8ppK:oEtMlYqda5kM8pK
MD5:	B2B3D18DD6420D1B3B70ED39DC9419F8
SHA1:	803E763F5C56B3B427567DC772BCF41E05E823A5
SHA-256:	9631319A55057DEE299C82995CA5CBE9F8E37FE89ED84FD70A208F23BCE44CF4
SHA-512:	201F3A401998824E2C9B887BD459EC70BD45C46E2A0FB677DBF07962E95A2FF1AEBB2F58462D09542CBC7C96CF42F5550AEE83FA328E8B647DF54101FF83A53
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...U.....31B709B1ED83C84A44DB84B36C7E22F3EE669C154928435823DADDC33207BBA7.....'.....O....X.....F.....I.....4..... .....x.....(S.4..`$.....L`.....(S...m..`.,.....i.L`0....9.Rc.....QbJ9 .....w.....Qb.Em.....A.....Qbb.]g....ma....Qb.v.....Qa....Qb.wX=....X.....Qb.....J. ....Qb..(t....Z.....Qb.....na....Qb.....oa....Qb2.....pa....Qb.....qa....Qb..o.....ra....QbrF.....sa....Qb*..W....K.....QbFZ.m....wa....Qb...n....c.....Qb.....Ra....Qb.....Sa... .Qb.wF=....s.....Qbr..G....T.....Qbz.....Ta....QbbKP.....Ua....QbR*.{....Va....QbrH>.....Wa....Qb.....Xa....Qb.....xa....Qb.p.....Q.....Qb.8.....L.....Qbv.Vh....aa....Qb.#0.....b a....QbN.....R.....Qb.6MO....ya....Qb.....G.....Qbf.....Ya....Qb&.k.....za....Qb..-_....Aa....Qb..:J....ca....Qb.b.....Za....QbV.P3....$a....QbJz@+....ab....Qb..C.....bb....Qb.=..... .cb....Qb.....Ba....Qbn.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0da2f868400f82ef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.752175171302235
Encrypted:	false
SSDEEP:	6:mqYk+f2pomBMiQfzhmJ2EgztKBVTehd0K6t:z++amBbAkJPDTeXG
MD5:	1F25F10C2D32AA36ACE191916E734430
SHA1:	892408AE242A0F8432B9FAFB1CE03A19DD6B6D33
SHA-256:	99774D69BB8B9CC66DFA7CF6DE61AC1270DD02448E26E1F8AC286D90A1774586
SHA-512:	8D8987D9F3E6564686408CD906468E31CC70BB8078EACCE447478C2FAD283326D75AD005F765C1E5693B2D8FBDE18F93BA39444B1CE614EBBC7F3744DC06F8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....J....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yj/r/IUy0P1uEqH3.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....MI.....T..Db.rqY'.....;..|.x. g.....A..Eo.....u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f016c508efa5487_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.6002106096573785
Encrypted:	false
SSDEEP:	6:mI7REYsyZc7HbF4UrFgB8kKiDSC0N6AFhK6t:TpuF0MxBN6K
MD5:	6751A6478FD45245AD2A7D75834F88C6
SHA1:	FB52D116897A1908B3F27F2BFB03E33DD8749C39
SHA-256:	8293E83F020B5D9B8C7BE24729FDFC3CE26CA338AB9593EF0A00FA622DE22CD7
SHA-512:	9D95B9527F83B5C1AE465D2B2B49A18DF98F9BC31C774CE78F3B5B6C97987F4E74ED6244ABC38B36765C046B251CB5F98DDC27733F6F748076DBEBDF32377FE 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^...Q^....._keyhttps://covid.census.gov/jfe/static/dist/c/db.21026c4133e1c59eaf45.js .https://census.gov/..(.i&/.....$.....}.{.. ..[...xX.vD!....q.rwi.....A..Eo.....]. .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f703b502561aec6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	875
Entropy (8bit):	5.422309929555119
Encrypted:	false
SSDEEP:	24:xQ5FyfvZrasn4qqn+h5Fyftyk0ovTKT/9LG:xQ5FyEsn4qf5Fy15KT/U
MD5:	0076B1D78345FC46AAC69AA95BF5886D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f703b502561aec6_0	
SHA1:	88276C4AD96013DB7ECE8019783AC9438064B377
SHA-256:	8BF18BD4A3AF9045DA64433A160FAAE4822FF02C36DDAE9BB7F31F99E10C5CC8
SHA-512:	A408D096B233C6C78D5489DC3810E0ED89F6BCA5A9BD6F74B6B4410A45241A7D409CF92C5A72148ECBABA52D2377E47AD271F21A6DBC4997BB9709D98E9FA8 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^....._keyhttps://www.census.gov/etc.clientlibs/census/components/common/body/embeddableimage/clientlib/component.js .https://census.gov/..i&/..... ...u.....&....s.t..}.b,..$...._.w.0^..d.A..Eo.....Q.?G.....A..Eo.....i&/. .....'.....O.....h.y.....$.....(S.L..`R.....L`.....Qcf>.....window....Qb.[2.....o n....QbB..F....load.(S.....Ia.....d.....IE.@.-....xP.....j...https://www.census.gov/etc.clientlibs/census/components/common/body/embeddableimage/clientlib/c omponent.js..a.....D`....D`n...D`.....`....&...&....D`....Dl]d.....K`....Dm(.....&....&.]...&.(...&...&.....&.Z....&....$Rc....`.....Ib.....c.....@.....a.d..... .....&....s.t..}.b,..$...._.w.0^..d.A..Eo...../T:j,.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\132051c5fac8d7cf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.345616267319854
Encrypted:	false
SSDEEP:	6:m7QYGLKcoRMQSnmPZmQMHg/d3ZPaFX8K6t:M9hSnmPYQMo7aY
MD5:	E553DAC141847DE1F164258664EE4438
SHA1:	9E69BEB21DF4CFC0C405DA0EDA86A241AB0DE1D0
SHA-256:	E30A6AEC6742A248770549F0E744C8611B9348AFBCDFD013F23DD8FC07EB42C3
SHA-512:	3673E4C401523F22FAD36CD6F1BD8DC63496105380E4D27EBE6C6B81EFA8A82511DBD37C99963A2CC4864D0E0F0AD7AE0240778041473C347D90B9B47BD412C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...c....._keyhttps://www.census.gov/populationwidget/js/main.min.js .https://census.gov/....i&/....._.....k..PXt.....@oo..I..D.pk*..\..A..Eo.....g.....A..E o.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1331133c1df1a2b2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.725350948655628
Encrypted:	false
SSDEEP:	6:m5Yk+f2pomW0cChmJ2mg1CPNELK4lzhK6t:c++amPcCkJeSqLxf
MD5:	28A8E3562CAB9AD3BA884DFD7230EE1C
SHA1:	BA24DDCC169FF7E54426AC8CDF34DB3F350654BF
SHA-256:	F0D92D31BF5AF15CC48AC7BAA33763384C0021E7064DD38092B3D08C9096E2A9
SHA-512:	5FE67824077301492DC8945FBC74E40D7D664B0BDEE7ABA6B76A2AC3C97B8E10DE617F39794D8F061CC7D1E8F7C0AF7AB1E82F4931F0DCD7AC2268005468F9 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...jE....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iMoJ4/yl/l/de_DE/W_RRpqaK3br.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....pJ.....j Tc.F.%e.a..0.g#...'..5.B...<.A..Eo.....u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\176e7d1d913270bc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.446626680784107
Encrypted:	false
SSDEEP:	6:mwh0lXYGL+MIwJJwMuYtgRHSJilxhm4RtbK6t:dGlwvsJUDi
MD5:	ABEE19DD9883E48D82A70D55AA5F4F95
SHA1:	E871FC758332302DCAA6F1901630A9F1B564A584
SHA-256:	2E64FA93747510D6B0C8DA0FD26FAC9BCB89903C2DA76A5ACACF8ACBB7F5510C
SHA-512:	05BBD26DD8491102A77781FC4A91245DBC59A6A6C8B6D7517D4ED97E13C6088FC30915F0B9C6BE8E6923C2AE5CE37D49FE6B208477FA0FCCAD87B831938A01 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.....I....._keyhttps://www.google-analytics.com/analytics.js .https://twitter.com/.J).i&/.....].....:.&..L...jC...1UR@u<$mz.B...u..A..Eo.....6.Q0.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\185f65919f8657a6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.73149472841564
Encrypted:	false
SSDEEP:	6:mjtgEYk+f2pomJ2iGyhmJ2HFgp18JwfrHrxlDK6t:eD++amJ2ivkJ918GzHlr
MD5:	F0B85ABE3043DA3CDD5DC92E302A5FE7
SHA1:	84DD46C294B9A472C596337E7E75672CCB7939BB
SHA-256:	FD4C8E36486804087E81EBB073B3A233B5DB2592DD931DAB06B7F5035F0400F1
SHA-512:	27863DE497237303937E4691236F8E0E71BC29432D74038FB0ABC8CBCF0EA5FB70A0AD0BB628A7B57A4E5E2388E361E4C7517C09A2252A4EA2DBA778DCA69D5F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y9/r/ugD21mPGNBo.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....L.....#...._.l.....).....~...._..b.A..Eo.....b.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ada5ae8963a52d7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.712891510086985
Encrypted:	false
SSDEEP:	6:mhl/lXYk+f2pomdMCWXewhmJ2kg4uQ1nAFjnK6t:IXz++amdzwkJVuQOjp
MD5:	C83D49CCE8C2107806436D89F9B07686
SHA1:	A462A4CC23834D5AB07472D2D743DF20EC03D7F5
SHA-256:	5A60500388164BB2C9D590FFE9B2DF423B5A7CB02495B37AA703EFFC9E526108
SHA-512:	9986BC265603A01AB362CDC2507FFA40DF5C86EED7820486E9602A0A208E87858C4FE112F05B4E576056FB17F4B6281641249C90B5070AC24DB99C5129E75985
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...J..V...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yv/r/GG1Y0sYc7My.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....NI.....i...c..<.%...7.....T....#.!..-.A..Eo.....[.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1e5d871230df8081_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	285
Entropy (8bit):	5.629462243702949
Encrypted:	false
SSDEEP:	6:mY6EYcv0KgJXZE2gVgAzMwARs1dWkvySpUygV9JkrPlzlhK6t:UfKt6if0s3p
MD5:	AE77F3544FFB6F9737BC7C3A37F2F902
SHA1:	D7285542915D058168A2ED0CEA275003F96B261C
SHA-256:	3F4D4B2113AD9D206310177264F918E2F786DEACC9AB570FFEA24139C041976C
SHA-512:	17878D0935F05499D6463AC0777C9A3D95671C6466717EA83886F1A89229745F0323C03B424D512717585798F6DCC263CA72171031DF3CCBB5C37C0007074614
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://assets.adobedtm.com/526d5084b7f8f688ea81a3aba09755d76a81f8e8/s-code-contents-6eafcaf24c53a8340cb08ca3a89da5a57f80a8cb.js .https://census.gov/..\.i&/.....n*.....^(r..|{^G:.U..+e..U...L...]M..A..Eo.....!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ec07728a6888289_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.625479686006093
Encrypted:	false
SSDEEP:	6:mLYk+f2pom0LmhmJ2gPugtWcus7q0BK6t:+++am0SkJn1fxb
MD5:	80B720F7C5D98A7E079A90525D8D6E00
SHA1:	E5F3D07B92BE7170629B8DA86E3EB7BB59CBF78C
SHA-256:	733180B68C58C3505B3F0CAA6622BB67112191856CC96C263A025F329D320257
SHA-512:	E6FDC2DC7DC3878861355C9E4F709B7EBB4DC3912FD9FE95E7A24A52314B2221ACA1153D984104808E7603183913EF42647CD18204896F5E880441859148DBD0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ec07728a6888289_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yC/r/j1y3xWkFSrZ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.$..i&/.....HJ.....Q....hn.pm...B...y..r.m Z..:v-.A..Eo.....i".....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c96d87979400e66_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.460446135159205
Encrypted:	false
SSDEEP:	3:m+lz/5OA8RzYRhmHT8NWQA7sxdFvDGLXWGhil/lHCxOjT11+MXClF6g4ml6pK5kt:ma2YSHT8NWQAgmhGgEvj+oCGAloK6t
MD5:	6D052A63BE3EF21C4B5E066BA323E525
SHA1:	A38178A823EA1692260DBB42033574FB88D5A2AE
SHA-256:	626F87216BAF76107E82C7004E03C4B8D96F59A3B30F0714A06D54C52D77EEF8
SHA-512:	0E81C741BC14B31A777A62CE322B1E9D0C913E8BC4063A61E30E72A16E1745EEEF66E119DF2564D607AEE249BE1A2D7780A722B24025FEC2B69BF3249E91204
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y....._keyhttps://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js .https://census.gov/x...i&/.....'.wq..v..I.Jec...Y.7..*..".jCc.A..Eo.....y2..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2da09afdc0937f28_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.6063644171812586
Encrypted:	false
SSDEEP:	6:mYUYj018IrAzyvLdXMsDugVvNvSH9hv/ZK6t:Fg1t/LdDfv9SX/T
MD5:	BFB98A20A6497DF4F7BA7892923FF8B8
SHA1:	20E6B32A4E69B23E57FBC98389343114288E55BE
SHA-256:	E723C50A3C2EDB9AA1AC50811198958307DFCD5D0337B665BB62CAA170100D83
SHA-512:	4FE168EE62030CB3F84DC14064E1E07981C8190F425E1338504D2417AF09EFB047BF7F258F8AC2E3D3FA7895DD2EFEF9B72DB608724BF4A6F0AD4285DDDB7D A
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...b&....._keyhttps://abs.twimg.com/responsive-web/client-web/polyfills.8133b945.js .https://twitter.com/...i&/.....W.....q0G|.eJt....L.....*H...'.S.{...A..Eo..... ..}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2fe0a2000559c66a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1897
Entropy (8bit):	5.791622260074858
Encrypted:	false
SSDEEP:	48:f5FM+F5eMvF5BMwF5TMIF5yM0F5u+eMqF5HMDr:f5l5B575F5Q5ze5g
MD5:	B9BF7AB79F279EBA0A1CE9C4F71AD077
SHA1:	6A219CA537F566CF8352CAB17704C6D9270969EF
SHA-256:	6D973C9E114D56C2D987C8ACAC50E7B99EAACCC8A2BFF891A83E59001F1FA1B8
SHA-512:	4BA6C5115246C25D02AFCA99D5FFD97871B9E13E48C0F845497445CD62FE00059C220CC0585B5632662D94C292FBB31566C8BF92A39EA19635992D3E5AF8A6D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....'....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement_Module_ActivityMap.min.js .https://census.g ov/.Z..i&/.....f..=.$.4.....D<Cv ?.X.$KF..A..Eo.....p.....A..Eo.....0\r..m.....'....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e5 40399dcc1f8208860b7b/AppMeasurement_Module_ActivityMap.min.js .https://census.gov/....i&/.....".....f..=.$.4.....D<Cv ?.X.$KF..A..Eo.....0 $.....A..Eo..... .....0\r..m.....'....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement_Module_ActivityMap.min.js .https:// census.gov/....i&/.....f..=.$.4.....D<Cv ?.X.$KF..A..Eo.....h.Q.....A..Eo.....0\r..m.....'....._keyhttps://assets.adobedtm.com/extensions/EPbde2 f7ca14e540399dcc1f8208860b7b/AppMeasurement_Module_ActivityMap.min.js .https://census.gov/..M.i&/.....'..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3246d48cc43e7d5a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3246d48cc43e7d5a_0	
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	6.2785282838842384
Encrypted:	false
SSDEEP:	96:GPIyUHV7jNx6SswK9Tp+3e3j1d7a31q7TnEoyf+IFiA6mM:GPIpHRNU9tp+3eRPX/yfVi2M
MD5:	6D6E062BD965689C9B77BF6EEC28CF50
SHA1:	1C233B8257FC46A4CE147700CC0418FB29FBF639
SHA-256:	815CE0EF3F2D3F78096CC45F988B4EDEECA57296421A4351A5602E58F3AAE7E2
SHA-512:	A52528099662421 50E1659A748A65F995F06E3B4F8A1E510539C2E1099BEC364BAD91A4C5515B129993E95676E4C57AAE17E361FA85E2A3A3291754C00C089D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K...J....._keyhttps://www.census.gov/ratingtool/js/ratingtool.js .https://census.gov/5...i&/.....0v.qj.4.v.....X....sW....?_....A..Eo.....O.PN.....A..Eo.....'..?....O....0.....K.....(S.0..`.....L`.....(S....`.....i.L`.....RcD.....Q.@.5nv....jQuery....Qd..x.....CODE_BASE.....Qb.JW.....PAGE..Qdr.....PAGE_TITLE....Qc..BG....rating....Qb...7....os....Q.@N.....browser...Qcz.B.....device... Qf.....digitalDataPageName...Qc.}x.....textArea..QdJH.....delaydisplay. QfzFD.....scriptLoadHandler.....QbFf.....mainl.....l`....DaB...4....(S.....Ia.....!.....@.-....@P.....2...https://www.census.gov/ratingtool/js/ratingtool.js..a.....D`.....D`T...D`.....`T...&...&....&.(S.....5.a.....Qd:.....script_tag.....a..... Qf"".....onreadystatechange..a....a...I...q#d.....&..."&.(S.....Ia+....?.....d....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3478c12dca436e2d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.6674294085903725
Encrypted:	false
SSDEEP:	3:m+lYm8RzYkwLf3G9LomYI207G3V2QufRJ2zxJl/lHCsolqeprlzt46XG8E6RmVxH:mdYk+f2pomTyhmJ2zFgV9ztBmVtK6t
MD5:	B22D537613E1F5A2281AD3AE26FCC37C
SHA1:	33563E0021308BCD97FCF49565379546B6F5DEA2
SHA-256:	08CF0D9F6785E868FF68C4808B882FBC701EBE194CF79B2FCD1001CDCCA2F835
SHA-512:	113AB8186D54D6ADF86B47055335B9129849086E5E5EF22DCB0D46D51D5CD4C71502C8DC82CF02D682CAC7E1975982233B6DBB83E7E1F1C00075F6A640756D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....z....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/ys/r/YL6q3hajciu.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/%...i&/.....K.....K...{..B..:&MM..FV..O%..r.....A..Eo.....x.t.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\37f4aff035cea44a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1395
Entropy (8bit):	5.541985590160896
Encrypted:	false
SSDEEP:	24:x05Fy1HIH/4TVblOAgzRKrgW6/qi+h5Fy1HQ/TF4eV6AXlmo8:x05FylySVbQtYV6/qb5Fyl2wAXA5
MD5:	41D0BBE0D0EA8ABD8E24C9AEC50086CD
SHA1:	07B1F4F466BA82122BBAA0D476D13C7B6537CD26
SHA-256:	236E98800B8EA874EBBEA0E4E7251EBEDD5220E31F8E91CF57C44AF6C6CB38A4
SHA-512:	9DA892ACB9CA06269961FA0165D500F5DB5AA309408535CD9061380D98D2AB1D3CA18C131CFA9C0701AB77B562E48603A93A3697E7CF260F1755B64B0227A46
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<....._keyhttps://www.census.gov/etc.clientlibs/census/components/common/body/expandablelist/clientlibs/component.js .https://census.gov/...i&/.....u.....7.....?d@..w&.."9!.".geY.....A..Eo.....T.....A..Eo.....i&/.(.....'.<%....O.....^.G.....(S.T..`b....$L`.....L`.....Qe.U.....CensusAccordion..(S.L.`T.....L`.....HRc .....Q.P..cY....digitalData...Qb.9I....._.....QdF.-.....accordions..c$.....$.....I`....Da>...2J...(S.....Qe^~.s....initAccordion...at....$...d..rC.....).....).8...8.;....<.A....B.I....$.....d.....d.....d.....d.....e..... .... .).....a...Q..@.-....xP.....j...https://www.census.gov/etc.clientlibs/census/components/common/body/expandablelist/clientlibs/component.js..a.....D`....D`I...D`.....P...`$...&...&..!.&..q..D`....DI]d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3a21ba0f0788745f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.4052386828389265
Encrypted:	false
SSDEEP:	6:mKXYEbZcXB6FVI0KoHgY4zYm9wArqhK6t:D9wB6F+zoj4n9wh
MD5:	3BFE206CBF5554FAC34177C419535517
SHA1:	6F0DEF4FBBD5A7E7EAA4D36AA261DC7E5B080A85
SHA-256:	2D98A84D154905CC0134F5A20C0EDB67C0A900DAA2FEE7F04CB1E7245DB88643

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3a21ba0f0788745f_0	
SHA-512:	34D9B3C92870BC4803641A0D7AE5C9F72DAF8335D9B99FF3F503ADE9EF3C7EF6E971F41869BC9BF37150F4B5785E2A58E7789F062ECBD7F586BAECBF4B8A759 B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J...v;)O...._keyhttps://data.census.gov/cedsci/js/app.3dfc6147.js .https://census.gov//.[.i&/.....i*.....Af.u.T.}}..-..}.a.k.$..`....A..Eo.....'{.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ae63f4d9678bfc8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10080
Entropy (8bit):	5.908466069615636
Encrypted:	false
SSDEEP:	192:Yw74nj8NPdq1cAx6P9R+R8SsQSqmaFXLD3E7OPq9w63lxqbhPja:1A9xsgph1u
MD5:	FB1888010360752194AFB735DF497A7A
SHA1:	44A09533AC340F21E2F060BE18F319B658523831
SHA-256:	80C9AFEBC04C40CFF30248BCCFBD5B0B41062C89084EA4021780B20151E1A353
SHA-512:	162B4A55F9698A9345AA8443C40C82EE79F9582CF719B1CA2AABC4C1F6A9E42C117966487AED23F67609C32F8B503108EE365700CF282E0F453296CC2EB3B62E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X....'.2...._keyhttps://www.census.gov/etc.clientlibs/census-core/clientlibs.js .https://census.gov/.$..i&/.....c..A....0|.M....q.q<.An\5.A..Eo...../..... ..A..Eo.....'..K....O.....%.....t.....(S.!...`.....lL`2....(S..`.....|L`:....xRc8.....Qejl5#....dataLayerEnabled..Qdj.B.....dataLayer.....Q b..,....NS....Qb.....IS....QcR.....keyCodes..Qd..z.....selectors.....Qd*a.....properties....Qc...9....Carousel..Qc.e.!....readData..Qe..D!....getDataLayerId..i..... .....l`....Da.....(S.....laD...xQ.....'..@.).0..@.2.9..@.:.L..@.M.\..@.].^..@._.`..@.a.b..@.c.d..@.f.f..@.h.l..@.n.o..@.p.|..@.}....@.....@.....@.....@.... ..@.....@.....@.....@.....@.....d.....$.'..@.....(.h.....;.>..@.?.C..@.E.F..@.,. .....d.....@.....a...!..@.-....LP.!.....?...https://www.census.gov/etc.clientlibs/census-c ore

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41aaa36d588890d1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.65892578652173
Encrypted:	false
SSDEEP:	6:m1FXYk+f2pomWSxzhmJ2+ygD/0Ix6bo5MDZK6t:qFz++amWUzkJJPx6boKT
MD5:	E4F9BD2C4F93D0CD628D5BB061FF3E62
SHA1:	0BF49E3D84EC68590D92750995BB87DC490AF59C
SHA-256:	79F3469001AF19C22A8C55211FD61ACA7C99FDD30AD5D20057B047C451F3D7C5
SHA-512:	93FC134CC4EE8782F1203CF34F15BE8B799FD838687F57B434D6C3DB2C01EBDADEF844F147224D98AA99E54BB36593E5B715AD514EDDDC130EA3267364624F 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....P...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yI/r/aYA1p2v5mas.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....J..... .[..u-T.v2..w.p..K !.Y[..6..A..Eo.....<.W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41f98b55e263f84f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.562688186350506
Encrypted:	false
SSDEEP:	6:mUb9Yj018IrAitpM/oFgItB+rzuEhlbK6t:pJ1tHtRBtBO
MD5:	7046314BE5B5D8BC214EF7629D968885
SHA1:	040414986C1944CABDCDD2CD80C98CC311770E42
SHA-256:	8C637660B2AE7FE8CDCD365B833E126F1DDAE768C1E67B1C87FAD9C43EBC7F81
SHA-512:	D61732F56FDAE39409DEA9DEF8BB98C14F0C2F2F190825E7858C426A48B7E8DCDB6F4CF7507B1B18C6044BB1B8450F02E5A4DF478EC9F24A356A2707041606C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...D.5...._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.IntentPrompt.58278755.js .https://twitter.com/`.".i&/.....y\.....o...[.V....G..?6CP.. 7..SQ#.....A..Eo.....M.W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\43e92767e44f49a4_0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\43e92767e44f49a4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2683
Entropy (8bit):	5.561788767610054
Encrypted:	false
SSDEEP:	48:b5FZXroxAH0PgnqnW5FZuc1ZEDZAO7r6OYGpR5JVTZZeDLq8LtfLwYy0dJ:buxAHIA+2FcDNrhY2kLqcLr
MD5:	8773796C741CA71E1FCD406A26B911BB
SHA1:	FA5F9DC33A96F7DF94FB492216C9CBFFE108E6F5
SHA-256:	6E7D55D09A929FE30773AB868A66C7BA23F8E62D83026FBDFA824C88938E6F1B
SHA-512:	D5BE5BAB6E370DAC48F65BEC0A98BA63907CB4704B9133204B4C2C52E8663B2A1D1CAE0FEAE35AD5CBD83034D4A4707A14DCECCD8092CB7E5E254FEB8564 64B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....A....._keyhttps://www.census.gov/etc.clientlibs/census/clientlibs/universalheader.js .https://census.gov/....i&/.....7.....8..9I.....-g.]9\.s.<68.6S.EZ^r...A..Eo. .....p.....A..Eo.....i&/.P.....'..U....O.....(.....(S.P..`X.....L`.....L`.....$Qg.....CensusSearchTypeahead....$Qg..C.....CensusUni versalHeader....(S.`.`|....0L`.....HRc .....Qc.....apiUri....Qd.....resultUrl.....Qd.y0R....isUSASearch.. Qf:.i.....onSearchFocusBlur...c.....l`....DaR....t...(S..... QfZj{$....initSearchTypeahead.a....p1...@..k'....."....".[....[._....a.b..... ....d.....d.....*.... .f.....U.....d.....%.U.....1.....@.-....XP.Q.....J. ..https://www.census.gov/etc.clientlibs/census/clientlibs/universalheader.js..a.....D`....D`V...D`.....t...`6...&...&....&..A..D&.(S.....a.1...8.....a.d.....&.(S....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4566c632b7d2b0f5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1389
Entropy (8bit):	5.432775859044565
Encrypted:	false
SSDEEP:	24:VI5FyyIqLa8jEo+Ihjqoh5Fyy8xoQAPxcF4V64K3XVajTeQz9Sa8jEmc:q5FyyFL1EohhjR5Fyy8x2i+VPK3XASmD
MD5:	3532909E0D7F1599ADEB44E49ABA23EB
SHA1:	A89A8CC58F92EADA69ED40CC07DEFF65665BB8D6
SHA-256:	57C70834C4464535A8AF7DC160D2C0258B0E5E147E53DE0EDD3B63809C100784
SHA-512:	E601166755267E9C875B7A3C2B8DB69198A691E2681FF80A91AB562AB20FB3390F76D4A9806B3643DC867318AAD4289242A2C727791DB12627C0EC78D10A73FC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....>....._keyhttps://www.census.gov/etc.clientlibs/census/components/common/body/languageselector/clientlibs/component.js .https://census.gov/a...i&/..... .....u.....f ....RGR..?.X.eh.&.../'..._x.A..Eo.....,.....A..Eo.....a...i&/. .....'.....O.....).....(S.T..``.....L`.....8L`.....(S.....Ia....z....$Qg..% 9....lanaguageSelectionClick..E.@.-....xP.....l...https://www.census.gov/etc.clientlibs/census/components/common/body/languageselector/clientlibs/component.jsa.....D` ....D`h...D`.....0...`....&...&..A.&.(S...Ia.....$Qg...`....handleToggleLangDropdownE....d....!.....&.(S.....Ia8.....d.....$Qg.X.....toggleLanguageDropDo wn..E.d.....D&.(S...Ia+...9.....Qd.K.....onKeyParent.E.d.....&.(S...IaN...R.....QdR].....onKeyChild..E.d.....&.(S...Iaq...r.... Qf.....moveLa nguageSelectorE.d.....&.(S...Ia.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\464a508e9dbc3c5e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.667319952874427
Encrypted:	false
SSDEEP:	6:mcVYk+f2pomtzhmJ2brg03ZxeeA+4yRK6t:J++amtkJa37M+h
MD5:	E3A4FFA16D18438B9973A9486867BD65
SHA1:	04947922EA5CDAFB24DF1B4D10A2B27FF9FCF784
SHA-256:	87C16366BEA21A68585A5B78B5E0E76DD519919E2A84E5D246610FE68DCCA1D0
SHA-512:	71C03FF35BB42313D67D6CDE5DBDDCC79F267F6465972EF67B568682FE43C6F428534DF2DB68CEEF2000795AFA40A5C5BDA42257A5599F2DBAB228531F8B76F A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....i)....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/ya/r/f_1WzHb-Lka.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....K.....q..U.}.\bMO.V.q...{p1.. ...K..VI.A..Eo.....?.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\47419ddc3ca4bada_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.57301342977817
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\47419ddc3ca4bada_0	
SSDEEP:	6:mAS9Ykvwy1O8lzNNNjgpJy0MD9hvY5K6t:zevwynIzNNNKy1D9ZYz
MD5:	6B1A51D6DAB00F851B7E0C30F9E6A53C
SHA1:	FA4D3766D342A9E5C4C7D02D7E044B0C20BDDB2E
SHA-256:	1624B316D670EC6ADAFCF67B07DA2D2692357BBC9AFE905290124F686B6B8362
SHA-512:	3BDD49E4140A0BB5895197FB6E8A0D687AC15486256FCFB03AFAE5E2FEC3839BCF2B776ACD427DE288A21F10568E4F6F7D3BBA9DAA479B686FE617D93E423E02
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....=....._keyhttps://static-exp1.licdn.com/sc/h/9x1ka0d4advijnuxgxnyns6ne .https://linkedin.com/..F.i&/.....f.....B...?.H.l.LY.\..i..E.WT.`wA....D.A..Eo.... ..6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\48cb7dc9e41ececc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.520226114691325
Encrypted:	false
SSDEEP:	6:mAYj018IrAmHPxMnIgQllRmaQ0xx/XK6t:t1tGimaFh
MD5:	8DA4860EF4603C517D566D05ACE78666
SHA1:	F7DA036C1DFE6054D696820DEEA96BC2D4C570B9
SHA-256:	8D3FA69BCEFAD0A5CEA62D98BB494AF34EFEF2F8BA52E4EBFDC44B6E599117A5
SHA-512:	8FD16D4B003067BF91A8D2E64B96F55974B593B1122D6B513B968CF6541F41252F634342DEFF08A9050D1C557A2B18ACC56D31BF3B96A3260193ED93CD7E2D60
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...a..J...._keyhttps://abs.twimg.com/responsive-web/client-web/vendors~main.3922ecd5.js .https://twitter.com/(...i&/...../X.....zQ.....A.a..1ek._.....n..! ...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5047ffbd2b109760_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.754331547131712
Encrypted:	false
SSDEEP:	6:m10XYk+f2pomW8AOwMNzhmJ2qxMyg9U/PhAEHRK6t:j++amcO/NkJZxM7U5r
MD5:	98478671FBC73D3DC478E08D59DCBC62
SHA1:	91D8CABA02D93D0C2003B06755ED5133A15BDA49
SHA-256:	994B2BCE1B595FEC922AEAA69B13DC4EF32870359A4CC6FD65C6858004E0BDB5
SHA-512:	8403E8C740A8FB0F9723C6A31FEABABDCB3EAA7BD2AD2828B0DE4F6B003CC8548E88C5D3C5C6688410E9975F52BDE74932E3F3F340ACE877927DA4B00B15EEEC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...Q/....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i2UN4/yn/l/de_DE/uQc7ePrylz3.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....vL.....O....4<.G.G #...u.....'.bR.9..A..Eo.....{:.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5118acef9d6064ea_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.641984088543261
Encrypted:	false
SSDEEP:	6:mEiVllyEYVb2FIBFM4B6fug33wEQgquhyAanK6t:TiPIpnB240w5gquhyjp
MD5:	F1F9B48C3B6DE7E528F6F300B1FE14EE
SHA1:	7497D8EC76510A9A2AC81BA70A12D38E26C1A668
SHA-256:	A0AC1E85E9B14C6EC45836CBEA0665381430914126301FFDBCF5263AF4FDAC2F
SHA-512:	499325231D5F5FA7C02371F65A5E6D4812DED835EA8D175E30EF9D3196CE7A28E9BDA57DF6C7C5BAB9599E4D58BCB2D3FB76F888DE451E156BDD9368C190158
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X....._keyhttps://s.go-mpulse.net/boomerang/N5F9F-5SXNV-TJA4F-B6CEM-65LXH .https://census.gov/_.].i&/.....*.....ne4:...c..e8...}t..X....a.+....A.A..Eo... ...)v(^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\51549337b845bf55_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	18905
Entropy (8bit):	6.427919134432923
Encrypted:	false
SSDEEP:	384:0V7uB8XpwkdgpPUFneCDo1lBlxBquTIuvJcAEnm2:0HTapsReCDSlBlxBqibvJZEm2
MD5:	119F5AE07FBD07F766B5D4DF6295693D
SHA1:	27A3A41E9CBFA1E5149E83E522409AA9C7C6E665
SHA-256:	AD78C59771138FA620AAC63F728B6CB8D1FA5A2DBE140ED1C1972DA1363177D6
SHA-512:	3E77E6B61693B84EF4432A8E2D3F34EFE0BAF0E65D267CB82CD1652199317E74D8DC3A4381EB87D01C7DA26F88001FCFB28E7910E041552A177CCB2849BDC8E3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q...8.X....._keyhttps://dap.digitalgov.gov/Universal-Federated-Analytics-Min.js?agency=DOC&subagency=CEN .https://census.gov/-...i&/.....E~F2...I.....=.Ap.Ey..dF.D..4.A..Eo.....;m.....A..Eo.....'.LI....O....0H..~?.y.....\.....(S.....`X.....L`p.....L`p.....Qc6.&_....oCONFIG..(S.<.`4.....L`.....Qe..Z....._updateConfig.... Qf.p....._defineCookieDomain..$Qg>....._defineAgencyCDsValues....K`....Di.....&.\.....&.\.....&.\.....(Rc.....Qd.D....._onEveryPage`....Da.....c.....`...@..@.-....dP.....X...https://dap.digitalgov.gov/Universal-Federated-Analytics-Min.js?agency=DOC&subagency=CENa.....D`....D`~...D`.....`D...&...&..q.&.(S.)..`.....@L`.....PQr.&..D...(([^.\/]+\.[^.\/]{2,3}\.[^.\/]{2})|(([^.\/]+\.)[^.\/]{2,4}))(\/.*)?$..Qbj.Kr....test..!...Qer.....SUBDOMAIN_BASED.....QdR\&l....toLowerCase...Qc.....replace...Qb.v4.....www.I..Qe6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\540527e51a0c22d9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1414
Entropy (8bit):	5.531291261550513
Encrypted:	false
SSDEEP:	24:iIQXWLq1oIQhWa1oIQyfWwc7oIQjWDoIQ2WxoIQIvW9oIQZWl:iLmLq1oL82oLyewc7oLKDoLtxoLt9oL6
MD5:	1183A5DBD622E0CDA0902944906EE84D
SHA1:	8660131FA83967A1CC5D9D1D2D3DB7BD8F70F5FC
SHA-256:	0A08DC08E7AAEC614F7FA90BA319E5B3A7301173A82D8480D440EF8F5CAF8FD4
SHA-512:	F1FD54D66EDEE94E3BB3D1F3325D6D442777C0D0B698E1A91B081744FFEB9DEA145B566030054AB23D456CBB7AA03877113F46D9D33A566A64CB545150802095
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F....{....._keyhttps://www.google-analytics.com/analytics.js .https://census.gov/....i&/.....N.OS.J.w.....D..4..\.....A..Eo.....j.....A..Eo.....0\r..m.....F....{....._keyhttps://www.google-analytics.com/analytics.js .https://census.gov/Y|..i&/.....s.....N.OS.J.w.....D..4..\.....A..Eo.....(-.....A..Eo.....0\r..m.....F....{....._keyhttps://www.google-analytics.com/analytics.js .https://census.gov/3Y..i&/.....I.....N.OS.J.w.....D..4..\.....A..Eo.....F.....A..Eo.....0\r..m.....F....{....._keyhttps://www.google-analytics.com/analytics.js .https://census.gov/.Rd.i&/.....+.....N.OS.J.w.....D..4..\.....A..Eo.....$.....A..Eo.....0\r..m.....F....{....._keyhttps://www.google-analytics.com/analytics.js .https://census.gov/.9..i&/.....7.....N.OS.J.w.....D..4..\.....A..Eo.....Wz.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\54d0f9e9d776bfe7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1220
Entropy (8bit):	5.58553838116629
Encrypted:	false
SSDEEP:	24:rd5FyLyUrz9s0O1Ck569TxTSEh5FyJWF4eVseZDgX:rd5Fyvrzqvok5QxV5Fy+GeZDgX
MD5:	717AC6C23673C912CE4BC316FEF52B46
SHA1:	E33C34CF50583D37627B563B67645C4CA32D3EE3
SHA-256:	1E63390DAFFBBB44E54F5D777E12B34080B1D936D6A1DAB25FC102B8FBF0A17E
SHA-512:	4D22343A39E7E61EE2A6A079FBD4B1900D22678C84F4DF2794EABA08F10694CB2EF6F56A5CCC2DCB370BCB39D759CE812BEE6FBF9A456F84309C33327ED3F33
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|...'....._keyhttps://www.census.gov/etc.clientlibs/census/components/common/body/carousel/clientlib/component.js .https://census.gov/...i&/.....v.....t;...,R".....i?K..x.c.....F.A..Eo.....A..Eo.....i&/.....'.:.....O....@....q.....(S.P..`X.... L`.....L`.....Qe.....CensusCarousel...(S.H.`L.....L`.....@Rc.....Qb.9I....._.....Qd.....carousels...b....$.....I`....Da<...66...(S.....Qd.....initCarouselab.....@..m.....!....!.5....!*.....e.....!..@.-....pP.....c...https://www.census.gov/etc.clientlibs/census/components/common/body/carousel/clientlib/component.js.a.....D`....D`r...D`.....4...`....&...&..&.....D`....DI]d.....a.....C...K`....Dl.....%...%...|.....&.}..)&.%./...%.....b.....s2.....d..... .....Q.@.5nv....jQuery....Qcf>.....windo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\55b1cbf4cecf862f_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\55b1cbf4cecf862f_0	
Size (bytes):	31189
Entropy (8bit):	5.733779188913716
Encrypted:	false
SSDEEP:	384:a32Yic1b76No/6Gg6Lgzwu/steCIcuBNpsv+PdmG+xjDax3Zg0suEuDDP24qi/Y9:aricBS7wdU3vPaxva3i0sJuDDP2klq3
MD5:	CE6F725EC54149145AB421278708EB97
SHA1:	805655CB6ACBE8B848155647EE75DC61F08F1CB9
SHA-256:	EAD1EC2BD16852D3406445923862C9CA169707A1BD355F6766FB6B9607E647C1
SHA-512:	73CFE0501BFF3B3F3BFD3E7E61E116CD396A253AAAB6E67F2A75F09725897358E59DD8C302EBA5A691FA82D1E220A1D59D7850EB3A563B6190E76D82FCDF1C4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....r.Z...._keyhttps://www.census.gov/etc.clientlibs/census/clientlibs/modernizr.js .https://census.gov/...i&/.....r.....~b....-L..V(d.gF..M.....".A..Eo.....".....A..Eo.....'.0.....O....8x.....d.....(S...`.....0L`.....Qcf>.....window...(S.M..`T....I.L` .....Rc.....:.....Qc>.,.....document.....Q.PF.&M....Modernizr.....Qe.AK.....enableClasses.....Qd.U.=....docElement....Qb..e?....mod...Qc..G.....mStyle....Qd.Cy.....inputElem.....Qc.....smile.....Qc...4....prefixes..Qe.k.....cssomPrefixes.....Qd.+/.....domPrefixes...Qbn.n.....ns....Qc.A. ....inputs....Qc...{....attrs.....Qc&.....slice....$Qg.....injectElementWithStyles...QeB|.....isEventSupported..Qe"ug....._hasOwnProperty...Qd..j....hasOwnProp....Qc..j.....setCss....Qd.)z....setCssAll.....Qb.q.9....is....Qc.....contains..Qd...f....testProps.....Qd2jt....testDOMProps..Qd:..M....testPr

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\591c9b3fbc124fc7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.533233404951724
Encrypted:	false
SSDEEP:	6:mIYj018IrAkh6E0pMb+1tgK/lW7s2Kz2nK6t:V1tv6jkulCzKi
MD5:	3C0AD6C3BB68E79068FF631DE9170C80
SHA1:	038A4F19BCAE228C3B91BF045F9264A6197B32EC
SHA-256:	0159BDE92C343972E4F3D82A6A1B25743EB113C4A60DD5ADEA27EF52F5A8DB37
SHA-512:	16D6D5EB83EFF598BBCA0DCCC91809378BB7D2E970D3F95482AB365E05A350C2C52B1E9F6C5B477256FE2C4F448FE62E1FCB46BF1EA3E260636A2D5EA0D5A388
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...L.v...._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.emoji.en.2314ed55.js .https://twitter.com/q...i&/.....z.....F...jH..:N.H...5.y.W....?.p.....A..Eo....._.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\592b770f27e6978c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	617
Entropy (8bit):	5.463705509503172
Encrypted:	false
SSDEEP:	12:k5OaN57Yml6OaNYdOaNKz8lgOaNg0gOaNDJsUPOaN:KO67YZO/OrTO10gOHQO
MD5:	CBF14C7AF3B8B23CB904368C7F8EE8AF
SHA1:	A9E069F3007EBBE1E90CA7159E5E476F55718D34
SHA-256:	04F3C15B50D4140CE7C054A37E96D4E2C598083855FF07D3A1C8E819310B4AB6
SHA-512:	CCC01A81C32A666DBE4EDFA231CF5A53146A758123F456D5B2AF2B6AB4E088B2E81690C4C08E2BB06FF14B4FD26CF13FE5A3E2F5618FB954C1C3C4D789753CD6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A.....q...._keyhttps://www.gstatic.com/charts/loader.js .https://census.gov/....i&/.....iW.r.i1....."....k7 ...Z.I..A..Eo.....U.d.....A..Eo.....i&/.....B.....iW.r.i1....."....k7 ...Z.I..A..Eo.....i&/.....iW.r.i1....."....k7 ...Z.I..A..Eo.....=.....&.C.i&/.....#.....iW.r.i1....."....k7 ...Z.I..A..Eo.....;.s.....?5~.i&/.....2.....iW.r.i1....."....k7 ...Z.I..A..Eo.....mk.....p..i&/.....{.....iW.r.i1....."....k7 ...Z.I..A..Eo.....V..M.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\59e0bdc12996c6e5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	245
Entropy (8bit):	5.596634580789476
Encrypted:	false
SSDEEP:	6:miL9Yj018IrAETJcpuHxEpMBtg4qRjSSWDBsYSDK6t:11tnS8HKY1qlLIBs5
MD5:	BB861C4FE58C83A648037369BB0B6EEC
SHA1:	3E6508A84C42A9216ACB9B1677DAC723A35C6655

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\59e0bdc12996c6e5_0	
SHA-256:	7748803D6F9C374DE16BC909C4D3EDF2F220E6EFB19ABD0179598905B14BCBA4
SHA-512:	86267006C0564927371B88A6EAE3697E975AEA741C4CA62E34348AA48B7F5CAFA51C0B369860F4BB2144B04142D7C124E19B39C460D378A76E46D4F62DF0A7F3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q.....9...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.AudioOnlyVideoPlayer.a88130e5.js .https://twitter.com/....i&/.....[.....^Bw1..I..8o. .....j..".s...A..Eo.....}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5fc2b8525e298fff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	175616
Entropy (8bit):	5.687513107842121
Encrypted:	false
SSDEEP:	3072:Ue1rEpd6OEkALpK5sUO/wDrpPrpoxgC7fcsUAuKagkyixiCguDD+wOrujmCG9ZJR:UVdPWmDSrIDkJXR59
MD5:	F8CBB3E70AA5E67A4AEA9AAC3E544034
SHA1:	2F6A6D82EC7BD17F734CCAC3FD9E7012A2582A42
SHA-256:	C6E9B7912F200C0D054F94D3F8366931EECDBF541BDCE3CB6786122CCF226255
SHA-512:	AC215471923A7430BEA1CCE4E46EB63DFE0DC7180165D3F4B0C4EF0A9B32006BD943E9E8547333C2D8EE58C6911116290563CEBB82C3B4F68D3DA8CBC27249C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...2.....1D895B4A26E2DB5F2F7767F2585499DE286A146B9A191841DBBC7F2B834FFA06.....'.:.....O:...H.....4.....P.....4.....I.... .....h.....4.....(S.I...`F.....L`N....(S....`.....L`~....XRc(..... Qb.....uuid..Qd:=.....runiqueId.....Qd.....focusable.....Qcn.G.....visible.e....$.....I`....Da.....h...(S.....Ia.....q...q..@.-....PP.1.....A...https://www.census.gov/etc.clientlibs/census/clientlibs/jquery.js...a.....D`....D`....D`.....`T...&...&..Q.&...(S.....5.a.....a.....a.....Qbn.....fn.....a.....Pd.....extend.focusa.....d... .....(.....d..... .....Q.@*.T.....focus.....q.....d.....D&.(S.....a.....a.....a.....a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6214889f7c2e82fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.699152894547791
Encrypted:	false
SSDEEP:	6:mMEYk+f2pomPMvmhmJ2GKFg0X+51HRdRlZK6t:Q++amAmkJW9XsHP
MD5:	620C62467E4EEE595F83451B6D5BD653
SHA1:	87EA1C59471C9282D6FBEC43DC2097C39FD5880D
SHA-256:	17ABF3A9A7DD4AE0CFDB5D1AB2C48BE59E1CA0BA5F9457B659DDB92B226318CD
SHA-512:	DA968CFF8D915524B327E77166239CF5FD8412A587F6B1A1BEF5F5B7B6D855367F95BB953C8DF6D1B4FE6D57757D6894F4E1BE8CBE0158787209EF9D7AEC84B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....>.B...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yd/r/Nk-rM4iWJZl.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....JI.....H}.Q..U3.1g\..=..6..n..x vT....?.A..Eo.....eq.,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6386862eb4b2bb21_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.675371370373962
Encrypted:	false
SSDEEP:	6:m+/VYk+f2pom70XzhmJ2UfgUlllUTs+xinuK6t:FN++am70XzkJaTr
MD5:	CED064384B6B894DABB7BCFF5B44B176
SHA1:	F1084DA1D677B8713615288E5ABB41AAD33AC501
SHA-256:	66408007CD4C4B48DA919B12A0F910C63450A6894D716C4EDF97746B4899199E
SHA-512:	190F17443A9F44CBB240CC5E28A30C5622E636684D6FEBA1BDC4D2A51B56256B2CF50FCBA6FF8A73EFC1800A704863683EAA67F1CEFF063D9966200B3CB3580
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y_/r/JopZtdti8dq.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/u...i&/.....L.....;...L.tUq9..,F....x..H.....).A..Eo.....9Q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6fb4242076012d35_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6fb4242076012d35_0	
File Type:	data
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.515114643371748
Encrypted:	false
SSDEEP:	6:m0g6EYj018IrAoUBCxMrg+Xrw2NXnrllbK6t:Rw1tzUAA0Q7/N
MD5:	8EB4A3EA8C1ECD2ABC4BC706D3F7D598
SHA1:	DB25E8A5969B26B84A8C4396DF66F80B7EFF8FE9
SHA-256:	23CC76BE0EA85F25D8B78B3B3DC3A7CDA11826EC08A3C2F85F9EA346B21E022C
SHA-512:	E290C94D83F290C5066FCB0D3B605D3A9D9C4AD7BA98B08888E75376D59B52E8CB8B26847CF7126FE1E3C366CCD25824706CBE092291E6E137542847FC587C8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....4.V...._keyhttps://abs.twimg.com/responsive-web/client-web/main.f6ffe885.js .https://twitter.com/.g..i&/.....xY.....c.k.<.Q.3R.9F.&..;.W...`P....\.A..Eo .....S?p.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\723d0aa90da2847e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.8441046587795515
Encrypted:	false
SSDEEP:	6:mTSlXYGLKciKyBZKsQAUWFVSgygtpN8KBRA7K6tMOSGfgScfzvCN8KBRA3:8Wq5rBZNQqFRXX8KWRgS+Y8K
MD5:	44EF27FE5403971EF3D6875D8562D803
SHA1:	9AB1E22503727C37AE95870C2D561323FA884CC5
SHA-256:	7A56373CE24A819A90B99D41F3896364DC75D5E307FCE81AC06A68EEC60E36EA
SHA-512:	2905A1D424188A9B78A7B6EE36B342432E022EDFC0C542767D68A547B9DFD6595CD04A1E953D1FB7B58837EA0438EF87FC68E61D8DF4528F06039847D5121CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z.....1....._keyhttps://www.census.gov/etc.clientlibs/census/clientlibs/jquery.js .https://census.gov/.1..i&/.....1.....+M...f.d...4.Y/rI5e.-aRg.....A..Eo.....4.. .....A..Eo.....1..i&/.X...1D895B4A26E2DB5F2F7767F2585499DE286A146B9A191841DBBC7F2B834FFA06..+M...f.d...4.Y/rI5e.-aRg.....A..Eo.....A..hL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\731d22992491e125_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.495224719646521
Encrypted:	false
SSDEEP:	6:mwrnYGLKcpK0IE9VjWFVS/WtgytGc891w3xzrblDK6t:VWrqqFPpGcCW3xbl1
MD5:	51E378C1631EB3BD3089FA7230E0DE95
SHA1:	8BE888D6A00256EB1CAFD56D437E2F2692B1A904
SHA-256:	DE2BC2E28C3B3DBEB69A55DAADD6C45768A10E4E878BA3A694E46E1E5B29472A
SHA-512:	3D5DBBC1E4393B8465D2D33ED7DCA2F97477B309723E738441C3FA02551D289C734C7903973842CCA4B6A8E6BE755B61C86799DD11C85FFCA54B69585F9221E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...3....._keyhttps://www.census.gov/main/responsive-header/jquery/jquery.js .https://census.gov/*...i&/.....q.....8....^.....20.\..M.;w.%.R..A..Eo.....|.c..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73e111c1fa43bacf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.433749268065672
Encrypted:	false
SSDEEP:	3:m+letK8RzYrSLbGtGgnRMKLSn0PIP2vDGLXWG+9l/lHCKntl2XlaM6dVmW8d/pK+:mPnYGLKcoRMQSnNugKXWla76vK6t
MD5:	FCB62A1D380974498D42CA5ACE0FBFC1
SHA1:	2C359C2A61C54C0CDEF4EE99B94B48972F181E48
SHA-256:	2A5DC4E2C9F5BCF8181E5EE322CE2C65CE9C630E9F7062A7D5E9C2C1FD11E622
SHA-512:	5C43FDA40A304155B5BBA324D5126947F0FEBDC6ADF518D8725DFAA6BCFC06398ED36DEDB5042B721C31027B168037599777E095AA507E6F58020FA314EF5FB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73e111c1fa43bacf_0	
Preview:	0\r..m.....N...Nq...._keyhttps://www.census.gov/populationwidget/js/counter.js .https://census.gov/.(..i&/.....i...,.A...6.._v.@...4.....A..Eo.....+.....A..Eo .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76015e3a4b6224a2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.74309703922349
Encrypted:	false
SSDEEP:	6:mjEYk+f2pomWzVeAOZTLahmJ2+rgh5E4k4+xRK6t:0U++amMOZTmkJ+5zkpxr
MD5:	3538D9C0766ED5CCE28DD383A8DE35FE
SHA1:	4C407390148B8545932552BD1141A0F47DAB3CF1
SHA-256:	431F2434C7C7FD4427FAF407DE5D48F06444EC6A642B3BF792422E51D11BE6A7
SHA-512:	D360F95B8117C727D2662CA5BE4EC16426980E8056C828EEF1B8FF371DCABFF4227231F0BA7F610B41EE307A8B4EBF8F1DDFE2C24FC778662D4B0697F2294F4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iVab4/y2/l/de_DE/RTkqPFbXKo8.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....K.....gE. 2@h[.R.g].Sqx...:7.Pl.8.;,..A..Eo.....F.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\79b184e16f34510a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.488598386950692
Encrypted:	false
SSDEEP:	6:mLXYj018IrAkRu6spML2Igp2GKgw5arkonHJhZK6t:WP1t3Ruvv12GeEkophT
MD5:	533290FA3024CD00E4A56FE2A7085C21
SHA1:	0018938BB11287DF189826B7DB0927EB55FA7F8F
SHA-256:	CA6D4A9118CCA07F77AA42C36D1D31542C8E18FD18E1F521520A330023F757AA
SHA-512:	74A6546FC6E22B617C6E388E8AFF469A7866F360B2D83AB421AC04E651CE461EEB277D9EA5249F44ED126EF5AB68DE905683FB44F84E4A1C6A4B7142B7DA4FB 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....j....._keyhttps://abs.twimg.com/responsive-web/client-web/i18n/en.1f1c4ce5.js .https://twitter.com/oh..i&/.....]X.....B.....if.U.;..1...l..\.....A..Eo.....A.. Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b2116ba6144cbda_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.428039050691238
Encrypted:	false
SSDEEP:	6:mlfYGLKcoRMQSnGnRMQ1ZGgJkjp4eg4ehkK6t:yChSnM1Sjp4eyc
MD5:	92EF116F63D31F7A411330781A246B63
SHA1:	640216754D1F067818A8AF6D8FBDEDB9F2FC1F6A
SHA-256:	6B704B87E1E050519EAD08E3AF605A1676DE65115379A8CC19758B93266C0713
SHA-512:	EBE60F283E70B3204EBA027DC9A596149A166533974F425959E09423AEFFCCD18548EF5DB4E7C1F95CDDBB9BD87D6AEDA5926B491B87672CFF1B8D3BBFA0D(A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://www.census.gov/populationwidget/js/population.min.js .https://census.gov/.6..i&/.....BF...F%..\.~.;A9....6.....v....A..Eo.....F..... .A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7cce5dc7a17256a7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1588
Entropy (8bit):	5.475873661068888
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7cce5dc7a17256a7_0	
SSDEEP:	48:n5FyitqJEkuQbZ5Fyi3otnyvN1/dgZnffro56Slv:HyhBByLEj/mtC6w
MD5:	D81F9676F239E5C07BFA53F9DE26E63A
SHA1:	ADDBD321C86708F0248BDEFB2AFE628AB911A30F
SHA-256:	1873A0FF8290F795DE53274FB2F957E9C5F842E1BC73A8A4BAD6AEAF47B6AB93
SHA-512:	300506FD7799D254AAFB513EAD2C63887132874CC611847EDAA13E60820CD0B36D0C577E8E21C2CC6E6DE77EEB23EAE2E92F7CFA1F6398830E53073957C5F99
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t.....7....._keyhttps://www.census.gov/etc.clientlibs/census/components/common/core/accordion/clientlibs.js .https://census.gov/.0..i&/.....t.....?...$.S.. JyB..Q..e%*...?/..J.A..Eo.....M.....A..Eo.....0..i&/.....'.....O.....s.....(S.0..`.....L`.....(S.p.`.....4L`.....XRc(.....Qd.?.S....addCont rols...Qd*.E....buildButton...Qc:..~....clickAll..Qd:~"}....addObservers..Qe.K.....watchChildren.....Qe.\&V....checkChildStatuse.....I`....Da.....'...(S.....Ia....J.... . .f.....@.....@. .....!.....@.-....hP.....[...https://www.census.gov/etc.clientlibs/census/components/common/core/accordion/clientlibs.js.a.....D`....D`d...D`.....@...`....&. ..&....&.(S.....Ia....X...I.....d.....@.....&..q..D&.(S...Iaf.....d.....@.....&.(S.....Ia,.....d.....@.....d.....@.....D&.(S...Ia.....d.....@..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\831107adf264f338_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.5035817930912785
Encrypted:	false
SSDEEP:	6:m/l/XYj018IrAWQ3nMrtgNyPqiNqVPm4KK6t:kln1tBQgaUH
MD5:	01877B69B42A9B1FDCF395DA87953FC1
SHA1:	CA8098BF1B6AD48128A535531C528C8DC6B5DCDA
SHA-256:	125309BB05733C1068A431740332F83D87D9661BF1C2FAB76D993DB0131B737B
SHA-512:	1C1D5C70220B7A7FBFFE0C9016B45BC9A59CB88CE219DADED0A6171F304AEDDC371255E2E4CB445EFDABFBD2BCCCD46B6211CB5AF26A7D90A5B2CA675AB EE3D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d.....M...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.SideNav.b5ea1445.js .https://twitter.com/....i&/.....Z.....4.m...G..G.c/.M...l....H..O.J .w.A..Eo.....*..z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\849c3de6865d8565_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.393637631555996
Encrypted:	false
SSDEEP:	6:mEanYiMs8pMPHgt/1j8IcNupgLrL4ktbK6t:Mr/49gIc8pG4MN
MD5:	CCE7A7DBE45E7EBE8C506DF65E7D6DEE
SHA1:	A585653CF7AE07F32460DC4A210C428305394B12
SHA-256:	9BFBE476E048B4C2FA644AC1F069852FB2AE443B72C96595AF232958EDCE1267
SHA-512:	ED0FCD5A2909EDEBD80BFEB7F50C2695DED9CC6815FFBEBB79615A158A45817AC5CA3E535C654C0A4E671743FB94C5894B1D5D8F3D3ADB3E7722E757531F9 C5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....._keyhttps://twitter.com/i/js_inst?c_name=ui_metrics .https://twitter.com/8.!.i&/.....v\.....D...L...9..g.....-...m...oN.B.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\852ffc409c1fa462_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19766
Entropy (8bit):	5.8854052312632685
Encrypted:	false
SSDEEP:	384:UWi1uS6ASTNNKhwblMMwYG+RScG96ELOR6:UWxYE2hwblM7z+kcTELOo
MD5:	01CC7EE6D5A6E234E22E42C22773EA97
SHA1:	81BF54ECF4984802A56205A45F8E4C2FBC0B418F
SHA-256:	68811122E757D4C79F1FCDCDBA99696451D61A85D5F494CFFFF363AEBEFAAB6A
SHA-512:	6670D1F4BE570E6B8F6A939F4AA281F2A112382AC9B5D378D4FB85097E23A2005BB34F8AAC700D78DA2DA776F7FB82A5695D3493162576D7061A6E0260C3429D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\852ffc409c1fa462_0	
Preview:	0\r..m.....f.....p...._keyhttps://www.census.gov/etc.clientlibs/clientlibs/granite/lodash/underscore.js .https://census.gov/.My.i&/.....4.....3.Yt.I..G.&.e..B.W4..9..1. .4Qu].A..Eo.....{.....A..Eo.....'.(o....O.....K...n./.....`.....(S.<..`2.....L`....(S....`:.....L`\.....Rcv.....Qdr.A.....idCounter.. ...Qe.%.....indicatorObject...Qd.4.....keyPrefix.....Qd../e....reNoMatch.... Qf.h.o....reUnescapedString.....Qdz.....argsClass.....Qd.&.....arrayClass....QdVCn:....boolClass... ..Qd.....dateClass.....Qdj.....funcClass.....Qd...]....numberClass...Qd.U.F....objectClass...Qd.....regexpClass...Qd.s.....stringClass...Qd..qP....objectTypes...Qe.]#....s tringEscapes.....Qb&<`9....root..Qdn>.....baseIndexOf...Qe.B.7....compareAscending..Qe.Y.7....escapeStringChar..Qc&.....slice.....Qc..<.....arrayRef..Qc._%N....oldDash .....Qc...R....reNative..Qb..]C....ceil..Qc".-.....floo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8590095ca51749a2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.633684463923391
Encrypted:	false
SSDEEP:	3:m+lPk/l08RzYkwIAd0CW/KNGKYGR8AWhEFnLxKQwJl/lHC8lllgnNK81SXD7C/MI:mZtVYkvwyGRZnNsrg8lllgYrcR/ZK6t
MD5:	A6D8E6FFA40A9FF585766856B49F3893
SHA1:	565C7636214D42182688022340FD18493D9E399A
SHA-256:	7494C3B2133CA9CE11EEA3BC4FB9125EF5857821EB27BA74C4927394B5E2D96A
SHA-512:	A1B36E62D3DFCC64BDBE8EBAE0790743113688615B0D0B42C9FE8F20672DA59939BFA48D7BF27636D9B8F214D83E98E2E6D005760420FB1A46823ABFDEF0D84 D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.....1...._keyhttps://static-exp1.licdn.com/sc/h/4zwn84zqft7j8zx33rolrjq6b .https://linkedin.com/..<.i&/.....d.....3...S.....Z.....L(.....m.&..D.A..Eo..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\862b38f3aceef2ed_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.496369372384377
Encrypted:	false
SSDEEP:	6:mhYj018IrAukGQAgOMUtgR/rbYLFig5RK6t:s1tRnQ/N/YLz
MD5:	6DD82F8A5AC9F83BCE30869432DCF78C
SHA1:	5E5289C4A6C9DBDA1513E797839E35412548AF98
SHA-256:	34C7A0DCA876CF5D1E360539D620D6DA745E48A4ACD195970E0F40F638840587
SHA-512:	E8C078958EFEAE6C68F2FE71A290A98C1DE5097DFF7296109377A74F5D668EBB5CD41661A2AFB37F7EC469472AF03615A31CEFD79468D623905ACD1728BE5DE 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.BranchSdk.cbe4c015.js .https://twitter.com/~...i&/.....j\.....r*._..\.O*f..^.../.LN.. 5E.U...A..Eo.....8~8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\89a981ce4d0a0464_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.6885213832882
Encrypted:	false
SSDEEP:	6:mSYk+f2pomdMGw1VwhmJ2M4nlHgi/U3IGH4AhK6t:L++amdnkJiniIGHH7
MD5:	6A7CF1B89FE686B93717D1CCD5FD0655
SHA1:	BD38DD736AB01C0C673E11632A20EB3EFE36F6DF
SHA-256:	A4F403469EE08D2E59046B7CC887B729864CB5795B655167150DC8ADB6D2E370
SHA-512:	130ABD129B4BD4BF1684839B694F2EFA3560EB0FA599A8CDC30423E42D42BF307B86031FF5A988E82C1C8F3A85E52A5A9B90860C2E7DCD55E74A504655935E9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yv/r/eRfcZJxUwCV.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....wJ.....C.I.GI:.....8.~....[x. ?..''...A..Eo.....o.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\89b6435f612a3aee_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\89b6435f612a3aee_0	
Size (bytes):	4485
Entropy (8bit):	5.942676870192564
Encrypted:	false
SSDEEP:	96:NiW8iQYV0hbSwpVM/4jMyrMScl+ou5XWilQPRKvY3UnA3yjKuM:NKEkbBoyIScd9Q9vY3yw
MD5:	B6762485EFAB304BBFC1E2ED06324E23
SHA1:	B27C886393FA9005066EA5976017BF58AB56DB5E
SHA-256:	67B6BEF78669AAFAFF64F428C11C00F1BAF4D00B95652649F2C0653DFB796C07
SHA-512:	65EE01238AE838F717181C7C600CB36D56117BA6ACCB493921BF59CD11902C37B74014D9C4F7736BB5CEB7E902C29D74A616E525A7FAAD9C5737E5FBBF22046A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....C.C...._keyhttps://www.census.gov/etc.clientlibs/census/clientlibs/analytics.js .https://census.gov/....i&/.....&...)...P..1.t|O.?2....A..Eo.....3E.. .....A..Eo.....'..%....O.....#.....(S....`.....L`.....L`>.....Qc6U.....curHost...Qe..|....govDomainList.....Qd..J.....fileExtList..(S.....Ia..... .....Qe.29`....isInternalLink..E.@.-....PP.1.....D...https://www.census.gov/etc.clientlibs/census/clientlibs/analytics.jsa.....D`....D`v...D`.....D...`....&...&....&.(S...Ia....D.....Qe." .6....isDownloadLink..E....d.....&.(S...IaY.....QdR.....isExitLink..E.d.....&.(S...Ia..... Qf.....bannerAlertLinkClickE.d.....&.(S...Ia.....Qd^.:.... .linkClick...E.d.....&.(S...Ia....i....(Qh>6.E....bannerAlertCloseButtonClick.E.d....$.....&.(S...Ia..... Qf6..8....navigationBLinkClickE.d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8b610968227cbc8e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	290
Entropy (8bit):	5.670014706676238
Encrypted:	false
SSDEEP:	6:mrTtVYj018IrAMUscQQc0HNy1x61GMd5WtgliCB89hRVZK6t:IT/1thUsjUHN5/iCB+T
MD5:	2DE857453B02BDB67DCBC7606BED2A02
SHA1:	5AFD5E48811B1DEEDA7031E877A1D26012710DDA
SHA-256:	E44499908B2A9A021208B7E186E621F4361BE0DF9B1E099E37A7B44ADE6CBFC4
SHA-512:	07A7EEBE165A9B98CB89D4AF7CF38184317C296DE252F71D522E1A4FCA2DD41AA41724BA775750928004217E0420782F7BF9E025BE1E25620054438AA776B715
Malicious:	false
Reputation:	low
Preview:	0\r..m.....6...._keyhttps://abs.twimg.com/responsive-web/client-web/shared~bundle.RichTextCompose~bundle.DMRichTextCompose~ondemand.RichText.89bf14c5.js .https://twitter.com/:...i&/.....[.....N.".G.b_..\....0%.[1.:Z)e.....A..Eo.....'5.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8c05ed04bad2f2cb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.590635485327
Encrypted:	false
SSDEEP:	6:mnKYj018IrAE8G1lM5htgMn/9zCveQMrNbK6t:Q21tgG11hn/9zCncN
MD5:	11C3E45C6CCDF260644A39AD1082F709
SHA1:	ACE5C61F1E0E06BBEB0488230433A821D9E7EA47
SHA-256:	FA7F6A21EB5EDA1C17DD44C158E708D06B03702B979A6127A06F312E8E5ABF45
SHA-512:	F50CCFDF3524502EA43C2AC38DB18F7544570AFCA4335769158B9D254452EE10736AE24552FB1A7A0A23B7216F9FAFEC34D3F29D5DEF6FCD0EBA1189A559D8E2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...W.q8...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.AppModules.c9a3b485.js .https://twitter.com/....i&/.....Z.....]^!..=:.{.Zl.6..^..HF~l5J ...q.b.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8d387a9a5d78e037_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.728013968877135
Encrypted:	false
SSDEEP:	6:md+oYk+f2pomWptt/ahmJ2UHygftffHsFhr5RK6t:lA++amgt/akJxfM1
MD5:	654A4AA410E47EE7F7A06449004AA5FD
SHA1:	67477CF87898FE0444A5729CA4EF246D35C97096
SHA-256:	BFC98910196BB948F0E10FE1AF1AFD0AF5165FBD44B1DDD07810A5D884BDF242
SHA-512:	FD9D5EDE3F9DD3BE4556F43BE5B53C543DAB9503CF9C6F1FAD74175D33A75F4A751C63B4A8877F37AE9BA29010DD3AECCD695D199A47B3C41A73BF1ECF959C9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8d387a9a5d78e037_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...9.&....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i0hL4/yj/l/de_DE/eymb8qr90fw.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/z...i&/.....J.....L.)A. .... (."......k.....A..Eo.....U_B.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8defe3daa4bc95df_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.597940683010661
Encrypted:	false
SSDEEP:	3:m+l77Zv8RzYrSLbGtGyrsSN2IKKoT9LRHKEBM+LK7GLXWGxOMGl/lHCltzLENtHT:maZEYGLKcLQ2IKt9PjoMygILrTzK6t
MD5:	14099A740CE6F067E5CB07263CB2BD63
SHA1:	E750F9BB4D0D2FFCFE7F43A228CE6D7786564B00
SHA-256:	872693D9DA8D005B3A620A3971791E11B1ADA7BF10412532E627DFD5F2C6492E
SHA-512:	1DE927345F81E71622BA93859F51CD80DD9D9D8E8BF975ACA145C56CD48D91EEE962CCE19DC9EFF76FF86E975966804142CF6BBA887FB94700FE027D1923DD6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....#9....._keyhttps://www.census.gov/data-tools/demo/hhp/runtime.689ba4fd6cadb82c1ac2.js .https://census.gov/.2..i&/.....b>L..l.....?.....yh..(|.A..Eo.....Q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8e5edf5491ede209_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.564027241933453
Encrypted:	false
SSDEEP:	6:mByEYkvwyEbA30VfNRrHg0TZISTS3tYbK6t:4bvwy/ENNF1NI4EM
MD5:	B2C6945F2382249C0EE87320A982BFFE
SHA1:	7FB3BF4325EAA07785CA8BCE4F4AFBC8C2C0D220
SHA-256:	6CE8700E673DD58564C214727E714B1744033E09E367D119C5EE16DA335D729A
SHA-512:	532730355795B0448A91E30616B68C371B91352BE9CC35342A773A00C3AF610BFB3D00F3AB6CE89B5AE9A68AE39AB89F2975C0ADEC91C2CC6561FD7BBDE6838
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.....2...._keyhttps://static-exp1.licdn.com/sc/h/58ikgnh04in2ngtxjdu5jjic1 .https://linkedin.com/.k=.i&/.....d.....vA...X..$t.b.^...'....'.[...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\922bd684a98ce1b4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.701135387496361
Encrypted:	false
SSDEEP:	6:mAHYk+f2pomWQr62VwhmJ2rrg2KtSLebunxs9/bK6t:h++amN6lkJCZiSLeiqFN
MD5:	A113EC73069FC4319EC49EB11F2C998B
SHA1:	827B985C99D517E6388BB8EF9E9863447128BF87
SHA-256:	EBA9897B72C10910E1D741405F56CDDC6EBE029F3326F9994887CBA2E6CF7431
SHA-512:	25917FEC1543FEA31BE45B7414B195C7426A7F38AE195404A185F0F4A473B832A9861994D2DFCC082F4715F54DB51C35444ECFC45F04CCBFEB3B4A2501B89B56
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...*....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3in-84/y4/l/de_DE/PU9jat9YP-b.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....5K..... .....jC....u'*Z...B.yty...2.).A..Eo.....\ ID.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9436ed6b703604fa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9436ed6b703604fa_0	
Entropy (8bit):	5.5828396212055615
Encrypted:	false
SSDEEP:	3:m+ls/HtgOA8RzYj0KKKXlMMIrAKTzKXF3OolMR0wJv/l/lHCvll3O04w7WmR5llB:mWEYj018IrAK+OiMuYtgtn1JK6t
MD5:	C94DF02AC62BF2C850E77FE10BA840B4
SHA1:	849E8D48B811F1210E3F9E88A5EFB67035610C2C
SHA-256:	702DF8B4D56420549ACC63E92CE69BBD75DBE8312B94B4D5E350F655C664A89F
SHA-512:	98651EB8629F93AFFC267A1AFED988DC4A728923DA17E597114450EC8161464BEED6176E37284448DDE3D9D5296C82A08C3C7C050A00BD76E01E136D23CF959
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l...>..L...._keyhttps://abs.twimg.com/responsive-web/client-web/bundle.RichTextCompose.77020085.js .https://twitter.com/....i&/.....[.....G..J..u..z.D.....&;7v$'....E..A..Eo.....:..2.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99c7340fa3da6419_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	5.37733253210399
Encrypted:	false
SSDEEP:	6:m2SEYGLKcoRMQSncRMQ6dvKnRMQ6dtZiYugl5rOYoe29hnHTzlhK6t:hSZhSni6dSN6dt4sr4e29hzzN
MD5:	2F5BA529AABD049A96ADD2992F76116D
SHA1:	D0CE140C30C3EC6D9B9197E89DABD459DC483513
SHA-256:	AFE1C52B6E55BB3CDD03000E0A5ED49D5ACA72853AFB8A5BAA1013FD8C391A3B
SHA-512:	7637FA86419C3C634742D6E043E2587573B99E2BA5656F4D27D45B22BF7D94018474362836D9C540B480F91B46FB06E6E57A2D60C349DDA5692C798C18F639A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v.....0M...._keyhttps://www.census.gov/populationwidget/population_counters/population_counters_controller.js .https://census.gov/.O..i&/.....j.Ly..u~.b.....+7.6."c....,.A..Eo.....g.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b392c532f5be8f0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.451292637932589
Encrypted:	false
SSDEEP:	6:mm9YGLKcpK0IGKWNMFgtzkN7kBe5UrhK6t:urElu+8g7
MD5:	10507A4D960D351A64B3DBF54F77E924
SHA1:	11E6F7B765DC03DBFB1A2D91E1343193D16822BE
SHA-256:	94AB85A7ED324B7F747C4B39D94A8DCB6537C697DE2BD48DFCC9B0894D965F3C
SHA-512:	DC968D0C5B572C5920C3A894EA485293958BB39AF5F01F5D90E9D404E219BB62AE51D2C7BD4BC4F5BDBC6100A05FE65BA5AA3966FB5B8255F3A660C3BF8F6E04
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...~....._keyhttps://www.census.gov/main/responsive-header/js/typeahead.js .https://census.gov/....i&/.....&.>...L.wK-..m.....\....F.qO.A..Eo.....#.=l.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9c7f758e9ab324c1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.442021198079551
Encrypted:	false
SSDEEP:	6:m3YGLKcNQKtENFPZQvtgPwJVVTQGNTfFrVnlZK6t:nEQr1mBTQGFfznlT
MD5:	E9433E1FBB2730C46E2DFAFD5746F57D
SHA1:	BDD49113C957594CF6AE152E02CDD43E9FA592EA
SHA-256:	30D60B3004ED195AFB31A060900C35CFA8A3C0BE7DE9EBED016520B5D927A806
SHA-512:	55C96087BF3C0C3F2699D55656BD8171810C966C1573580F341ECF483EDC4398F4EC046D4E55B18B8A31724E74E612F8D0849D584C0432DB67185854E513BD13
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...$.BC...._keyhttps://www.census.gov/ratingtool/js/ratingtool.min.js .https://census.gov/....i&/.....*.....=..,p..Jy...o._j'v.!.....Kb.|.A..Eo.....;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a365c7ddd6fa6bff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10874
Entropy (8bit):	5.75164233148199
Encrypted:	false
SSDEEP:	192:yUylZSjBepe3YXrwmtSspavk9I0wWceh+lx2rirGZamL6zllcVYxlxE:mp0UaM9IMf8aWlDF
MD5:	EDB037AC5EE13C668D17590FD6799D35
SHA1:	BD0B7D69259AB205C9D4F7066F51BC547FA70B85
SHA-256:	EA4338E830D0F76898954ABC705F0F0D1BAD76E0924AFA63AC18C4BDCFBCFFA7
SHA-512:	DF22C2FA9ED3973C0CFBBE4748348CF1D904EB8FCBF505988450F71872B546E077878A3DE9EFE477DC6967A227767A31D5396408CE8EE3715BFB1E80F8B00F7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z...E....._keyhttps://www.census.gov/etc.clientlibs/clientlibs/granite/utils.js .https://census.gov/.Ly.i&/.....-.....v.M..j..>\...M.+....!.....U.I.A..Eo.....l.....A ..Eo.....'.....O.....(..4.....(S....`2....TL`&....(S.h.`.....L`.....Q.@Z.....module....Qc.A.E....exports...Qcf>.....window....Q.@.^.4.. ..Granite...QcF:B2....Sling.....K`....Dt.....s.....&.(.....&.\..-....#...&....&.(.....~&.-...'..\..-.....(Rc.....I`....DaN.....e.....P..,`..,@.....@.-....PP.1.....A... https://www.census.gov/etc.clientlibs/clientlibs/granite/utils.js...a.....D`....D`....D`.....`v...&...&....&.(S.(.`.....L`.....aN..... Qf* .....SELECTOR_INFINITY.....Qd...;... ..infinity.....Qc.{&u....CHARSET...Qd^3o....._charset_.....Qcn..!....STATUS....Qc.....:status...Qe&9e.....STATUS_BROWSER....Q.@N.....browser...Qd.....OPERATION... ..Qd...+....:oper

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a4091bb1a80ffca9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.6032766048475695
Encrypted:	false
SSDEEP:	6:m7rnYGLKcLQ2IKsXi3s3ygfnAbfFUrbK6t:cr66YBA4N
MD5:	97438B330D7C98CB85EF0785F23C8AFA
SHA1:	45ED86A473FBC584DA29965E0F93E0594FC2FAB5
SHA-256:	C5EA293B62879562B37E1DA001D584C400DDCD901F524AC7FBA1138E49644B34
SHA-512:	B17786B9462F54BFBBFDFE62EF3D209B7481956F1A125C85B2A38CECA7A0D9E0B02C4802632C6089D6FEF16A178CD6ECA3EF336629420F10425ECF396785EFF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...}..N...._keyhttps://www.census.gov/data-tools/demo/hhp/main.79647588e103ae3fb146.js .https://census.gov/....i&/.....,X.l.c|/.....J[y..^*..5.*..~8.. A..Eo.....3..b.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a4f80eb73d5ec764_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.532312329018038
Encrypted:	false
SSDEEP:	6:mm26EYsyZcvXsqL7BfZWSXg6Ze1De//nn7DK6t:dPO7poQZJp
MD5:	F00A48B072F37606C06F14152AAFBE55
SHA1:	9E724A831E8B7EC6F831EC3EF358F794B491CDCA
SHA-256:	D59286D4A85CAC8A3873D734C72EADDBC5BF5A0330E73C5B7E0B177B230F4FF2
SHA-512:	56386925EF65AA2FE4B9EC6793BCF5AFB19C8D31D296250A9A9669C3B642B6437F583985E01F98636440A7DC7B9F0808CCD0929FB3667D4E1834228C2E8A6AF1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e....(.J...._keyhttps://covid.census.gov/jfe/static/dist/c/prototype.213678de24c47bc84650.js .https://census.gov/.]-.i&/.....z.....qNd.....M..O...'...d.T.WC ...A..Eo.....h.q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a66c353e1a1c147f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.440452623953804
Encrypted:	false
SSDEEP:	6:mW/XYGLKcpK0IiLElQOEXAFgIntv0xDWP4KlhK6t:T/qrwcnB0xS7
MD5:	DA8A14C9240B1EB2D40814221829B6DF
SHA1:	D7B0ECA4EADD061DCEE165BBCB5505D26B418660

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a66c353e1a1c147f_0	
SHA-256:	8551EB59690E18315A1B37242C75AA7377D6A60AFFC0419268530BCDC1C40985
SHA-512:	6A8B33560CCF264B06A4175F11E94E77857F21A67F19C1FB67B20EC25CF1632B7B8C303A5813694BB427E5D19B425B7C408E986151DE3F2F7C7931EF687228CA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...Tz./...._keyhttps://www.census.gov/main/responsive-header/bootstrap-custom/js/bootstrap.js .https://census.gov/....i&/.....<.....R.....eQ...P..a." ,..F.A..Eo.....r;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a830cf2055d86cb7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.410801808339288
Encrypted:	false
SSDEEP:	3:m+lKP//la8RzYrSLbGtGwNQWkGPWFvDGLXWGs6Hl/lHC6llSrXVGUPZuyhMmQWhR:mN9YGLKcG5ZsegzrXkzyhFhlbK6t
MD5:	F10703299A16830CFF40C57F057AEBE7
SHA1:	86323E10EB9F16BA924B5A236AE30E4D3A9A1999
SHA-256:	F2B6A7A1BBF6C305098BDE8B92434A4838E0B1593205DAE88EE6C23BF9E09E19
SHA-512:	E9EE0DB7E8C308E77A7482A12EF549A6C94825F413DA2B5AFB89FB4FFD6B29C37B68A40F8DD99FA6A1EDC7DD698A874449D4D1C71F82CA1155106FAE6DDA9 E5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...U.P...._keyhttps://www.census.gov/main/resources/js/census.min.js .https://census.gov/....i&/.....\.....3.....F.~.k....+Q.4...C.A..Eo.....q.@.....A..E o.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\abb45d97ebf09494_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.9559855562889785
Encrypted:	false
SSDEEP:	6:mbXYGLKcNQK1UQTjJ7ZCugel/x+BO40DK6t4qSPNSJhQ8Xx1NHXK+C8+BO4j:qqEQK3J7Yc/sYvuquA/h15KbYI
MD5:	3E6D3A3F8C0B82608D9F9A2A2EDF9F0C
SHA1:	A7A42201AA8F67ACD8EE940DC3B6352871C4ACD2
SHA-256:	6E2F2F6D3DD547FE00ECADA15D967EEB04041388C3A18FBEA9B0F44AD722A2CB
SHA-512:	1740312F671AA5E2FB879370AD504CC17F7A9FE7AF44960E39245491986C12331A772FC1E5041F40F889824DBFE3D69FC4C4B738B55A75CDC3333EB0FE4DCC7E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...W....._keyhttps://www.census.gov/ratingtool/js/jquery-1.4.2.min.js .https://census.gov/_...i&/.....t.....\.....d.L.....Gk.Bf....^w.A..Eo.....".....A..Eo..... ....._...i&/.....31B709B1ED83C84A44DB84B36C7E22F3EE669C154928435823DADDC33207BBA7.\.....d.L.....Gk.Bf....^w.A..Eo.....WW.5L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ad4b379ac706a647_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1764
Entropy (8bit):	5.760943341050606
Encrypted:	false
SSDEEP:	24:HtXwZtS63Zt1JJZt4bZtDIprZtbGZI5Zt7lL7:HFwZc63ZTJJZGbZuprZI+5Z37
MD5:	D3F3BC59E5B82C445ED5305693A27B17
SHA1:	19C1182C4813F1E08D415E4DABB79EBFCB0A7C61
SHA-256:	40F14F7DAA91FCC74B4E33A4916AFEFB6F221D2F9E8ED6B4B0F31F600F408E27
SHA-512:	391086E9DDD51FDB8ECFB40F8626127DB79FC73E109B9D7C04CD0010C297627307E7907FD93D4405307C6A164144A3F5391233B53AE680EC0F45CDF1C3F83A6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x....& ....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement.min.js .https://census.gov/wG..i&/..... ...*..b....O..$E.`....V..7.....A..Eo.....3-.....A..Eo.....0\r..m.....x....& ....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/ AppMeasurement.min.js .https://census.gov/..i&/.....*..b....O..$E.`....V..7.....A..Eo.....u.....A..Eo.....0\r..m.....x....& ....._keyhttps://assets.ado bedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement.min.js .https://census.gov/....i&/.....*..b....O..$E.`....V..7.....A..Eo.....3P! .....A..Eo.....0\r..m.....x....& ....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement.min.js .https://censu s.gov/..M.i&/.....}'.....*..b....O..$E.`....V..7.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\adf7722569fd0bc6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.777066285628198
Encrypted:	false
SSDEEP:	6:m49Yk+f2pomX8N7yhmJ2ClFgelluSIrNen1iK6t:rl++amX8okJPlPEi0
MD5:	CAA439D65CE3EEF894198BE93D3FE95F
SHA1:	36C76CE03D24987E444EB4D9FED2C9923B5B9EAC
SHA-256:	0E37865559D705CD56FEC51629015E0632956CC2359D1A78E1A5ABF97B7D18CC
SHA-512:	EE69FA37409D707EA8B5E66AF0EDA8851FEA1E4921D3D4961EA67E0B419C07BEC793E511920248812FD518294DA081FBA76F38D5EF310CEDCB96243ACA9E54F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....'....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y3/r/CrII4R3C1FT.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....ML.....7.6I.#....1.Y.z.....D6...#-Go...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b343428e4e214036_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.696498983610542
Encrypted:	false
SSDEEP:	6:mv8gl/VYk+f2pomWmoO+oLahmJ24JygZIw5a4d9lZK6t:48gN++amGO+FkJtlf+T
MD5:	32E8E331F590DAE44DCB1BE3C59DE9AB
SHA1:	977050933494149A2A21E891932729F317B4099C
SHA-256:	B420446625AC1C9EBE6CCED187DC09E394A15B378354ED47422AC7CAA36CB966
SHA-512:	2E4EE22699DAA5717D1823A9595877E3D712303754AD978616209450FB6019F33BA3754D7B73C73081649EA661EB61522DC4A26466492B0EE6A4A2C5384E13BD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....T....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iOTn4/yF/l/de_DE/AghE3rjighB.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....i&/.....<K.....Bt."..%R.....o...oK.....A..Eo.....D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bd70629d46f06879_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	109120
Entropy (8bit):	5.870894802537158
Encrypted:	false
SSDEEP:	1536:xTfcY2hNx2QIyLS4K51THyvCeu2fX15MpF80pRTCCkeH9RIbUnP5:JcRxLorTc5fX0FzmCkeH9Rv5
MD5:	440B199DD7F843C27F61D34235E1EA29
SHA1:	563125FD68F3AC486861E6FD04D7C831EEA3BB2B
SHA-256:	EA91004D75F60867A72BD019327E5732A2E6BC91A143E63E86215DB7A7BAB2A3
SHA-512:	4F68B06430FF091463E296F7D3FD1113FA48A0558A356BD632DBC807009E18CDC0EC68B3E6F951797E4F5D2188DC52B12257DE10B3866FAA038D35386CB868C4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...!iG.....E8502C367E960B687F4D4F5F8C0813EC97B00051BA7C78C159C8F90F42AAC3A7.....'.8.....O$.....c;.....l....'.....,.....l.....(S....`.....HL` ....(S.l.`.....L`....0Rc.....Qcb.....factory.`....I`....Da0...r.....Q.@Z.....module....Qc.A.E....exports...Qc>.,....document.(S.....5.a.....Pc.....exportsaa.....I.....@.-....PP.1.....B...https://www.census.gov/etc.clientlibs/clientlibs/granite/jquery.js..a.....D`....D`....D`.....`....&...&....&....&.(S....'..`:O.....L`d.....I.Rc.....H.....Qcf>.....window....Qd.=.....deletedIds....1...Qc&.....slice.....Qc..\.....concat....Qb.S.....push..Qc.y1.....indexOf...Qd...`....class2type.....Qc.e.....hasOn....Qc.2.5....support...Q.@.5nv....jQuery....Qc*..K....rtrim.....Qd..I.....rmsPrefix.....Qd.`.,....rdashAlpha....Qdv.xh..fcamelCase....Qd>..z...

Static File Info

No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/23/21-17:24:59.484812	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64140	8.8.8.8	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 23, 2021 17:24:03.393996000 CEST	192.168.2.3	8.8.8.8	0x6fbc	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:03.395006895 CEST	192.168.2.3	8.8.8.8	0xad0b	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:03.400038958 CEST	192.168.2.3	8.8.8.8	0x25e8	Standard query (0)	covid.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:03.993607044 CEST	192.168.2.3	8.8.8.8	0x9023	Standard query (0)	gov1.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:05.274859905 CEST	192.168.2.3	8.8.8.8	0xff91	Standard query (0)	uscensusbureaucovid.gov1.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:09.019908905 CEST	192.168.2.3	8.8.8.8	0xbc6f	Standard query (0)	www.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:10.216062069 CEST	192.168.2.3	8.8.8.8	0x2a1d	Standard query (0)	assets.adobedtm.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:10.218883038 CEST	192.168.2.3	8.8.8.8	0xc75d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:10.990438938 CEST	192.168.2.3	8.8.8.8	0xcc9b	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.428085089 CEST	192.168.2.3	8.8.8.8	0xfa6	Standard query (0)	uscensusbureau.demdex.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.456897974 CEST	192.168.2.3	8.8.8.8	0x45d8	Standard query (0)	cm.everesttech.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.484860897 CEST	192.168.2.3	8.8.8.8	0xbbb4	Standard query (0)	censusbureau.tt.omtrdc.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.504674911 CEST	192.168.2.3	8.8.8.8	0x5ed5	Standard query (0)	s.go-mpulse.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:12.821427107 CEST	192.168.2.3	8.8.8.8	0x1d56	Standard query (0)	c.go-mpulse.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:12.853024006 CEST	192.168.2.3	8.8.8.8	0xcd8f	Standard query (0)	dap.digitalgov.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:13.913285971 CEST	192.168.2.3	8.8.8.8	0x3b6d	Standard query (0)	censusbureau.d1.sc.omtrdc.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.774529934 CEST	192.168.2.3	8.8.8.8	0xb19	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:17.092976093 CEST	192.168.2.3	8.8.8.8	0xc572	Standard query (0)	www.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:32.685525894 CEST	192.168.2.3	8.8.8.8	0x35c7	Standard query (0)	kqiticdijx3nayh234wq-f-a6f6e7152-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.068295956 CEST	192.168.2.3	8.8.8.8	0xf364	Standard query (0)	6852bd0c.akstat.io	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.830317974 CEST	192.168.2.3	8.8.8.8	0x5786	Standard query (0)	kqiticdijx3nayh234yq-f-fe811546c-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 23, 2021 17:24:41.413297892 CEST	192.168.2.3	8.8.8.8	0xa840	Standard query (0)	data.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:42.608930111 CEST	192.168.2.3	8.8.8.8	0x91e4	Standard query (0)	kqiticdijx 3nayh2344q-f-5302de751-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.674211025 CEST	192.168.2.3	8.8.8.8	0xf9a6	Standard query (0)	kqiticdijx 3nayh2345q-f-ac8018cd7-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:47.992916107 CEST	192.168.2.3	8.8.8.8	0x4a49	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:48.634835958 CEST	192.168.2.3	8.8.8.8	0x492a	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:52.256483078 CEST	192.168.2.3	8.8.8.8	0x2e64	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.632687092 CEST	192.168.2.3	8.8.8.8	0x8294	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.934438944 CEST	192.168.2.3	8.8.8.8	0x9dad	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.934667110 CEST	192.168.2.3	8.8.8.8	0xdfcc	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.934772015 CEST	192.168.2.3	8.8.8.8	0x8212	Standard query (0)	api.twitter.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.976959944 CEST	192.168.2.3	8.8.8.8	0xb452	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.978993893 CEST	192.168.2.3	8.8.8.8	0xe760	Standard query (0)	video.twimg.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.529834986 CEST	192.168.2.3	8.8.8.8	0xa200	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.901981115 CEST	192.168.2.3	8.8.8.8	0x6348	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:56.655095100 CEST	192.168.2.3	8.8.8.8	0x9b5f	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.450268984 CEST	192.168.2.3	8.8.8.8	0x5429	Standard query (0)	platform.linkedin.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.526645899 CEST	192.168.2.3	8.8.8.8	0x5477	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:08.976563931 CEST	192.168.2.3	8.8.8.8	0x3790	Standard query (0)	gis.geo.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:09.214092970 CEST	192.168.2.3	8.8.8.8	0xe2be	Standard query (0)	server.arcgisonline.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:09.470818996 CEST	192.168.2.3	8.8.8.8	0x2cc	Standard query (0)	kqiticdijx 3nayh235jq-f-4b8ecdb08-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:11.204070091 CEST	192.168.2.3	8.8.8.8	0xb797	Standard query (0)	server.arcgisonline.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:03.420093060 CEST	8.8.8.8	192.168.2.3	0xad0b	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:03.427150965 CEST	8.8.8.8	192.168.2.3	0x6fbc	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:03.427150965 CEST	8.8.8.8	192.168.2.3	0x6fbc	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:03.441113949 CEST	8.8.8.8	192.168.2.3	0x25e8	No error (0)	covid.census.gov	uscensusbureaucovid.vanity6.gov1.qualtrics.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:03.441113949 CEST	8.8.8.8	192.168.2.3	0x25e8	No error (0)	uscensusbureaucovid.vanity6.gov1.qualtrics.com	akamaisecure6.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:04.033334017 CEST	8.8.8.8	192.168.2.3	0x9023	No error (0)	gov1.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:05.311801910 CEST	8.8.8.8	192.168.2.3	0xff91	No error (0)	uscensusbureaucovid.gov1.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:09.057416916 CEST	8.8.8.8	192.168.2.3	0xbc6f	No error (0)	www.census.gov	www.census.gov.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:10.250787973 CEST	8.8.8.8	192.168.2.3	0x2a1d	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:10.252674103 CEST	8.8.8.8	192.168.2.3	0xc75d	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.32.159.255	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.240.90.211	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.250.252.43	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.16.73.168	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.200.197	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.17.54.18	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.168.199	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.025325060 CEST	8.8.8.8	192.168.2.3	0xcc9b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.211.62.226	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	uscensusbureau.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.200.233.208	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.171.163.246	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.171.168.191	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.49.107.116	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.240.90.211	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.31.176.223	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.212.101.97	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.465306044 CEST	8.8.8.8	192.168.2.3	0xfa6	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.248.156.174	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.511856079 CEST	8.8.8.8	192.168.2.3	0x45d8	No error (0)	cm.everesttech.net	cm.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:11.519880056 CEST	8.8.8.8	192.168.2.3	0xbbb4	No error (0)	censusbureau.tt.omtrdc.net		52.213.168.74	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.519880056 CEST	8.8.8.8	192.168.2.3	0xbbb4	No error (0)	censusbureau.tt.omtrdc.net		34.252.166.160	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.519880056 CEST	8.8.8.8	192.168.2.3	0xbbb4	No error (0)	censusbureau.tt.omtrdc.net		52.212.193.208	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.519880056 CEST	8.8.8.8	192.168.2.3	0xbbb4	No error (0)	censusbureau.tt.omtrdc.net		52.18.150.20	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.519880056 CEST	8.8.8.8	192.168.2.3	0xbbb4	No error (0)	censusbureau.tt.omtrdc.net		34.252.156.174	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.519880056 CEST	8.8.8.8	192.168.2.3	0xbbb4	No error (0)	censusbureau.tt.omtrdc.net		18.203.205.32	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.519880056 CEST	8.8.8.8	192.168.2.3	0xbbb4	No error (0)	censusbureau.tt.omtrdc.net		54.75.9.158	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.519880056 CEST	8.8.8.8	192.168.2.3	0xbbb4	No error (0)	censusbureau.tt.omtrdc.net		52.212.164.82	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.539419889 CEST	8.8.8.8	192.168.2.3	0x5ed5	No error (0)	s.go-mpulse.net	ip46.go-mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:12.855499983 CEST	8.8.8.8	192.168.2.3	0x1d56	No error (0)	c.go-mpulse.net	wildcard46.go-mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:12.890044928 CEST	8.8.8.8	192.168.2.3	0xcd8f	No error (0)	dap.digitalgov.gov	d27f3qgc9anoq2.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:12.890044928 CEST	8.8.8.8	192.168.2.3	0xcd8f	No error (0)	d27f3qgc9anoq2.cloudfront.net		52.222.174.63	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:12.890044928 CEST	8.8.8.8	192.168.2.3	0xcd8f	No error (0)	d27f3qgc9anoq2.cloudfront.net		52.222.174.129	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:12.890044928 CEST	8.8.8.8	192.168.2.3	0xcd8f	No error (0)	d27f3qgc9anoq2.cloudfront.net		52.222.174.90	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:12.890044928 CEST	8.8.8.8	192.168.2.3	0xcd8f	No error (0)	d27f3qgc9anoq2.cloudfront.net		52.222.174.50	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:13.957933903 CEST	8.8.8.8	192.168.2.3	0x3b6d	No error (0)	censusbureau.d1.sc.omtrdc.net		15.236.176.210	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:13.957933903 CEST	8.8.8.8	192.168.2.3	0x3b6d	No error (0)	censusbureau.d1.sc.omtrdc.net		15.188.95.229	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:13.957933903 CEST	8.8.8.8	192.168.2.3	0x3b6d	No error (0)	censusbureau.d1.sc.omtrdc.net		13.36.218.177	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.201679945 CEST	8.8.8.8	192.168.2.3	0xabb9	No error (0)	www-google-analytics.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.803091049 CEST	8.8.8.8	192.168.2.3	0xb19	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:16.803091049 CEST	8.8.8.8	192.168.2.3	0xb19	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:17.120778084 CEST	8.8.8.8	192.168.2.3	0xc572	No error (0)	www.census.gov	www.census.gov.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:32.726058960 CEST	8.8.8.8	192.168.2.3	0x35c7	No error (0)	kqiticdijx3nayh234wq-f-a6f6e7152-clientnsv4-s.akamaihd.net	kqiticdijx3nayh234wq-f-a6f6e7152.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:32.726058960 CEST	8.8.8.8	192.168.2.3	0x35c7	No error (0)	kqiticdijx3nayh234wq-f-a6f6e7152.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:35.671051025 CEST	8.8.8.8	192.168.2.3	0x5c6a	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.114842892 CEST	8.8.8.8	192.168.2.3	0xf364	No error (0)	6852bd0c.akstat.io	wildcard46.akstat.io.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:36.868629932 CEST	8.8.8.8	192.168.2.3	0x5786	No error (0)	kqiticdijx3nayh234yq-f-fe811546c-clientnsv4-s.akamaihd.net	kqiticdijx3nayh234yq-f-fe811546c.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:36.868629932 CEST	8.8.8.8	192.168.2.3	0x5786	No error (0)	kqiticdijx3nayh234yq-f-fe811546c.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:41.544712067 CEST	8.8.8.8	192.168.2.3	0xa840	No error (0)	data.census.gov	www.census.gov.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:42.649672031 CEST	8.8.8.8	192.168.2.3	0x91e4	No error (0)	kqiticdijx3nayh2344q-f-5302de751-clientnsv4-s.akamaihd.net	kqiticdijx3nayh2344q-f-5302de751.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:42.649672031 CEST	8.8.8.8	192.168.2.3	0x91e4	No error (0)	kqiticdijx3nayh2344q-f-5302de751.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:45.730103016 CEST	8.8.8.8	192.168.2.3	0xf9a6	No error (0)	kqiticdijx3nayh2345q-f-ac8018cd7-clientnsv4-s.akamaihd.net	kqiticdijx3nayh2345q-f-ac8018cd7.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:45.730103016 CEST	8.8.8.8	192.168.2.3	0xf9a6	No error (0)	kqiticdijx3nayh2345q-f-ac8018cd7.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:48.030308962 CEST	8.8.8.8	192.168.2.3	0x4a49	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:48.030308962 CEST	8.8.8.8	192.168.2.3	0x4a49	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:48.659862995 CEST	8.8.8.8	192.168.2.3	0x492a	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:48.659862995 CEST	8.8.8.8	192.168.2.3	0x492a	No error (0)	scontent.xx.fbcdn.net		157.240.15.13	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:52.283847094 CEST	8.8.8.8	192.168.2.3	0x2e64	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:52.283847094 CEST	8.8.8.8	192.168.2.3	0x2e64	No error (0)	scontent.xx.fbcdn.net		157.240.15.13	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.659204960 CEST	8.8.8.8	192.168.2.3	0x8294	No error (0)	twitter.com		104.244.42.65	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.659204960 CEST	8.8.8.8	192.168.2.3	0x8294	No error (0)	twitter.com		104.244.42.129	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:53.961354017 CEST	8.8.8.8	192.168.2.3	0x8212	No error (0)	api.twitter.com	tpop-api.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:53.961354017 CEST	8.8.8.8	192.168.2.3	0x8212	No error (0)	tpop-api.twitter.com		104.244.42.194	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.961354017 CEST	8.8.8.8	192.168.2.3	0x8212	No error (0)	tpop-api.twitter.com		104.244.42.66	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.961354017 CEST	8.8.8.8	192.168.2.3	0x8212	No error (0)	tpop-api.twitter.com		104.244.42.130	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.961354017 CEST	8.8.8.8	192.168.2.3	0x8212	No error (0)	tpop-api.twitter.com		104.244.42.2	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.972249985 CEST	8.8.8.8	192.168.2.3	0x9dad	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:53.972249985 CEST	8.8.8.8	192.168.2.3	0x9dad	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.972635984 CEST	8.8.8.8	192.168.2.3	0xdfcc	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:53.972635984 CEST	8.8.8.8	192.168.2.3	0xdfcc	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:53.972635984 CEST	8.8.8.8	192.168.2.3	0xdfcc	No error (0)	cs2-wac-eu.8315.ecdns.net	cs672.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:53.972635984 CEST	8.8.8.8	192.168.2.3	0xdfcc	No error (0)	cs672.wac.edgecastcdn.net		192.229.233.50	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.001786947 CEST	8.8.8.8	192.168.2.3	0xb452	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.001786947 CEST	8.8.8.8	192.168.2.3	0xb452	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.001786947 CEST	8.8.8.8	192.168.2.3	0xb452	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.001786947 CEST	8.8.8.8	192.168.2.3	0xb452	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.014555931 CEST	8.8.8.8	192.168.2.3	0xe760	No error (0)	video.twimg.com	cs296.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:54.014555931 CEST	8.8.8.8	192.168.2.3	0xe760	No error (0)	cs296.wpc.edgecastcdn.net	cs2-wpc.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:54.014555931 CEST	8.8.8.8	192.168.2.3	0xe760	No error (0)	cs2-wpc-eu.8315.ecdns.net	cs531.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:54.014555931 CEST	8.8.8.8	192.168.2.3	0xe760	No error (0)	cs531.wpc.edgecastcdn.net		192.229.220.133	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.565892935 CEST	8.8.8.8	192.168.2.3	0xa200	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:55.565892935 CEST	8.8.8.8	192.168.2.3	0xa200	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.927032948 CEST	8.8.8.8	192.168.2.3	0x6348	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:56.690810919 CEST	8.8.8.8	192.168.2.3	0x9b5f	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:56.690810919 CEST	8.8.8.8	192.168.2.3	0x9b5f	No error (0)	cs1404.wpc.epsiloncdn.net		152.199.21.118	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.489248991 CEST	8.8.8.8	192.168.2.3	0x5429	No error (0)	platform.linkedin.com	2-01-2c3e-0055.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:58.559257984 CEST	8.8.8.8	192.168.2.3	0x5477	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:58.559257984 CEST	8.8.8.8	192.168.2.3	0x5477	No error (0)	cs1404.wpc.epsiloncdn.net		152.199.21.118	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:09.105537891 CEST	8.8.8.8	192.168.2.3	0x3790	No error (0)	gis.geo.census.gov		148.129.75.137	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:09.256220102 CEST	8.8.8.8	192.168.2.3	0xe2be	No error (0)	server.arcgisonline.com	wildcard.arcgisonline.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:09.509247065 CEST	8.8.8.8	192.168.2.3	0x2cc	No error (0)	kqiticdijx3nayh235jq-f-4b8ecdb08-clientnsv4-s.akamaihd.net	kqiticdijx3nayh235jq-f-4b8ecdb08.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:09.509247065 CEST	8.8.8.8	192.168.2.3	0x2cc	No error (0)	kqiticdijx3nayh235jq-f-4b8ecdb08.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:09.534955025 CEST	8.8.8.8	192.168.2.3	0xeb3e	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:09.534955025 CEST	8.8.8.8	192.168.2.3	0xeb3e	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:11.241661072 CEST	8.8.8.8	192.168.2.3	0xb797	No error (0)	server.arcgisonline.com	wildcard.arcgisonline.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:11.122224092 CEST	63.32.159.255	443	192.168.2.3	49741	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020	Mon Jan 03 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 23, 2021 17:24:11.559416056 CEST	18.200.233.208	443	192.168.2.3	49743	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020	Mon Jan 03 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 23, 2021 17:24:11.608624935 CEST	52.213.168.74	443	192.168.2.3	49745	CN=*.tt.omtrdc.net, O=Adobe Inc., L=SAN JOSE, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 00:59:59 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jul 23, 2021 17:24:52.620078087 CEST	157.240.15.13	443	192.168.2.3	49921	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jul 23, 2021 17:24:53.700438976 CEST	104.244.42.65	443	192.168.2.3	49926	CN=twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 23, 2021 17:24:53.700553894 CEST	104.244.42.65	443	192.168.2.3	49927	CN=twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 23, 2021 17:24:53.999193907 CEST	104.244.42.194	443	192.168.2.3	49929	CN=api.twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:54.064408064 CEST	104.244.42.133	443	192.168.2.3	49937	CN=t.co, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 23, 2021 17:24:54.902766943 CEST	104.244.42.194	443	192.168.2.3	49943	CN=api.twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 23, 2021 17:24:55.606611967 CEST	152.199.21.141	443	192.168.2.3	49949	CN=*.twimg.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 05 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Wed Nov 10 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 23, 2021 17:24:58.603816986 CEST	152.199.21.118	443	192.168.2.3	49969	CN=*.licdn.com, O=LinkedIn Corporation, L=Mountain View, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Oct 10 02:00:00 CEST 2019 Fri Mar 08 13:00:00 CET 2013	Thu Oct 14 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jul 23, 2021 17:25:02.090857983 CEST	152.199.21.141	443	192.168.2.3	49985	CN=*.twimg.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 05 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Wed Nov 10 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:25:09.439440012 CEST	148.129.75.137	443	192.168.2.3	50001	CN=gis.geo.census.gov, O=U.S. Census Bureau, L=Washington, ST=District of Columbia, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	Tue Feb 02 01:00:00 CET 2021	Mon Feb 07 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
Jul 23, 2021 17:25:09.552699089 CEST	148.129.75.137	443	192.168.2.3	50002	CN=gis.geo.census.gov, O=U.S. Census Bureau, L=Washington, ST=District of Columbia, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	Tue Feb 02 01:00:00 CET 2021	Mon Feb 07 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5496 Parent PID: 2052

General

Start time:	17:23:57
Start date:	23/07/2021
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 'https://covid.census.gov/jfe/form/SV_3en1hX9u1RWIp38?Q_DL=SqN0lR2ri39yTOI_3en1hX9u1RWIp38_CGC_daprBTqzoTB4ekC&Q_CHL=email'
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: 3504 Parent PID: 5496

General

Start time:	17:23:59
Start date:	23/07/2021
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=1564,18278074203958404562,9764153470081692 97,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 3420 Parent PID: 5496

General

Start time:	17:24:58
Start date:	23/07/2021
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=1564,18278074203958404562,9764153470081692 97,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=4612 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: 4952 Parent PID: 5496

General

Start time:	17:24:59
Start date:	23/07/2021
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=video_capture.mojom.VideoCaptureService --field-trial-handle=1564,18278074203958404562,976415347008169297,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=4644 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly