ID: 453276
Cookbook: browseurl.jbs
Time: 17:23:07
Date: 23/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report https://covid.census.gov/jfe/form/SV_3en1hX9u1RWIp38?Q_DL=SqN0lR2ri39yTOI_3en1hX9u1RWIp38_CGC_daprBTqzoTB4ekC&Q_CHL=email 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 4
Thumbnails 4
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 5
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
Contacted URLs 7
URLs from Memory and Binaries 7
Contacted IPs 7
Public 7
Private 7
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 39
No static file info 39
Network Behavior 39
Snort IDS Alerts 39
Network Port Distribution 39
TCP Packets 39
UDP Packets 39
DNS Queries 39
DNS Answers 41
HTTPS Packets 45
Code Manipulations 48
Statistics 48
Behavior 48
System Behavior 49
Analysis Process: chrome.exe PID: 6016 Parent PID: 3896 49
General 49
File Activities 49
Registry Activities 49
Analysis Process: chrome.exe PID: 5156 Parent PID: 6016 49
General 49
File Activities 49
Registry Activities 49
Disassembly 49

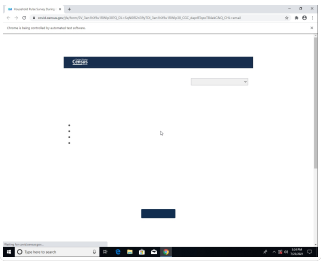
Windows Analysis Report https://covid.census.gov/jfe/f…

Overview

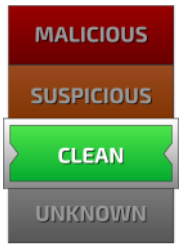
General Information

Sample URL:	http://https://covid.census.gov/jfe/form/SV_3en1hX9u1RWIp38?Q_DL=SqN0lR2ri39yTOI_3en1hX9u1RWIp38_CGC_daprBTqzoTB4ekC&Q_CHL=email
Analysis ID:	453276
Infos:	

Most interesting Screenshot:



Detection

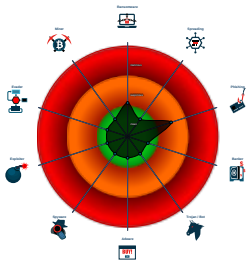


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

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: 6016 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: 5156 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1616,5429937548656341176,3177274583310322343,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /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

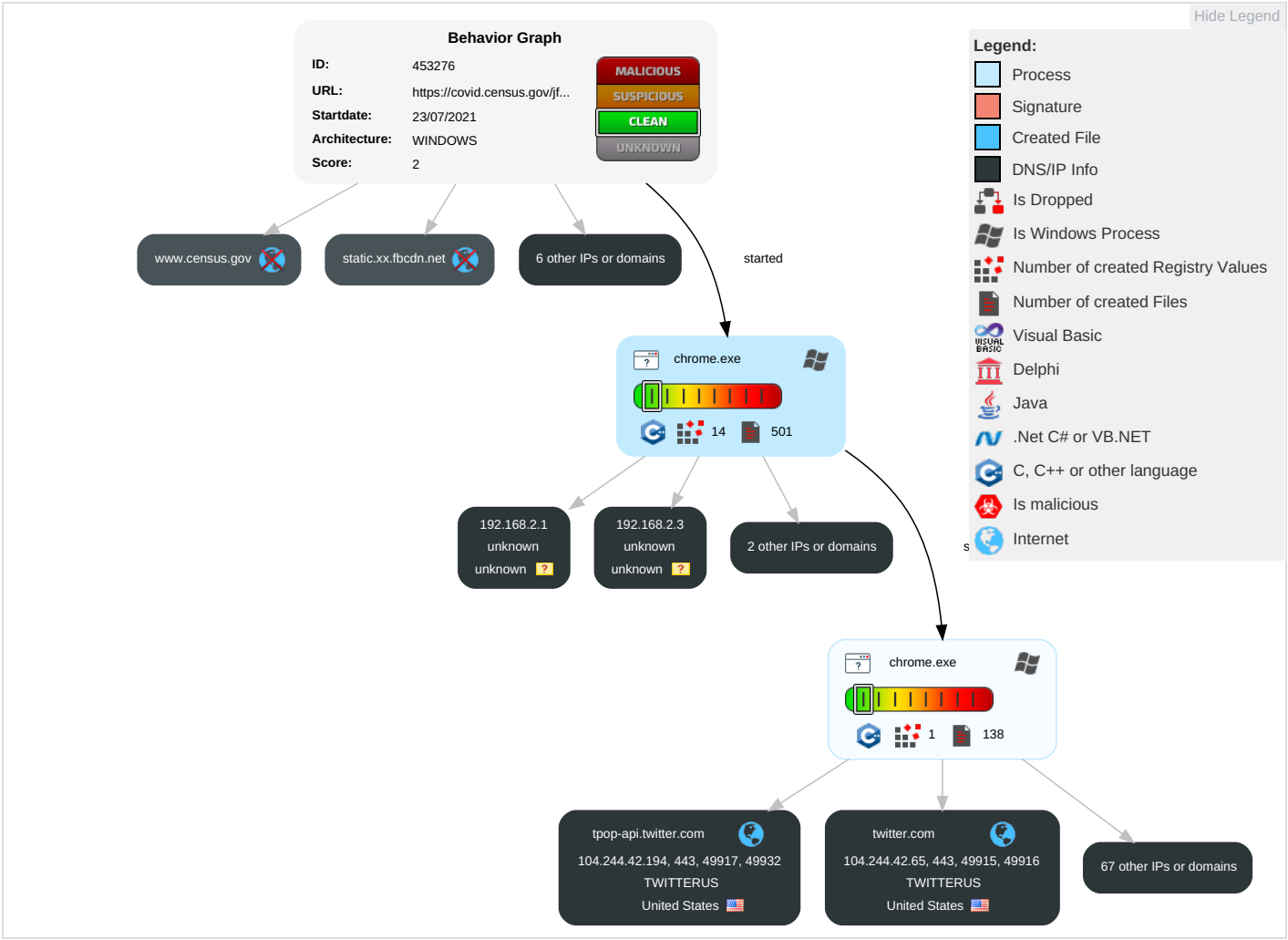
Click to jump to signature section

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

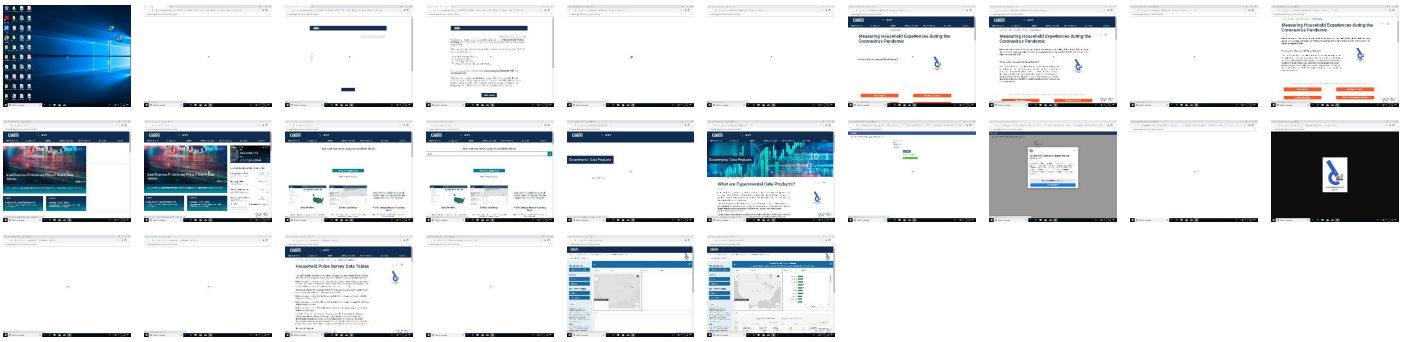
Behavior Graph

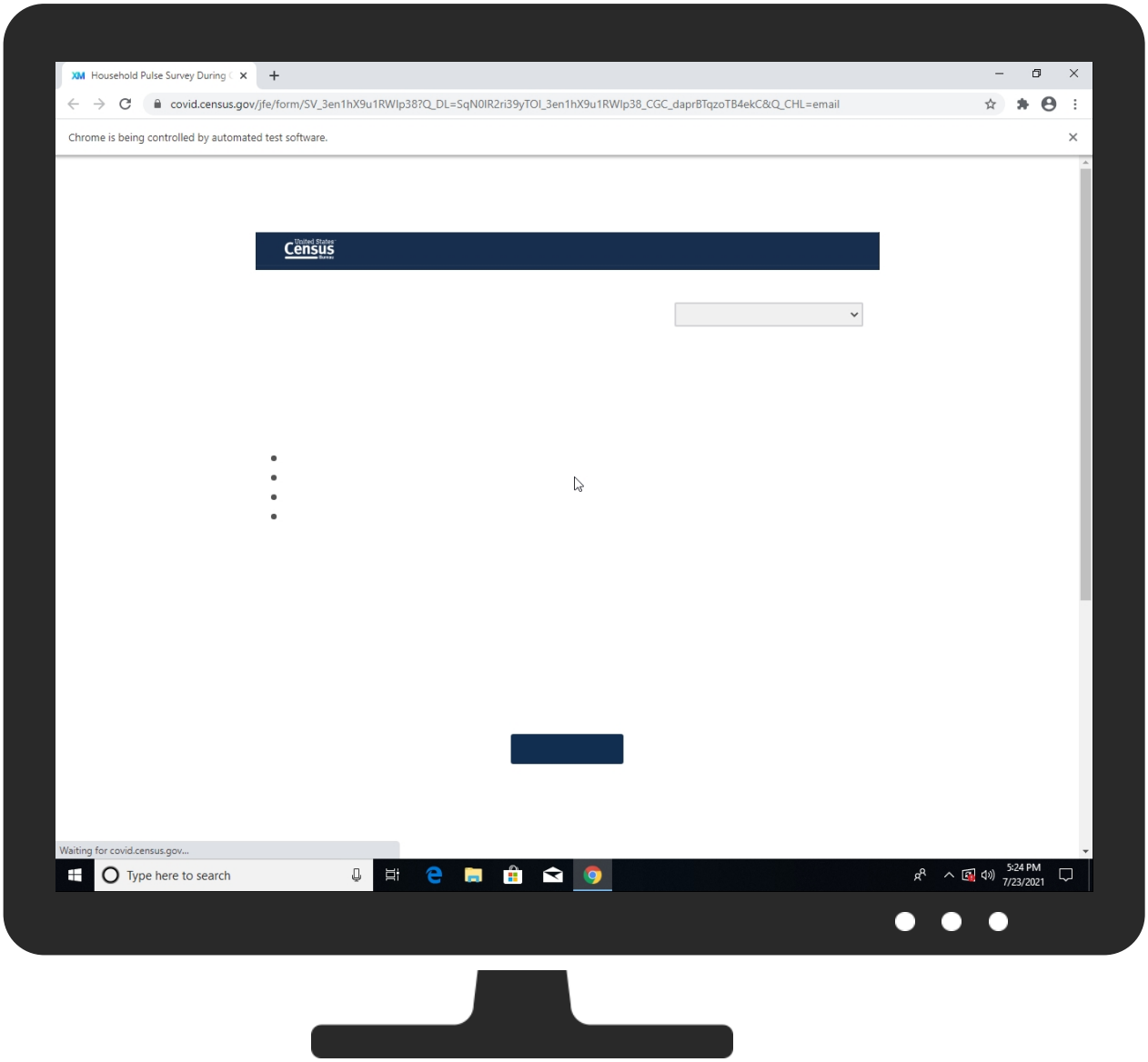


Screenshots

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	104.244.42.69	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
kqiticdijx3nayh2343q-f-afc6b30b3-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
cm.everesttech.net	unknown	unknown	false		high
api.twitter.com	unknown	unknown	false		high
www.census.gov	unknown	unknown	false		high
kqiticdijx3nayh234za-f-6bc069541-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	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
gov1.qualtrics.com	unknown	unknown	false		high
kqiticdijx3nayh2346a-f-6fe3f05b4-clientnsv4-s.akamaihd.net	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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kqiticdijx3nayh235aq-f-2cacd6b69-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
static-exp1.licdn.com	unknown	unknown	false		high
kqiticdijx3nayh2347a-f-0071a8c97-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
static.xx.fbcdn.net	unknown	unknown	false		high
685d5b1b.akstat.io	unknown	unknown	false		unknown
c.go-mpulse.net	unknown	unknown	false		unknown
server.arcgisonline.com	unknown	unknown	false		high
kqiticdijx3nayh235kq-f-34ab7faf7-clientnsv4-s.akamaihd.net	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
52.18.85.49	unknown	United States		16509	AMAZON-02US	false
104.244.42.65	twitter.com	United States		13414	TWITTERUS	false
104.244.42.69	t.co	United States		13414	TWITTERUS	false
192.229.220.133	cs531.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	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

Private

IP
192.168.2.1
192.168.2.7
192.168.2.3
192.168.2.6
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	453276
Start date:	23.07.2021
Start time:	17:23:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 20s
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.win@45/558@43/28
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
17:25:12	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:	24:7ShGlGv46u7sBHRS6Vb3IhU+pjJguEAVGX95rs56d5CdUinUfkuhgy042X:7kJvOsTSu7IjJghAVm0ueUMuhgyj2X
MD5:	B64852C81713421B7E47E4302F97658A
SHA1:	6938FD4D98BAB03FAADB97B34396831E3780AEA1
SHA-256:	25768713D3B459F9382D2A594F85F34709FD2A8930731542A4146FFB246BEC69
SHA-512:	6A6F6DA5D47D88757F16853723198D5AD55F4A041E1EAA5200AF7F1054800CD4A9EA734AF8763DF1209A8CE2273DC0DBBFC766731DB5117BFC66D44DB2B7009
Malicious:	false
Reputation:	low
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...200924000000Z..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):	3.105738285350884
Encrypted:	false
SSDEEP:	3:kkFklF5l9ttfllXlE/NtoGr/vhDvcalXl+RAIdA31y+NW0y1CSkNm/flgGNl5lqr:kK2UtBcalgRAOAUSW0tXNQ3OiW/n
MD5:	CD6DE4769968AC49F46F18DAAA5A0FE2
SHA1:	178A851A68DFFB38B96B8A2056C7C0A872EF67C1
SHA-256:	867E5F59AD8CB1FE9A29F87976EFD69367530B5A26F0F2E8CFCBB3FB31D0D249
SHA-512:	6FFB3BE1B1BAE0BE84D3E42CA437BB826EA7373375E4DF8855B092828FC9E0D9B8857F14CA5DF291D5F83A863922568E8C8AF0D73EBDCC6509DE07D3D6F9C8FF
Malicious:	false
Reputation:	low
Preview:	p..... ....x...O..]"...(..... .....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\0dbb6b15-404e-4c12-9128-5ba5f2847904.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
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.....*...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\3ea76a94-dfaa-433a-bec2-392ab86f2f46.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):	365626
Entropy (8bit):	6.015109837339848
Encrypted:	false
SSDEEP:	6144:llBLBtL/F1CfVO8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB9:M9bbCfpxzurRDn9nfNxF4ijZVtilB9
MD5:	DD459AFA3545A981AF51384F0F0FA794
SHA1:	1A939558A185E78B3FF1C41859D517EAD2D61914
SHA-256:	D5A134A37D3BC5B784932853DE3D5603B64511A3D8984E39C66980578C52467F
SHA-512:	2765E73828FB182D85586C285C4D055BA2993A7890F5657DC7EE566F9FD1116F7DBCB59FD6F4FCC49FCE844591E6C737DF200CAB75DF2D0E4A05CD14D077804
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":1.627086243324637e+12,"network":1.627053844e+12,"ticks":4690089703.0,"uncertainty":4734552.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075242231"},"policy":{"last_statistics_update":"1327155984019

C:\Users\user\AppData\Local\Google\Chrome\User Data\4350bea3-565c-4259-8b49-4a5fef96ea82.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):	369209
Entropy (8bit):	6.027576409689962

C:\Users\user\AppData\Local\Google\Chrome\User Data\4350bea3-565c-4259-8b49-4a5fef96ea82.tmp	
Encrypted:	false
SSDEEP:	6144:9lBLBtL/F1CfVO8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB9:/9bbCfpxzurRDn9nfNxF4ijZVtilB9
MD5:	D9AF9EFB57AAA6A29B908CF47843E00D
SHA1:	32207808644D88636D93F8FCBC34DF0EF362B05F
SHA-256:	6E2A4599C947D38ED215B57516352BEAEA5C98B73191038AF69D1FBD175ABC8D
SHA-512:	302C8F7B0C31C11ADB09A7482CCD42C769EDBFE53203C92F847C4884BDFB96AFDE6186A5B3935E79D3B1E32591F99C3EEB0FA8E6965BB0956B1D4FA47D1AA2 1A
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":1.627086243324637e+12,"network":1.627053844e+12,"ticks":4690089703.0,"uncertainty":4734552.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075242231"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d3e2bb5-691d-412b-9ad5-ee35005b6905.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:	7A0D092DE65A1A73326DBBF2A7D22C25D1A8F04671BFBB7E41560BAE647C573BB038ADD4A341B4B3C989989CE4BBA7EC60F375752953E441B3FC9B7DC3B474 55
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\83ac264c-d16a-4eb9-8b3f-534e2e638e04.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):	365625
Entropy (8bit):	6.015109298025072
Encrypted:	false
SSDEEP:	6144:slBLBtL/F1CfVO8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB9:o9bbCfpxzurRDn9nfNxF4ijZVtilB9
MD5:	7BACA7F9D64636AD3FD72D26F0FE8561
SHA1:	3FFD006F66E9940C08E5D5460637329F1A0ED781
SHA-256:	75F481A83EA35E0804D40C726DBF22E0982837C76DE30EDFAE6C7B3768BD9932
SHA-512:	6B43CAE300AB08DC033A624234CE02882FB1103B08FA4D8EAA66BAE7322A98E24285800B28EC7F06A9FC52660AB00D9069C547860BE5971EF6F99F4691B91D7F
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":1.627086243324637e+12,"network":1.627053844e+12,"ticks":4690089703.0,"uncertainty":4734552.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327155984019

C:\Users\user\AppData\Local\Google\Chrome\User Data\892ffb72-b002-4e04-93dd-2e79706eb599.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):	365625
Entropy (8bit):	6.015109737263568
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\892ffb72-b002-4e04-93dd-2e79706eb599.tmp

SSDEEP:	6144:4lBLBtL/F1CfVO8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB9:89bbCfpxzurRDn9nfNxF4ijZVtilB9
MD5:	95715C746B77B48C58D4FCDC4A7068F0
SHA1:	54F8A4765BAA8E92917DC5F01B617D17F09C2569
SHA-256:	C077D396BC3DC858EFD98FD4FD32312634126E6B00571B5C830ABEC56CC0194A
SHA-512:	E47B8F57C46076341F72A3FD01D97A622FB8A23799B390F65B0A8801FE73A7DEA11AC42E27F4CE0BB1471E2C8E43FC33A6B084F296C863BCD2E66F1CAF15606
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":1.627086243324637e+12,"network":1.627053844e+12,"ticks":4690089703.0,"uncertainty":4734552.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1Qfj oKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP0 5zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327155984019

C:\Users\user\AppData\Local\Google\Chrome\User Data\93a6dba2-3f85-4b87-8c01-aaa8cf244dfc.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):	365626
Entropy (8bit):	6.01511020380053
Encrypted:	false
SSDEEP:	6144:plBLBtL/F1CfVO8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dB9:j9bbCfpxzurRDn9nfNxF4ijZVtilB9
MD5:	8225037E0A4932286F11DE4430E8158B
SHA1:	7D00B3C53B5D3641944873EFECDA20D8F9B5B518
SHA-256:	70B2E60D2A9EA6E050E5C6045D4378A3C7B0C2F40D47B909658F711515B04E8B
SHA-512:	288C0E3C9EA8F61C571A77CE4BD8766A9245888AFF25A513F3548E6F2D01F5BE456A74A5F60AA8D79CF56A957DFB2C7BDC31A5042BB92C9B8F6D0A3837EABAB
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":1.627086243324637e+12,"network":1.627053844e+12,"ticks":4690089703.0,"uncertainty":4734552.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1Qfj oKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP0 5zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075242231"},"policy":{"last_statistics_update":"1327155984019

C:\Users\user\AppData\Local\Google\Chrome\User Data\9656cc3a-acc4-4bca-9016-52ea732a22ae.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\Crashpad\settings.dat

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\101259dd-be28-40fe-96d0-0d88f1ac9174.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):	5.536359470082404
Encrypted:	false
SSDEEP:	384:MHitaLl9dXY1kXqKf/pUZNCgVLH2HfDNrUAHGdnTPqZ2B4F:0LlDY1kXqKf/pUZNCgVLH2HfRrUEGdny
MD5:	9F7CC9F9610209F7E04E5DD63E12C027
SHA1:	869A5B02F2A76FB4F9BA92F9D2D3BC3A62379F1F
SHA-256:	20A4AB617F42B7513BA3C054096FCD49F8F75B95305EDC907116F79259E385E1
SHA-512:	76B63A3AEC2AD00ECEFF50BE37383A3A32E71D9198ABABD6B155333940350C3AAAF92C8DB9127F664967E59B3FB32860DBC6228B8B6496083ED11E76BA85D3F E
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13271559840273626","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\20d61d38-d595-429b-bd62-22ca6f5df183.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):	2882
Entropy (8bit):	5.59301297421428
Encrypted:	false
SSDEEP:	48:YxFU8/LUd3e6UUhVEUsHUcKUAjUA4/yUTlUwKUp5lUOBsmUigU5UeCPwUIc2USUc:eUOLUdzUUEUsHUcKUQUAKyUTlUwKUNUK
MD5:	462D2F8070A67F1BF6D5178B6912C911
SHA1:	B25EA386242C6A8225010AEA02DE342BFB9B4E8F
SHA-256:	8247049008808DCB81B3902E7F13345CD91F326B007AC581250D4422BA1A36C3
SHA-512:	EAB7051EF6BE08F903ACFE14B4B56A2B0DE80289C107EA8C54D74967F6C261D144B3743AF794FBFC7EEA07B4E49105B831EA86EC1E4D73EB110F6DBA6ABFF1 89
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658622304.104662,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains" :false,"sts_observed":1627086304.104668},{"expiry":1658622298.312735,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_i nclude_subdomains":false,"sts_observed":1627086298.312738},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"f orce-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1642638296.908974,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h 4YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086296.908979},{"expiry":1658622246.07142,"host":"TbNXujyuKYzExGI5EVjLC j66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086246.071427},{"expiry":1658622256.886206,"host":"UXkw KK50RSIe0pxRNE8AV4z71mmitHDrvDfp8QzFpcE=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3d4ff4b9-b78d-4dd5-938f-fc538003410f.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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3d4ff4b9-b78d-4dd5-938f-fc538003410f.tmp	
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41572a7d-1a31-4e43-9060-268c0c6bca26.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2882
Entropy (8bit):	5.598176802052628
Encrypted:	false
SSDEEP:	48:YpFU4/LUd3e6UUhVEUsHUcKUAjUA4/yUTlU3KUqw5lUOBsmUigU5UeCPwUITj2U2:OUCLUdzUUEUsHUcKUQUAKyUTlU3KUtUX
MD5:	8D8CEF79A82DA4D49FEB7A7B164CA279
SHA1:	454157D8361DFE7272C050307B88935F29BD16B2
SHA-256:	DB7342C61D9AA91E37BF7F6D64A20954C5E005F2AF85B6E9315436C3E1B3CB27
SHA-512:	30F051D407AC89805262522F3023BB81677FB5CE81A94F609D53EA173802E8FCBC97F8034FA429B429CEF7939E95C29702A582CDA1676D33C7AB1CC5FB47C634
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658622311.939435,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086311.939442},{"expiry":1658622298.312735,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086298.312738},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1642638296.908974,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086296.908979},{"expiry":1658622246.07142,"host":"TbNXujyuKYzExGI5EVjLCj66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086246.071427},{"expiry":1658622256.886206,"host":"UXkwKK50RSIe0pxRNE8AV4z71mmitHDrvDfp8QzFpcE=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4b051a75-d61c-45f3-9078-0cb740e3b833.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):	1875
Entropy (8bit):	5.595813300067595
Encrypted:	false
SSDEEP:	48:YT6UUhXHUcKUAjUAVlUDDKUe/U5UeCPwUIOg2U6ZUeh:JUURHUcKUQUAVlUDDKUiU5UH4Ul/2U65
MD5:	4316AC7A6FA96DC648D1631611A48EC4
SHA1:	A4AC02A6268A278466C764E446C756586B13CA8F
SHA-256:	E50DAA475CEB51B7991DF168FA512256C8049B15D7DBA71ED5B42306DCB459FE
SHA-512:	59C797AD646B2F22C53AAFCE97031D48F0D4EA2CA8096F513FC2CC32B0195E8A70B7B9BF4372E5BEEE5D5921BB35A0C0147D003FA9482068A9D571D9F6B9FC0
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1658622246.07142,"host":"TbNXujyuKYzExGI5EVjLCj66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086246.071427},{"expiry":1658622256.886206,"host":"UXkwKK50RSIe0pxRNE8AV4z71mmitHDrvDfp8QzFpcE=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086256.886211},{"expiry":1658622256.991779,"host":"YHSMTQnYC85xpfxQXKcYuC0wBIhWAWiCTB+UjCnXwn0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086256.991785},{"expiry":1637972658.213778,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086258.213783},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5341d7c2-30a4-47a4-b3de-829605f0e7db.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):	5699
Entropy (8bit):	5.189080898913924
Encrypted:	false
SSDEEP:	96:nOIrQ/S6MBYwSKIk/Ik0JCKL8mkM11tbOTQVuwn:nVr96MBYwSSC4KpkMl
MD5:	C9ED6CE34E83231C873EBCBA00D6C3D4
SHA1:	C3972A4985D9BC28094FF5D255D478B87A066E50
SHA-256:	EA2CAA7F31823B1BF6551E505108A84D1C778E31DA4B1A68A829A97935B934FD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5341d7c2-30a4-47a4-b3de-829605f0e7db.tmp

SHA-512:	957D40C8489E631DCDACF0EDD083F3F5E36DB9FA209244C7BA9D238D2DFEDA29312B860231B2DD734C8E5AE89ABE3F2B355ED78E915E72F7C0B3DFE8706F22D
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271559840548065","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\59d8b836-9dcb-4396-9999-6070df0cf062.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):	5103
Entropy (8bit):	4.970636612353649
Encrypted:	false
SSDEEP:	96:nOIrQzS6MpSKIk/Ik0JCKL8mkM11tbOTQVuwn:nVrf6MpSSC4KpkMl
MD5:	DBE8A3E4150BF6C45C6E142D70CDC3B8
SHA1:	5F557760DD030D1B0CAF0EB52C6390AE649E58EB
SHA-256:	8D4B4627C0C815F847BDF60C6A454E46A289F40D3E34034D79C9F978CAA918AC
SHA-512:	B525C19E0431343E27376F608ACB40624940080673BF663405C18017A2FDA30E890FCCB1EE008D7D2FCFB8EDE6ADF193F65284F8D1A95C01C9B46D9D5DE1E4E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271559840548065","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\705b1fed-0893-4b2c-8726-ec40f6e45845.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):	1875
Entropy (8bit):	5.591611145668123
Encrypted:	false
SSDEEP:	48:YT6UUhXHUcKUAjUAVlUwKUGU5UeCPwUIJ2UAUeh:JUURHUcKUQUAVlUwKUGU5UH4UIJ2UAUc
MD5:	E1382C8CFA6095DF07825B47AE3D3132
SHA1:	E61EE63AAF2284AE73B7D93E838B75B8D7B613AF
SHA-256:	F85E7AD704BDACCF8BD8C1A71B93DE6CA0C6E12629D1C9C10D68FEF17040906B
SHA-512:	2F4084DEF552AF3A6C5E1270652BC8EEC411F4C93764C1E7392EB24EA87E154718483B1435D4A8B0FF41B6616CAE272124A7DAACB86BEF5F8D4CF5A16DC2BABA
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1658622246.07142,"host":"TbNXujyuKYzExGI5EVjLCj66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086246.071427},{"expiry":1658622256.886206,"host":"UXkwKK50RSIe0pxRNE8AV4z71mmitHDrvDfp8QzFpcE=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086256.886211},{"expiry":1658622256.991779,"host":"YHSMTQnYC85xpfxQXKcYuC0wBIhWAWiCTB+UjCnXwn0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086256.991785},{"expiry":1637972658.213778,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086258.213783},{"expiry":1658622280.463775,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7d4f198b-f10c-4d4b-bf48-b4c6412c19e9.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):	5797
Entropy (8bit):	5.191500047873279
Encrypted:	false
SSDEEP:	96:nOIrnqsS6MBYwSKIkFIk0JCKL8mkM11YbOTQVuwn:nVrC6MBYwSOC4KpkM6
MD5:	E86CBD5CCC7126AE2BA2AFF891742F22
SHA1:	09C506C7D9116904939CB07706D46AA253A958D3
SHA-256:	6A92755BF4529EC6912233E0320B61BD1299674F6B1D6824DB782A5630ECFD0F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7d4f198b-f10c-4d4b-bf48-b4c6412c19e9.tmp	
SHA-512:	4F0BF6E9429093C994F6D4ECF9C4FBB7AF9EC959068FBC54CAD1E345E44CE7C21B0B2A9B3D41D4D648082E6EE5FAAE3F0DD1EDFBA256C28DE4A0651531474D2E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271559840548065","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\899b02f3-da42-4ab0-9df9-24dc3be1a1b7.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):	5699
Entropy (8bit):	5.189187770664659
Encrypted:	false
SSDEEP:	96:nOIrQ/S6MBYwSKIkdIk0JCKL8mkM11tbOTQVuwn:nVr96MBYwSIC4KpkMl
MD5:	2DC496B33DB7F169DF03530568ABA5F4
SHA1:	B9E8358B25D0CEB151BAD2A31BA0029843B0C641
SHA-256:	65B5E942DCBEEAE71B5C5FFFE4D21895B5706A44C9DC7C3B31473C50CCF0F899
SHA-512:	F2EE33C3118D376A56477A18BAD935310B35B4B2019D93855E85E7EF41C1461E89619297B7EB0C8EC54D4D72155B379A395D4665D3AE230F2CFB7BE6D84A64C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271559840548065","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9916a1b4-4984-44d3-aafe-3175ff36effa.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):	1541
Entropy (8bit):	5.597508515541971
Encrypted:	false
SSDEEP:	48:YT6UUhXHULjUPDKUe/U5UeCPwUIuX2UiUeh:JUURHUXUPDKUiU5UH4UIuX2UiUc
MD5:	EDC1387838832B11FAF58451E0D5D8D2
SHA1:	4286D3CDFAEFA40444680B1A60CEFB0CF88A689E
SHA-256:	C7B4D493F3A2F36A73DE8CFAAB02AC6B23B2751BDB071EAC35326CB7A8C9E886
SHA-512:	7FA625C54D7EE617FB6044A59F8D86BD767D3AC27FCDEF9F53317D3C6DD3F0A43192DAB52DC977D4549BDB2DA534522D927CF743087E0376D61FE8C6FF22E9B
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1658622246.07142,"host":"TbNXujyuKYzExGI5EVjLCj66Y/dVNhzv0bnrKtgcQLg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086246.071427},{"expiry":1658622253.848204,"host":"YHSMTQnYC85xpfxQXKcYuC0wBIhWAWiCTB+UjCnXwn0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086253.848209},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1658622247.079207,"host":"wPBGK7SV+UX5bqJcu0I1WRTpTkGu+94cCkvBBYprdTY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086247.079212},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obs

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):	336
Entropy (8bit):	5.196391897366136
Encrypted:	false
SSDEEP:	6:mf7q2P923iKKdK9RXXTZIFUtpO3ZmwPOjfkwO923iKKdK9RXX5LJ:Gv45Kk7XT2FUtpS/Pg5L5Kk7XVJ
MD5:	CB2151CAC22EF1AB21A5E024EEC03605
SHA1:	5D128B879E15D7A9A81E89EBE079B2389C93DDFB
SHA-256:	815AEABE79BF6A8569EAD61CADD4D27DD34FAC59652E889A1B564BD3FC69BE1D
SHA-512:	F9A35BD2647E4842F76EB9EC5CF79B74C61ED2F5BA4F04C65700F457DF41A43FD6691170E54960EF4D886A6212BC17A48DA726BB067973FE1A33E30C63A74A0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/07/23-17:24:18.477 1b24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/23-17:24:18.481 1b24 Recovering log #3.2021/07/23-17:24:18.483 1b24 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):	320
Entropy (8bit):	5.218152074559418
Encrypted:	false
SSDEEP:	6:mfzcq2P923iKKdKyDZIFUtpOvuhXZmwPOvuhFkwO923iKKdKyJLJ:9v45Kk02FUtpsqX/PsqF5L5KkWJ
MD5:	CAC757B842B99A1B827863B1F46A94EB
SHA1:	3D7FE06D2FBBF32914E4D6F7D1E390453E6E3F85
SHA-256:	ED6BFE27D8BB60930F03A533CED59878C58D1FE0323A357AA2BBB43B5915EB4E
SHA-512:	A696280011899E3ACF63E7B1FAB06561DF980DC0CB86ACBF2E89D6E14F857BBA2B3F1658350FA04C05D200BE001CD639EAB3D83FF27C50E6D89249A4D22029D
Malicious:	false
Reputation:	low
Preview:	2021/07/23-17:24:18.458 1b24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/23-17:24:18.460 1b24 Recovering log #3.2021/07/23-17:24:18.460 1b24 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\02cd5775951acf29_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	128400
Entropy (8bit):	5.998816619528192
Encrypted:	false
SSDEEP:	3072:QsvIGyq01syIYLVsvHz777RFjMiGaZhtJ:QsLWqy5svHRFQi95
MD5:	16BBD516AE33B9E36266CD21FFB1C254
SHA1:	5B67AAFCA524E6DDD6B2FC13EF6AD2F386C9E063
SHA-256:	C6F5D67E4863005B66CAD2716115C894E0EF937122D2EE875293F244E75BBF1D
SHA-512:	54E8A57986877F6F65E5227575C5BA2928D6BA829251104F4EF628B19EBDB66AE6493EC2106F90AABD6CD6FBABABE7C3ACE9C3743B445957C6199FD7C430873C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....".....8C80D505F576C437AF196E6FD23A916780D4459B110F02746CEDA7D9A2B2987B.....'..(....O,.....g.....D.....(S.....`Z.....L`T.....L`.....(S....`d....`L`.....Q.@.Lfn....window....Qc..F....parent....Qc.....document..Qe.Q7....getElementById....Q.P.1d.....boomr-if-as...Q.@.#.....BOOMR.....Qe...!....boomerang_frame...Qc...D....domain....Rc.....O.`..... Qf.....isCrossOriginError....Qc..<.....addError.,Qi.4. ...BOOMR_check_doc_domain.domainFix..Qcf.....indexOf.....Rc.....`..... Rc.....Qb.u.....c..`.....a...Rc.....`.....Qc".0.....replace...Qd.....^[\w\-]+\...I.$Qg:..3....BOOMR_check_doc_domain..`Z....HKp....X.....-...>.....N...Y.....o.....D...0.....%.....&.(...&....h.....&.(...&...&

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):	5.336873127382754
Encrypted:	false
SSDEEP:	3:m+lyTggOA8RzYrSLbGtGE36J/ViLXWGlQx/l/lHCpktKvjCTQG6SJp9PeXmC7t/B:myVYGLKcNJ90lagKo+Qem2YK6t
MD5:	AC4643378C050AD6EBBC37CAAA936720
SHA1:	D1B946B6227D2BDC1AFBCCCAE521195A943BF071
SHA-256:	38438FD3C2058208732D8FDFC289CC1EB9A213B2130A8336A58E1BA42D81CBE4
SHA-512:	F43333AC7B8F31049D1E2D0D4AFB2AB07E34E78810B0DDEC3F4C34BEE639B338E214D0C5B1BA3B34FFA096C51C7B58AFAFDF680470B44CF0511A942687BD1F65
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...Rb....._keyhttps://www.census.gov/akam/11/2260023c .https://census.gov/.g..i&/...../t.)1...4g6u.s.6.s.!...E..zu.A..Eo.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a69c121d2aba1b8_0	
File Type:	data
Category:	dropped
Size (bytes):	22949
Entropy (8bit):	5.718003234456753
Encrypted:	false
SSDEEP:	384:7HwSnQm9ev1tEWmXTZ46vTHbrk9hatwV8DufZ8WrCIOGA0:8IQvMWa5HkXQ5SfZ86xD
MD5:	28A01E22C6F5AF2717FF9ACE078D946A
SHA1:	71336B2705E120F469FD36135E9E1C193375D705
SHA-256:	89FF44C26288A3C7A104B3831DB16F86B01C488D6EC05F74AFB0D99A43C40E07
SHA-512:	420A174D58E346D17122668CF1738FE53638448A24EDECBA9CC15AD9219AC7564F5189CFCE8D5931D31980F4C15BCA26F63A8D18C1EA710EE998AFFE2D51FF7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]..........._keyhttps://www.census.gov/etc.clientlibs/census/clientlibs/bootstrap.js .https://census.gov/....i&/.....jBX.B...o....(V.k.@[...a.A..Eo.....=.S. .....A..Eo.....'.....O.....X....J.....$.....(S.....`.....HL` .....Q.@F..5....jQuery.....4Qk..;E&...Bootstrap's JavaScript requires jQuery... (S...`.....$L`.....Qb.v.....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.....QeZ..

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):	5.508843527226
Encrypted:	false
SSDEEP:	6:mSlPYsyZcDA3RdZSU8DugQGdf69QZ5P4ZK6t:NlsdSD58q/k
MD5:	E2855C395AFA69E97A3975AC97011232
SHA1:	9F0056B2938A79C589064E2A6FE441DC68FB3CBD
SHA-256:	5F4743368B548F2FCB5E78773B1AD1FFA86942BECB35ACD88F7FE0E11D8BA95D
SHA-512:	364105255A93A5CDF00DEDBC8FDE4F01A775B6452AF9D08982255DEDDE580FE3AB56C11CAF9F3A4BC13744CF222F45430A8A6327415BC462B8DF583EDCBFDE D7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...S\0....._keyhttps://covid.census.gov/jfe/static/dist/jfe.f5270bb8374885d2b2ea.js .https://census.gov/.S2.i&/.....OC..wzg}.....0B=.].....BD...A..Eo.....| .....A..Eo.....

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):	5.742046529244764
Encrypted:	false
SSDEEP:	6:mqYk+f2pomBMiQfzhmJ2ctgZRBVTeh6hK6t:z++amBbAkJHyRDTeQ
MD5:	2F3A20989CCBFF1275EE6F660E0D7868
SHA1:	29B859671130AAE4C1CF1F489C6AB7B1D7BA25D9
SHA-256:	B52CAC9E5B66AB896B53C60C34FB6C96DC1787B4266399F2987151EC76655649
SHA-512:	16B5DBE776096A5BDFB2FC143BD9EDAB51A09A47FFEB0272F053B36CE56D4CAC37B53B6B161B9BEB9A5DD93717AC5BD408AF04F33E6155A281DAC6648B39C ACD
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&/.....s.....T..Db.rqY'.....;..|.x. g.....A..Eo.....M.;.....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):	5.566981516717878
Encrypted:	false
SSDEEP:	6:mI7REYsyZc7HbF42FgGEtUiDSC0N6A1bK6t:TpuFotUxBN64
MD5:	9B2446BE207F0C35566AEE4C35D76E4A
SHA1:	EA752D437ED845B3F43E6A8AB4257CAB211A6D0C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f016c508efa5487_0	
SHA-256:	5F38352A6B403BDD31594C3C08195527A832CDC084D80A006BFBFA28ACC7E1CC
SHA-512:	5A86AD4B8FE1773784C8198770158466E25F9849DCB88603A39369B123A22242253AA318A20B730EF60C0E8A317CB6501E0FFE2CF912B70D6E0AD4BFB4B83736
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.....q.. .....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):	5.413837504477699
Encrypted:	false
SSDEEP:	24:xQ5FyfvUNbrZZwL4Lqn+h5Fyftyk0ovTKT/9LOv:xQ5FyU7ZwL4Lf5Fy15KT/s
MD5:	4A407809B9CBF61238B658C042917625
SHA1:	7FCCF2BB4AB8688B2669486FB2FD245442F9D406
SHA-256:	1D9F488F9482363CB901A356F3E2C98094EBB39FCF48713451CAAB87846D74E0
SHA-512:	9A613EDEBB9E3954542BD0532F614ECA4E98A0B59C99A83B8D2E2A34A147ABE3B9308C0313B299AD5AA902D4BF9D63AF1EFE12DD3758056317D10EC0E3A38D6A
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&/..... .....&....s.t..}.b,..$...._.w.0^..d.A..Eo.....I.....A..Eo.....i&/. .....'.....O.....Hi0.....$.....(S.L..`R.....L`.....Qc.Lfn....window....Qb:.... ..on....Qb.3.+....load.(S.....Ia.....d.....IE.@.-....xP.....j...https://www.census.gov/etc.clientlibs/census/components/common/body/embeddableimage/clientlib/component.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.....}],.....

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):	5.366896954503138
Encrypted:	false
SSDEEP:	6:m7QYGLKcoRMQSnmPZWgP3ZPaFrehZK6t:M9hSnmPFaBe
MD5:	55C5673D0506D387E319497F23A77FA9
SHA1:	DACD00F12B1D3C3E8C1BCDC005FA79B68D03B870
SHA-256:	48371FC0B06F4A70EC3CECD1052B26D66A63F6ABB8FC0F2F3040C3609DDE1364
SHA-512:	AF97C49EF4C4164E86E41569929A8E3100D49EB15090C394FED42F1E4239F92FC5C4626FE9CC099E8A6EDC154FDCD27A253F7164BF9C39BAB9B8E40E7356088
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...c....._keyhttps://www.census.gov/populationwidget/js/main.min.js .https://census.gov/..T.i&/.....>.....k..PXt.....@oo..I..D.pk*..\..A..Eo....._.....A..Eo.. .....

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):	5.73096561241236
Encrypted:	false
SSDEEP:	6:m5Yk+f2pomW0cChmJ2+wFgV9CPNELK4lDK6t:c++amPcCkJTjSqL3
MD5:	250BC223B68E8F50D944AFB3E9FF7906
SHA1:	EA746DDD1772E93188A3EF801238208AB363F191
SHA-256:	C2E96064FC581565E612DBF0607048DB36F1415A1A340259C804B4095B3F3916
SHA-512:	BFF841904C271827E7EDB80DFB1EDCE91828B05C4D895922B25940470C1909B81B0BE51CBFB8DFB509E93BDBCBEAB4F404873262E2415C28DA93AA6C1F4D76D5
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&/.....{u.....jTc.F.%e.a. .0.g#...'..5.B...<.A..Eo.....''..d.....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):	5.426922247286569
Encrypted:	false
SSDEEP:	6:mwh0lXYGL+MIwJJwMntgPHSJilxhm4DsbK6t:dGIwvJaUDesN
MD5:	F5187CFCD0399633B1D60D29CB2402A5
SHA1:	E9ADE7ED307C5C3392E72F20FE00A7FB5664C74D
SHA-256:	A119D73F10A101580E7C8B3B77844978AFDD2059C1D7AA16E27BB5E62F739715
SHA-512:	1EEA665E32A755BB6B43159C35BAED0D701EDCCBFAF399D972C4C255B28BAC6DE16F3ED1CF166DE5136FC8460C5B3B932243A2A45C7FC9AC4E419FCA5C105 038
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.....I....._keyhttps://www.google-analytics.com/analytics.js .https://twitter.com/:.d.i&/.....:.&..L...jC...1UR@u<$mz.B...u..A..Eo.....`V.h.....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):	5.748443880958012
Encrypted:	false
SSDEEP:	6:mjtgEYk+f2pomJ2iGyhmJ24ghtgd8JwfrHrGnK6t:eD++amJ2ivkJShi8GzHi
MD5:	E8F74FCE12CC20CC7909D37CDF2741AA
SHA1:	3EB2BB44BFB0F0DC855E201A4D5CBDAB3890117B
SHA-256:	B7C34042D2248F4BE4F984D006767D40824A4DBBDB996F1CAF29146A34F290E6
SHA-512:	8FBDC8D44FA7DA95F917BE285F8848BAA38E737A8EA53731654834F03EBB10FD87371B4577800593A8650656ABD79F3D6CBC43D49CD17EE7C66EDB47F273C28
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/..2.i&/.....w.....#...._.l.....)....~.. .._..b.A..Eo.....(.....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):	5.683215503402027
Encrypted:	false
SSDEEP:	6:mhl/lXYk+f2pomdMCWXewhmJ2ADtgsQ1nAtVN7DK6t:IXz++amdzwkJ7bQ6VH
MD5:	0B94C2026EB8A66F24B83F2FFB5D7D2D
SHA1:	70187583328CE3B9B2A1AC77DAE05FB3DA3FEA06
SHA-256:	24596C2506EB88AB0DC5595B3F075F325EE9AC0804E2A6835BEB6F29AC5A6664
SHA-512:	D1A1237F9F681D688E004E85EA90C02DE5254F77CC06B72070AB9B10B10DA046A447720E8C889E4B19E3E50444CF6DC20DC23F6656E74A1CF7E7C638A568122
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/C...i&/.....t.....i...c..<.%...7.....T....#.!..- .A..Eo.....p(.....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):	5.599453972364855
Encrypted:	false
SSDEEP:	6:mY6EYcv0KgJXZE2gVgAzMwARs1dWkvySryKFgNA9JkrBzK6t:UfKt6if0suKeR
MD5:	4E55594B795D5EAA4CE1F595D02EFBD8
SHA1:	BC39A2191FFA60C11E7525CC36850621AA2DFDE6
SHA-256:	7E3F3DBC741F10ED3B45AB37B138249DE42ECE7BD4D5A34394F556AEB30DEAAE
SHA-512:	E73B32C8F70FE3879182626E0959FA6F3A51E81542A1F2CF19F0F2A70425B849EB5BFAC64A99BB66E0A46D0EB41C94ACD4D348724D15B816DCD444A3A753E24

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1e5d871230df8081_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://assets.adobedtm.com/526d5084b7f8f688ea81a3aba09755d76a81f8e8/s-code-contents-6eafcaf24c53a8340cb08ca3a89da5a57f80a8cb.js .https://census.gov/|p..i&/.....(W.....^(r..|{^G:.U..+e..U...L...]M..A..Eo.....L.....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):	5.612152368091996
Encrypted:	false
SSDEEP:	3:m+lYDLA8RzYkwLf3G9Lom0y+S3V2QufRJ2FPIHl/lHCX1G9cuqHd7G4mcZt/pK5M:mLYk+f2pom0LmhmJ21IFgOcus7qUK6t
MD5:	C36F66A63CA3C5C7FC795D9DEC0B02F8
SHA1:	EAFBF1CF024435B40E4672CEBD0D500ABF28A2D9
SHA-256:	E528BCBDE0E159DD4F639268315E59D4AFA74A086007706BD88CE02586B367BF
SHA-512:	558DA30FCD048E013DA2C3395AEEBA4A8F03449324DFF1E08A3F5A6A53B41FDB80CAAEBF5A4BDF53953DBB01AD68603A705114E397F6E78CC240456641E17CCB
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&/.....su.....Q....hn.pm...B...y..r.mZ..:v-.A..Eo.....\^.....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):	5.457030354606429
Encrypted:	false
SSDEEP:	3:m+lz/5OA8RzYRhmHT8NWQA7sxdFvDGLXWGNeh/l/lHCLltbOjT11+MXClF6g4myP:ma2YSHT8NWQAgmIrgevj+oCGAybK6t
MD5:	84A2C18F996D0EB42D4B8E6FA64F8ACA
SHA1:	4C5C42D797736490A9F9AFECFEEDFE9A4FC9F81E
SHA-256:	CC64A6B76B78BC114185A0F8A7154C3515D6FECD8FF63A912B0F861B25A95348
SHA-512:	F86E4BA40DF262FDA3531704E6940B7AA30EC5214EBA466E99C76B5B552AB3DBDAAD5F104C281D8FD34811D1AAA3AF730A172C9C2D985010C9D26FF6C347641
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/(.I.i&/.....h<.....'.wq..v..I.Jec...Y.7..*..".jCc.A..Eo.....1.....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):	5.5677966308281155
Encrypted:	false
SSDEEP:	6:mYUYj018IrAzyvLdXMeughSNvSH9hR/kK6t:Fg1t/LdG9SZ/2
MD5:	99433884863485ED94850877EDE38D53
SHA1:	B9B842607BF4E5EA5A3839D67E0BF285BCD2777B
SHA-256:	79A59C64A4C4FEEB5F857E4483FC2BDF550DA9672B5E07815D1246E7472F1641
SHA-512:	65898DD25B0E77D8B18FEEED6E78E458CA6CFE4335044AC06A0F20B9D7DEFA78CD20F41BC4E06A3063170F6E0D095FF5DA0D3FEFD4C71022017FB3EA8E90C6A
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...b&....._keyhttps://abs.twimg.com/responsive-web/client-web/polyfills.8133b945.js .https://twitter.com/..P.i&/.....1.....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):	1626

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2fe0a2000559c66a_0	
Entropy (8bit):	5.809196590547289
Encrypted:	false
SSDEEP:	48:f5hm8MyF5qMBF5vMCrF5bMrF5iyM0F5zMc:f5UA5b5J55o5ig5
MD5:	60D38C7FA6628955722BEBE70CC28330
SHA1:	6AA51555BCC62CC4F58A895C50DC08C42FB971F4
SHA-256:	6A42981755FC78ACC6C9DBE4B40589537D1F5FA0CDCA5A84CCAF46B7C73A8D10
SHA-512:	8543BD374487BB63C5AF9ADD13FCC340C676626577F556E3A867F9577BDEF632128B0922EFED7BBEAE1307C2EEF3558322E5CC7BA7766FD775B0CEB03AEB93 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....'....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement_Module_ActivityMap.min.js .https://census.g ov/3...i&/.....f..=.$.4.....D<Cv ?.X.$KF..A..Eo.....Y<.....A..Eo.....0\r..m.....'....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e54 0399dcc1f8208860b7b/AppMeasurement_Module_ActivityMap.min.js .https://census.gov/....i&/.....).....f..=.$.4.....D<Cv ?.X.$KF..A..Eo.....q<.....A..Eo..... .....0\r..m.....'....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement_Module_ActivityMap.min.js .https://ce nsus.gov/....i&/.....R.....f..=.$.4.....D<Cv ?.X.$KF..A..Eo.....w.....A..Eo.....0\r..m.....'....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7c a14e540399dcc1f8208860b7b/AppMeasurement_Module_ActivityMap.min.js .https://census.gov/T...i&/.....&c..

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
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	6.270507315249057
Encrypted:	false
SSDEEP:	96:MP06oWHVmujzhAJVvUQs9n1nOJRC1eEa31q7TnEoyf+IFiA6Io:MP06BHkuJpQQ9OJWeEX/yfViYo
MD5:	1C27B964292E994C05B6B5EE94660F15
SHA1:	A1989F64B629D99612C45C9DE9DCD821D9190458
SHA-256:	9E7FF76AD734B2A02B723929B4A63BC6133D56ADDA6C1A8BB88EE0B01B047174
SHA-512:	86CC20C02EB30B8F5314027B4777C18980A23A46A0314B3EB1CA2EDBDFA0ADCB9CE3DE0673346DB37CFCCF06BF4970C30AAAD5A8BAE0E9E1EB0471EA891F3 F2C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K...J....._keyhttps://www.census.gov/ratingtool/js/ratingtool.js .https://census.gov/....i&/.....|.....0v.qj.4.v.....X....sW....?_....A..Eo.....A..Eo..... .....'..?....O....0.....(S.0..`.....L`.....(S....`.....i.L`.....RcD.....Q.@F..5....jQuery....Qdn.(.....CODE_BASE.....Qb..L....PAGE..Qd.t.....P AGE_TITLE....Qc.....rating....Qb.....os....Q.@".G.....browser...Qc...G....device... Qf.Q.....digitalDataPageName...Qc.e.....textArea..Qd..r.....delaydisplay. Qf.....script LoadHandler.....Qb&.....mainl.....l`....DaB...4....(S....la.....!.....@.-....@P.....2...https://www.census.gov/ratingtool/js/ratingtool.js..a.. .....D`....D`T...D`.....`T...&...&....&.(S.....5.a.....Qd.....script_tag.....a..... QfV.-.....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):	5.702804474461545
Encrypted:	false
SSDEEP:	6:mdYk+f2pomTyhmJ2N5yg+lll9ztBmr4TbK6t:I++amTykJH/jno4TN
MD5:	CD6B0BE91868564F59BD7AD7FC31E35D
SHA1:	6F22A89E58152C5E0D15AF3D11C08AB87D2971A1
SHA-256:	2931938E4CFF6299802BECFA9618F366A3706686F6310385E63ABF33963BC9DF
SHA-512:	F93F1E69516331AD4F54D41101562A8044D67EF28BC418835D49FA7A2FAAB4EB047B28F21FAB15693121DFD7F7BF19B5256BD6F4AF8C1C44753944AAF66347FB
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&/.....v.....K...{..B..:&MM..FV..O%... r.....A..Eo.....0.b.....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):	5.524926228099556
Encrypted:	false
SSDEEP:	24:x05Fy1HIye7oThJubmggzwrgW6/qi+h5Fy1HQ/TF4eV6HZfXlmo7:x05Fyl+oTLubmNUV6/qb5Fyl2wH1XAO
MD5:	729CD41A4EB3C3F2D28AAB390C1BA48E
SHA1:	5964482F8302FF90718C68CE41AE41A32ABD9F22
SHA-256:	FC08A4FAD9F29B8F3645CAD30BE6678377D7735666A004973920C052BD9777BD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\37f4aff035cea44a_0	
SHA-512:	6B89FD929CFFEFE4536915628DEA231ADE848ACEC343B632B1B0A5F391BFFE2741E1C87C02B01836838DDB62BC73A840A8A61EE92DDD0030DD40FD1FF28F290
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&/..... ...7.....?d@..w&.."9!.".geY.....A..Eo.....A..Eo.....i&/.(.....'.<%....O.....z.....(S.T..`b....$L`.....L`.....Qe.....CensusAccordion.. (S.L.`T.....L`.....HRc .....Q.P..d.....digitalData...Qb....._.....Qd.>H#....accordions..c$.....$.....I`....Da>...2J...(S.....Qe.@b.....initAccordion...at....$...d..rC..... .....)....).8....8.;....<.A....B.I....$.....d.....d.....d.....d.....e..... .... .).....a...Q..@.-....xP.....j...https://www.census.gov/etc.clientlibs/census/components/common/body/expandablelist/clientlibs/component.js..a.....D`....D`l...D`.....P...`$...&...&..!.&..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):	5.464460677694362
Encrypted:	false
SSDEEP:	3:m+lOGtlA8RzYEiyZtGXB6KPSVDYRCsDGLXWGHtDK/l/lHCqTCzYmAY3EYt6RmO2D:mKXYEbZcXB6FVI00gVzYm9wA35RK6t
MD5:	EC3FDBD76D5ED9209F7EA5FF67420870
SHA1:	D58C510B73FA727EEFA4E6B1D58604BB376B2556
SHA-256:	BCA12B26CA612E2262323231503CE76AFFAA4A6F8FF23982932D6FF93CE43995
SHA-512:	6251977B831F74F4C771E60ADBB508D9F657EC914AC1120B8A4BFDD88C16DFABA92AD3FA51A1442347253721887D070CD955CE01AC4F6620B865DD18D1E0FC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J...v;)O...._keyhttps://data.census.gov/cedsci/js/app.3dfc6147.js .https://census.gov/"*..i&/.....X.....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):	5.908714056318656
Encrypted:	false
SSDEEP:	192:LCjJj8N9UkhcAS6P9n4CsQSqmaFXQhEHNgJPq9w+IxqbhQMk:LwsSuI7Dk
MD5:	5A1608348E5EFFFEE50D5EF5A0B0ED33
SHA1:	A85D29D2A61B9F1AB7AA2D38A77628F5AEDC6270
SHA-256:	A62D478C30AEE4EF5014BA6C92279DB2DD9184352BB164F27D887EC865F728E3
SHA-512:	787380AE2574A3BEBD9845F250CA44138FF4790D576D9FADAF82C4DF1C65145B2BEBDFED1C5D374E7555A2DA492AADA06B237E5F44044EB213080FE7D7667F 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X....'.2...._keyhttps://www.census.gov/etc.clientlibs/census-core/clientlibs.js .https://census.gov/...i&/.....P.....c..A....0|.M....q.q<.An\5.A..Eo.....d.R..... ...A..Eo.....'..K....O.....%.....G.....t.....(S.!...`.....lL`2....(S..`.....|L`:....xRc8.....Qe...K....dataLayerEnabled..Qd..1w....dataLayer..... Qb..u.....NS....Qb..#.....IS....Qc.K.....keyCodes..Qd..S,....selectors.....Qd../.....properties....Qc.Ke.....Carousel..Qc6.~.....readData..Qe.....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-core

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):	5.6250274814369865
Encrypted:	false
SSDEEP:	6:m1FXYk+f2pomWSxzhmJ2gFgUlx6bo5Mt/bK6t:qFz++amWUzkJ8x6bo2/N
MD5:	A08CEAC2E4D7D93C861B31629DA28CFF
SHA1:	1F4C6D2F2CB38F64D15A966918E9197E29941407
SHA-256:	2C024C644F9EA7DABEB6370B3C274B735FE81C4D6B17CFA1E39696066A09CB5D
SHA-512:	29910A6D1CC9385FBAC39E414E0A8B225D0719180EEE2166F4B29A86F64DB092124ACF9F5752B79D2B304570E2DCEBAD9E26B070CEF0D5F6EF48BBE10FB3ED 66
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41aaa36d588890d1_0	
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&/.....v..... .[..u-T.v2..w.p..K !.Y[..6..A..Eo.....yG.....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):	5.558936734667496
Encrypted:	false
SSDEEP:	3:m+l5bzA8RzYj0KKKXlMMIrATXfXSdsIDlMRIGMD+1/l/lHCJTEnahWkrzFRm6ttB:mUb9Yj018IrAitpMrhtg6+rzuYK6t
MD5:	8EDFEC768654A60938EEB56B889A474D
SHA1:	1C4F0F833BB82EB71E6CAF02B2658D19C26D5D7D
SHA-256:	14A2364870016145E8956BB3A498FC27AC3F3A143E861322AEF54BA57AE2C6BD
SHA-512:	DE36820D4F0C7434E685DEB7F5E8FBA9948AF00ADAEFAD3D7FE383CE06F90B245EFF2AD958238F94FD0CDC2FA8DAF2C0BC99B154764AB932302B524571225D D9
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/'!d.i&/.....~.....o...[.V....G..?6CP.. 7..SQ#.....A..Eo.....m..F.....A..Eo.....

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):	5.561794882776586
Encrypted:	false
SSDEEP:	48:b5FZ8ppDkr3VNqnW5FZud1d4EDZAC+r6OYGWaR588WZDgeBLq8LtfLwYy0ds:b0DYz+2UTDX+rhY1VxLqcLe
MD5:	B12A498B286EF839589D09410F116B1E
SHA1:	B853F769D4E7FA43CE8DD46FBBB9D51EA88FCDC3
SHA-256:	3DA5FE69C468E60A5FAE0AA5B9542C99731E60085879039CE7A8BB6F7FB5F9DA
SHA-512:	1754975F0CE936DD2773CCA3EB6400288F0860B19C679F11486BF87F878EB780EC93C9700E6562967CF0AC2635859D9DCA4403D174650D28179A9360669701CD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....A....._keyhttps://www.census.gov/etc.clientlibs/census/clientlibs/universalheader.js .https://census.gov/...i&/.....8..9I.....-g.]9\.s.<68.6S.EZ^r...A..Eo.. .....#.....A..Eo.....i&/.P.....'..U....O.....f.....(S.P..`X.....L`.....L`.....$Qg.].....CensusSearchTypeahead....$Qg~).e....CensusUniv ersalHeader....(S.`.`|....0L`.....HRc .....QcJ.....apiUri....Qd.1.....resultUrl.....Qd~j.....isUSASearch.. QfF}.c....onSearchFocusBlur...c.....l`....DaR....t...(S..... Qf.Sd9....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):	5.433254299555044
Encrypted:	false
SSDEEP:	24:VI5FyyIALa8jEgKuqoh5Fyy8xo5A2x7qVzZu4KwXVajTeQz9Sa8jEF:q5FyyHL1EgKuR5Fyy8xMhqVz5KwXASmP
MD5:	D6DC9F9634F0FB3A444FB37A06C232CF
SHA1:	4E1741FE7F4BA8CC3B65C3EAB72219D779BCF79C
SHA-256:	F3524F02A2D28A5E7A4DC4E47F1D0DA12C418F45A2F23085019CB1C38B1816A0
SHA-512:	E2942A702DFAF93D80AD63DCEC73F711FFC19C66F92C3B10467677D9F60FA58AB13C41CFD4AE50289115CFED06259B6B441EA88C710F6B9848C78A9E39A75FA 0
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&/..... .....f ....RGR..?.X.eh.&.../'..._x.A..Eo.....x.\ .....A..Eo.....a...i&/. .....'.....O.....n.....(S.T..``.....L`.....8L`.....(S.....Ia....z....$Qg22B. ....languageSelectionClick..E.@.-....xP.....l...https://www.census.gov/etc.clientlibs/census/components/common/body/languageselector/clientlibs/component.jsa.....D`. ...D`h...D`.....0...`....&...&..A.&.(S...Ia.....$Qg6*.....handleToggleLangDropdownE....d....!.....&.(S.....Ia8.....d.....$Qg.....toggleLanguageDropDow n..E.d.....D&.(S...Ia+...9.....Qd6.....onKeyParent.E.d.....&.(S...IaN...R.....Qd.0.....onKeyChild..E.d.....&.(S...Iaq...r.... QfZ.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\464a508e9dbc3c5e_0	
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.6874677812734244
Encrypted:	false
SSDEEP:	6:mcVYk+f2pomtzhmJ2VgS3ZxeeA+4unK6t:J++amtkJGM+B
MD5:	4900A5F22F5D17E195A9617771EFC1EC
SHA1:	F223AFEF444AE60B2AEDED1CEA8C3DAA07D14E64
SHA-256:	22773DAEE9342C58860FB53BEAB9E60B20A2E5B1C980197B8E5F59319D6236A8
SHA-512:	76BE5CE6314AFE184A8819163D1B36F0F27F4ED4C0970E0B33130CAAE99C3226C15A20A83743FC151C0C50025021A5587D3C2861D4EE4817068EB547E24EBC73
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&/.....v.....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):	5.591278269960818
Encrypted:	false
SSDEEP:	6:mAS9Ykvwy1O8lzNNNZKtgr/l/Jy0MD9hJdRK6t:zevwynlzNNN7tBy1D971
MD5:	B4D4366CF4134FD770B8CB448F47B0B6
SHA1:	900ED72A852E2A7D28B1D82EBA7F0D9EC007C15B
SHA-256:	79B723E4CC62AAF03D4CE00CBC64BFF23E6796C98DE818EB0B728DE0D10FDDCA
SHA-512:	868E14A5846DE621AE833EADEA5586CA7610F00DBC22E5CC15FB2F34DE77F36B8C467445B849746DBF9FD2B8ECE1E036DD0BCC49C8D3FFCFF59DD4D0A182F CE3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....=....._keyhttps://static-exp1.licdn.com/sc/h/9x1ka0d4advijnuxgxnyns6ne .https://linkedin.com/7.{.i&/.....3.....B...?.H.l.LY.\..i..E.WT.`wA....D.A..Eo.... ...C.Z.....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):	5.501037214204946
Encrypted:	false
SSDEEP:	6:mAYj018IrAmHPxMyDugvvmaQ0xx/98/bK6t:t1tJmaFS1
MD5:	9DAF5D0A25C432DED099770B251C185A
SHA1:	DA6846718AAC159D815BD363758B4E96B1351CD8
SHA-256:	DCE200CEDE4C08E3C04B4FA73295C97FBB10822C1686D0F2B2BD1CEDF066E066
SHA-512:	76D47B02013A3D2F8D8D3A6FF9B8AE50F7AF2915BFA7F6B4B009A602BA43B7326949E0173C2DDF192CEEF89AAAF974D252760BA3BC3FA9C48A97974A6F9F84E 1
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/(.P.i&/.....k.....zQ.....A.a..1ek._.....n..! ...A..Eo.....Dsz.....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):	5.765484937828731
Encrypted:	false
SSDEEP:	6:m10XYk+f2pomW8AOwMNzhmJ25tgz/PhAr4/ZK6t:j++amcO/NkJe2BT
MD5:	923DB483EAF29139982084E7F2532CD8
SHA1:	3099C52915ABAE3C1A2CA7F5D84D4E5598A10A04
SHA-256:	16C6246C8A06410D8FC3278AEA51D08F5C5E570BC0E9629D681162BE9F95CC4E
SHA-512:	740F524C474389DE509AEE02CBEAAF27AB45B0673CA9F93793569A57E4D25A8FFA13878F4A60E09BE652F7823214368F42ED02D12B1C5A134A5EFB26FE7A8D02
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5047ffbd2b109760_0	
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/..2.i&/.....w.....O. ...4<.G.G#...u.....'.bR.9..A..Eo.....k9.....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):	5.660165906725078
Encrypted:	false
SSDEEP:	6:mEiVllyEYVb2FIBFM4B6VugbEQgquhyAFnK6t:TiPIpnB24G5gquhyU
MD5:	9BCC9036FC994CF5144860ABE9D08077
SHA1:	4BE6DABF033D7AA51D504F6CFF8D33B843763E3B
SHA-256:	B095DCFB4308A3FD34D16CA0DFEA53AD5D7E12902B26189C6A30E5ECE65D6467
SHA-512:	6D2DA9E54F1B38AB12D726C23109A4C9400C218F022368EA3F30DABA44315C262C0A095ED1D0EE59526DCEADA3D8FD47510FA4880C3CC539CDC1752F06C2B 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X....._keyhttps://s.go-mpulse.net/boomerang/N5F9F-5SXNV-TJA4F-B6CEM-65LXH .https://census.gov/2..i&/.....vW.....ne4:...c..e8...}t..X....a.+.... A.A..Eo.....d.Zq.....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):	6.4272480555883975
Encrypted:	false
SSDEEP:	384:74CO0FYYkjqzFregmcPBBlxBquTIeHIB6HMb:7CB2zNegmoBBlxBqijIUHMb
MD5:	C3883ADAE6F4E034966DFF21DFE47C99
SHA1:	2B81DAE25A46FB7ED91DFD2B479587F504DDE472
SHA-256:	EF76C62879D62BC3D65D46BC3D17E99971ED0A5D6CA9DDC9A60B95AF8D46512F
SHA-512:	D635DC4F753E82AE3767CBB7423F03C90623D127A9062814BC0EE4EC396836881D6B2EA6831BF407BF9F484BACDA31A4679E037CB4D25F1FD3F3791F0AF95C0
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.....Z]Wr.....A..Eo.....'.LI....O....0H..y7.....\.....(S.....`X.....L`p.....L`p.....Qc.D."....oCONFIG..(S. <.`4.....L`.....Qe....._updateConfig.... Qfv..1...._defineCookieDomain..$Qg&X....._defineAgencyCDsValues....K`....Di.....&.\.....&.\.....&.\.....(Rc.....Qd^.+ ....._onEveryPage`....Da.....c.....`...@..@.-....dP.....X...https://dap.digitalgov.gov/Universal-Federated-Analytics-Min.js?agency=DOC&subagency=CENa..... .D`....D`~...D`.....`D...&...&..q.&.(S.)..`.....@L`.....PQrz&.D...(([^.\/]+\.[^.\/]{2,3}\.[^.\/]{2})|(([^.\/]+\.)[^.\/]{2,4}))(\/.*)?$..Qb&.1.....test..!...Qe..p.....SUBDOMAIN_BASED..... .Qd...i....toLowerCase...Qc".0.....replace...Qb.....www.I..QeJ

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):	5.504425891531673
Encrypted:	false
SSDEEP:	24:iIQL2WBoIQsWBoIQDvW3oIQnwWIoIQvWDoIQTWMoIQp2Wz:iLLtBoLfBoL63oLnLIoLODoLaMoLptz
MD5:	1752EB01937895ED3F028471EE4CE0E2
SHA1:	310D6AFD14450C1BDDD4043652B2BCF7EC17DB1D
SHA-256:	D72937AEFD22DE8F96F7EFE42DA4EA3572C02D7980F5ADDB45B95305BE76B7A1
SHA-512:	270E4CE6CF9CF4CB441324A50714FF7AA143B8C133A1D84F0AE6FB57C256F9881968811CD7CCE3D16254DD08F0EB4761E53E0EB3244282441B7E5E90A175F5F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F....{....._keyhttps://www.google-analytics.com/analytics.js .https://census.gov/....i&/.....S.....N.OS.J.w.....D..4..\.....A..Eo.....{.p.....A..Eo.....0\r ..m.....F....{....._keyhttps://www.google-analytics.com/analytics.js .https://census.gov/"...i&/.....m-.....N.OS.J.w.....D..4..\.....A..Eo.....''+=.....A..Eo.....0\r..m .....F....{....._keyhttps://www.google-analytics.com/analytics.js .https://census.gov/9kY.i&/.....O@.....N.OS.J.w.....D..4..\.....A..Eo.....W'.....A..Eo..... .0\r..m.....F....{....._keyhttps://www.google-analytics.com/analytics.js .https://census.gov/.s..i&/.....g].....N.OS.J.w.....D..4..\.....A..Eo.....ctR.....A..Eo.....0\ r..m.....F....{....._keyhttps://www.google-analytics.com/analytics.js .https://census.gov/P...i&/.....f.....N.OS.J.w.....D..4..\.....A..Eo.....0.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\54d0f9e9d776bfe7_0	
File Type:	data
Category:	dropped
Size (bytes):	1220
Entropy (8bit):	5.566510536582933
Encrypted:	false
SSDEEP:	24:rd5FyL44CoLB1NLkSz9TxTSEh5FyJWF4eVRZdeZDX:rd5FysLoLbNLk6xV5Fy+vDeZDX
MD5:	D295A383B7FF938BB0E724541A27C8B5
SHA1:	CDA957393770EC09A4A256D37EC555B0EDBEB116
SHA-256:	A6BA4AB9437970B9953AF7730F5E00B2AF4FBEB1B79AF527C9C60540A4275DC9
SHA-512:	7850EDCE7565F71019B13F08121220056D64667FB83E2BD928469CC238EBE06670FB4404E0C921FDAA7D6FAFA25F1A135FEB90D26F64C412D1B3629A1AC1D6E
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&/..... t;...,R".....i?K..x.c.....F.A..Eo.....@.....A..Eo.....i&/.....'.:.....O....@.....h.....(S.P..`X.... L`.....L`.....Qe.S)h....CensusCarousel...(S.H .`L.....L`.....@Rc.....Qb....._.....Qdn.....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.@F..5....jQuery....Qc.Lfn....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
Size (bytes):	31189
Entropy (8bit):	5.732520380519748
Encrypted:	false
SSDEEP:	384:1qkkcW7g7S/HXbA6+Wvp3Wn/pwWCinWbBR8/hueYhcd9qocaKr6ZjdA+lmHBUEOL:1jkcW3r3WRNgiu8/qLpr6Vd/mHBUEhY
MD5:	AE8E6098274BA4EF311F50410818C475
SHA1:	2123E07BD254CA41693E43CAE5FA6CE55A9D1E23
SHA-256:	DBAFC0462E3569F3A8B10BD35607ACD5DA25C82B16800DAF66D7543186DABEBD
SHA-512:	67DCE8C96AC1DE8180091034000378C74B21D736BE1E51102D6C08C4CAF07D5BBCCFAAC58532D692779165359 43E855728C78B839BE262210E4B246FE8E852F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....r.Z...._keyhttps://www.census.gov/etc.clientlibs/census/clientlibs/modernizr.js .https://census.gov/.C..i&/.....~b....-L..V(d.gF..M.....".A..Eo.....6 .,.....A..Eo.....'.0.....O....8x..>.....d.....(S...`.....0L`.....Qc.Lfn....window...(S.M..`T....I.L` .....Rc.....:.....Qc.....docu ment.....Q.P.2l.....Modernizr.....Qe.....enableClasses.....Qd..>9....docElement....Qb..X....mod...Qc...W....mStyle....Qd".....inputElem.....Qcv..c....smile.....Qc.....p refixes..Qe.....cssomPrefixes.....Qd2.W....domPrefixes...QbNs[.....ns....Qc..f.....inputs....QcZ@.....attrs.....Qc...#....slice....$Qg.....injectElementWithStyles...QeF..... ..isEventSupported..Qe:M....._hasOwnProperty...Qd..4.....hasOwnProp....Qc.!.m....setCss....Qdz.X.....setCssAll.....QbB.....is....Qc*.....contains..Qd...\....testProps.....Qd..J ....testDOMProps..Qd.....testPr

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5858d13777102a84_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	69008
Entropy (8bit):	5.749357031305854
Encrypted:	false
SSDEEP:	1536:61m/sETblMzW6ggdpfU/bQvfyHmAjXG8pph:gETbl++byf78ph
MD5:	BFC4DD27AEF4A0A92E4AD1AD3880F8C7
SHA1:	C99C208F032A46D51A0D0B18E6D8766288974D20
SHA-256:	0FCB8FDCA0D0C5AEC4CF0B8FE1517B90E69FEDAEFCA8E62B54FB2CD41AB6F69A
SHA-512:	7F8E6C998F005077327B0FFD41D1312D0701EEAB467D8025A934B98D455210DA4C1C874FD56456D2F992B4EF561352A98255DCFB137F4437273C9FCBBB623BC6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....577D6B56FAC71FCB9653458F09AB6FE28574B0015E784AC0B791698B05E949DE.....'.....O....X..._.....l.....4..... .....x.....(S.4..`$....L`....(S...m..`.,....i.L`0....9.Rc.....Qb.iCy....w....QbJc.u....A.....Qb.eA.....ma....Qb...j....Qa....QbF.7....X.....Qb.[.q....J.....Qb" {.....Z.....Qb...;....na....QbZ;.....oa....Qb..-'....pa....Qb.).o....qa....Qb.@.....ra....Qbn.....sa....Qb.....K.....Qb~,i&....wa....Qb.u.....c.....QbZ}/.....Ra....QbV}.....Sa....QbjR.m ....s.....Qb*..D....T.....QbR.._....Ta....Qb.?.....Ua....Qb.....Va....QbV.....Wa....Qb.U....Xa....Qbr4.z....xa....Qbb86.....Q.....Qb.w.....L.....Qb.3.....aa....QbV]/8....ba....Qb ^.:.....R.....Qb..b.....ya....Qb.....G.....Qb.....Ya....Qb.,.....za....Qb...:....Aa....Qb..4.....ca....Qb..+?....Za....QbZ. ....$a....QbV.%]....ab....Qb...m....bb....Qb.rR.....cb.... Qb.D.....Ba....Qb."aU..

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\591c9b3fbc124fc7_0	
Encrypted:	false
SSDEEP:	3:m+l7bNa8RzYj0KKKXlMMIrATQUMLAFuLKvDlMRRdal/lHCuPgwUiP2y6wyChMm6b:mIYj018IrAkh6E0pMdugAg7s2KzQK6t
MD5:	FA6498D1E95EA06F5B4AC76557A9DAC1
SHA1:	5C5970A5FC6DADE1F7B6590E500EED322E2C8E08
SHA-256:	9A94A3664914A53454CE14734D76A999651283A5BD778B7874F7AFB70E417536
SHA-512:	4918459A688326F4C17AFF800D9691FB0D6D98C1F959636518FAC2A048038D76339436D26E8BEB040841864C8298E8491974BD7FEEEADBE19DB3D2423989EB6D
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/3O..i&/.....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):	533
Entropy (8bit):	5.452509211678464
Encrypted:	false
SSDEEP:	12:k5OaNTJjcGgOaNp9OaNEwWwOaN8lgE6OaNh7:uOiJjyOm9OCHOXqE6OE
MD5:	EC9503B4BE7C57E5960266627BCD0D22
SHA1:	338D650F6036B14F4A752539755E0CF42020E523
SHA-256:	560A73F1AF53F56798F01AD1295F5F22EF19C50232B4F53C5DD793ABEA1E619E
SHA-512:	F4D236E5B14833C501B50B6EB4AB824396F571FEDFAEAA0035C48D021D3E9B5EB4F23DC0EF2A764ADDE79406AA58498F4806A855BBF320558098BC34AB1B022B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A.....q....._keyhttps://www.gstatic.com/charts/loader.js .https://census.gov/.C..i&/.....k.....iW.r.i1....."....k7 ...Z.I..A..Eo.....q.....A..Eo.....x...i &/.....)....iW.r.i1....."....k7 ...Z.I..A..Eo.....Q.....6.i&/.....n7.....iW.r.i1....."....k7 ...Z.I..A..Eo.....?].g.....i&/.....RQ.....iW.r.i1....."....k7 ...Z.I..A.. Eo.....O..,.....U...i&/.....[.....iW.r.i1....."....k7 ...Z.I..A..Eo.....

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):	5.596634580789475
Encrypted:	false
SSDEEP:	6:miL9Yj018IrAETJcpuHxEpM3gJkqRjSSWDBsYnU/hK6t:11tnS8HKRVlLIBs64
MD5:	0B59D6DF10996DD3A277DBA485CC5235
SHA1:	7CC358E162AFC6C627BA997549FDB83495FEFEBA
SHA-256:	E5459B4D58AC485675F27CDB834948023020B875B6C6041285A6075538387156
SHA-512:	78E3F94DC38D82E84759F59B065415355405A537E618330F64BD0529CEC40B75279DBF46310E05D0C8BFAF77469BE0F9A39E9069DD0719533AB35F7350857A00
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/.*Z.i&/.....^Bw1..I..8o.. .....j..".s...A..Eo.....4~.....A..Eo.....

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):	5.687902801191632
Encrypted:	false
SSDEEP:	6:mMEYk+f2pomPMvmhmJ24VWtgTI51HRdmahK6t:Q++amAmkJ1W6OH+6
MD5:	009B335D22C268072C81F1FC4188ED23
SHA1:	16837B43EC49F0AEFA43D6427D1CA55575038A94
SHA-256:	2812252E69108992818F4467344604C270352509681E8B0D044E76F7A4D37BFB
SHA-512:	3A516DAB67B1CB7961FF9587C4DE81EBDC6E6819E66D6DFB86DDD16C516751970B03CDBA28FF5302FE8040D52BA44169E86E0F097F7960100CEC88D6FD57FA7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6214889f7c2e82fe_0	
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&/.....s.....H}.Q..U3.1g\..=..6..n..x vT....?.A..Eo.....@.T'.....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):	5.680647270788524
Encrypted:	false
SSDEEP:	6:m+/VYk+f2pom70XzhmJ2nWtgxDTs+xinVZK6t:FN++am70XzkJgWaDTuT
MD5:	A08301EB77D1F5AC8A47CB61243559F2
SHA1:	332FB20692AF09681F1EBBDE0FC61499C3426C32
SHA-256:	E9D5373F0B2315E72261E9FA46D98FA1447D48AC492B77FA6DCBA96164143FBE
SHA-512:	47CB787378A035B31BB146E3006EB0FB9EFCD13229B27C3C6605DCC2A5E507002E10EAE3EBBBDEEC7F580AA9F8D32E0C4B755540E9EA762F78BD7E1968DE40 2F
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/8.2.i&/.....w.....;...L.tUq9..,F....x..H. ....).A..Eo.....vU.....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
File Type:	data
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.520723258226869
Encrypted:	false
SSDEEP:	6:m0g6EYj018IrAoUBCxMGgH9/zw2NXnl8DK6t:Rw1tzUAWkQV81
MD5:	5324032074C2454CEDC34CA9307BE6AF
SHA1:	41935DEBD3AB8AC186FE8BC370BE4061A9EA5926
SHA-256:	F6C97E129B1ACA555B40CAF6493A05714C88B420FCAD19D644396AAAD437B160
SHA-512:	C951F774B219270B2D8C4F48E4BDA3DB6A67D51CF180B89B8E6D09C55129C521CAEE88EF7C38CEFAC53F4003345F49B5E714FA96647B4A9FDA80EBC0B5D931 5
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/B.Q.i&/.....c.k.<.Q.3R.9F.&..;.W...`P....\.A..Eo. .....z.....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):	5.830791442838807
Encrypted:	false
SSDEEP:	6:mTSlXYGLKciKyBZKsQAUWFVSqUbgB6kpN8KBRAFnK6tNQ0kVhSGkKTGHnpHuWuO4:8Wq5rBZNQqFrUg6kX8Kgb+tkKTmpOWus
MD5:	C1FD73AB3B597CFF93EC2EE68550620C
SHA1:	9585BEA80147EF3873531B670B9FF2DEB8D48114
SHA-256:	C42540BA67A0BD740F45875D661DACC646C54923524DD0C56AED8946885555EF
SHA-512:	391C7CF3CC2A90D2F6D6379972C2E8BB268DB7A3F8456B0E4CD68EAFBE07ED4555121DF44F1E2EC1F20DCB7C079D511055DAF5BB1525EB18BD6965CCEA6A5 D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z.....1...._keyhttps://www.census.gov/etc.clientlibs/census/clientlibs/jquery.js .https://census.gov/....i&/.....+M...f.d...4.Y/rI5e.-aRg.....A..Eo.....k..i. .....A..Eo.....i&/.X...BA6469834505F430DE22A02DA58026D52CE6F91233FBED038E8DFAF7E6FEDF9A..+M...f.d...4.Y/rI5e.-aRg.....A..Eo.....Q.AL.....

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):	5.504357139737847
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\731d22992491e125_0	
SSDEEP:	6:mwrnYGLKcpK0IE9VjWFVStSrHgyEc891w3xzrIhK6t:VWrqqF+kEcCW3xU
MD5:	4C9B209C432A3108318FE9A37B9A2FBC
SHA1:	7B0541A88856BEBCF6D0A0F6E181E7FC02D1CFCB
SHA-256:	2DDD80AF026D153B0CFBE70EB113E19A016156A3023035C69D3A19AC1E2CE153
SHA-512:	FB46DBDD8A486B6893E3CBACF4A485BF3E282FB6FB1CEF3A317FCFFD30CB0CF2543CD38D220D2C7C5C503A570CC3902BE587A0CA40C711D7FFD682F1A4AD E76
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...3....._keyhttps://www.census.gov/main/responsive-header/jquery/jquery.js .https://census.gov/....i&/.....8....^.....20.\..M.;w.%.R..A..Eo.....E.I..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73d1d61ae8236299_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	175616
Entropy (8bit):	5.686014841222375
Encrypted:	false
SSDEEP:	3072:8PyRsrX8dkALpK5sUO/wDrpPrpoxgC7fcLUAuKagkyixiCn3Fhv1tynwylHeP4kD:8PQVrvDQ50P4kD
MD5:	4FFCD4B2967224B1C06AD57CA4BF1517
SHA1:	0F1F94A45705B51FA2AD9A45AE94FDC9C3D95F23
SHA-256:	784A90697256C9C7E7EA7C41AE90A241AB85F709DE1B1532DDEEA9EC2A7A7F55
SHA-512:	D06982AFA2DA3B3143E6BFB060BD3E4535FDA8DD065139EF735BC778ED31720BC65A77B4F7AE4A8C98D1A65289D85ACAC54B3C7A1442A1C6408AF92F575010 E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...).g.....BA6469834505F430DE22A02DA58026D52CE6F91233FBED038E8DFAF7E6FEDF9A.....'.:.....O:...H.....0.....P.....4.....I.... .....h.....4.....(S.I...`F.....L`N....(S....`.....L`~....XRc(..... Qb".d.....uuid..QdR.....runiqueId.....Qd.....focusable.....Qc.P/'....visible.e....$.....I`....Da.....h...(S.....Ia.....q...q..@.-....PP.1.....A...https://www.census.gov/etc.cli entlibs/census/clientlibs/jquery.js...a.....D`....D`....D`.....`T...&...&..Q.&...(S.....5.a.....a.....a.....Qb.v.....fn.....a.....Pd.....extend.focusa.....d .....(.....d..... .....Q.@.....focus.....q.....d.....D&.(S.....a.....a.....a.....a.....

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):	5.4604618417534665
Encrypted:	false
SSDEEP:	3:m+letK8RzYrSLbGtGgnRMKLSn0PIP2vDGLXWG4kKWv/l/lHC+mXlaM6dVmR1pK5M:mPnYGLKcoRMQSnN4kKyg+mla76RDK6t
MD5:	CE494932B6B4A9B0FECB4E0012D85E7D
SHA1:	C9DB7599C061B2323065EBAE21D249CFE4DA3CDC
SHA-256:	6A03E470ED3B390AB8C7E4F80C431DE3E115E0EDE7FF861B37B164387EAD472A
SHA-512:	FD44F26EBFC62AE7BF63F38150D4D47237D662AE3B15A31C6092746214D93F5D1004AF319AB33ECBEA4FA09786FDF9096105D3ED1EAA9B40A9C03EBF06A0AD D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...Nq....._keyhttps://www.census.gov/populationwidget/js/counter.js .https://census.gov/..T.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):	5.702611209263974
Encrypted:	false
SSDEEP:	6:mjEYk+f2pomWzVeAOZTLahmJ2+Bgv/E4k4eK6t:0U++amMOZTmkJTU/zk7
MD5:	9EDCEBE056ED863DD3CDBC05D0636B11
SHA1:	6F7A77CFA100AFFFA00340EFBAEA1CF71AFDEBAD
SHA-256:	0094ACE1216BE4A2001B33FAF04764952780C3F55242C63572B3E74E7EC70F54
SHA-512:	D0B78BB62D5AADCA5D4FB2980BC9CDD8838256ED93527D37E1591E0F66F537160A2A577BC6C2116EBA6383EAE126EF16CC713B77CD5F54C642A91A03F53204 4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76015e3a4b6224a2_0	
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&/.....v.....gE.2 @h[.R.g].Sqx...:7.Pl.8.;,..A..Eo.....n.L2.....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):	5.518176262648707
Encrypted:	false
SSDEEP:	6:mLXYj018IrAkRu6spMJWg6E2GKgw5arkontrK6t:WP1t3Ruvs52GeEko7
MD5:	877C1D32BE080BA52C3745A23300095E
SHA1:	FF9DB423AAB2D129640E479D3447C4761A088E2D
SHA-256:	40C071B127C8B1CC7365770C733752A11382881EB4AA0853E445E20BA1BDADC3
SHA-512:	1C9AF39050041EBE3E7A9A9BC670D3C2E4457B7FB9DA8EC84D4B87E9EC6E8A481CB1CA12FF284865BA6ED4CEEB06E2974604B432948F9CE02BCCEB2B8FA02 165
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....j....._keyhttps://abs.twimg.com/responsive-web/client-web/i18n/en.1f1c4ce5.js .https://twitter.com/W.Q.i&/.....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):	5.477600744249595
Encrypted:	false
SSDEEP:	6:mlfYGLKcoRMQSnGnRMQ1Z3HgF6jp4eg4ehNK6t:yChSnM11g6jp4eyF
MD5:	38464A0D4C486608BBC9EFE55A04FC6B
SHA1:	07E1816AACD281A4467A473FA2AC6AF2050E4FDE
SHA-256:	C8ED538AEDDFEC624C0D3AB1615898C047C1E0D583B9DDCF6ED2DD5F96F7BE90
SHA-512:	8ACE41BAE64187CF242E83D0B1C10D8DA570474BBE850CB2017020D3BE7FC38696454CC12201B5F68713D67D78CCB6ADBECA335FCEFA84FD03819950E1B8EE 15
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://www.census.gov/populationwidget/js/population.min.js .https://census.gov/Z.U.i&/.....>.....BF...F%..\.~.;A9....6.....v....A..Eo..... .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):	1340
Entropy (8bit):	5.291381889022249
Encrypted:	false
SSDEEP:	24:uqIjsjUDddde7n/h5FyiWcotnytIV8GMVN1/dg2qYPnffL84Be56SZ4:IIjsgQbZ5Fyi3otnyvN1/dggnffro56v
MD5:	DC379FD83855B5983A7E4D50EC5ACA4C
SHA1:	906FFAD2CC9EFDCE56F89D82B3FDA95594951B46
SHA-256:	CADEDA8E7EBEF6BB530F7AC6CA3A9BEFFBFBD6859FD97F7EFAAF962EC0ACF117
SHA-512:	F1B3A458A05074E92FEFAB3BDE11B879238450530550D7E5D2315A69A8BE42C4BA032B86BA1DE21B621B297913BE266D715E724E0D3D4A6D6921EB5B3375CAC D
Malicious:	false
Reputation:	low
Preview:	.D..i&/.....'.....O.....3.....(S.0..`.....L`.....(S.p.`.....4L`.....XRc(.....Qdn*.{....addControls...Qd.....buildButton...QcjJ.....clickAll..Qd..a... ..addObservers..Qe*J.....watchChildren.....Qe.o.....checkChildStatuse.....I`....Da....'...(S....Ia....J.... ..f.....@.....@. .....!.....@.-....hP.....[...https://w ww.census.gov/etc.clientlibs/census/components/common/core/accordion/clientlibs.js.a.....D`....D`d...D`.....@...`....&...&....&.(S.....Ia....X...I.....d.....@.....&..q..D&. (S...laf.....d.....@.....&.(S.....Ia,.....d.....@.....d.....@.....D&.(S...Ia.....d.....@.....1...d.....@.....D&.(S.....Ia_.....d.....@.. .....&.(S...Iav.....d.....&.'..@.....d.....@.....D`....DI]d.....@.....a...A.....,QiN..v ....uscb-accordion__expand-collaps

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\831107adf264f338_0	
Size (bytes):	232
Entropy (8bit):	5.480973549566121
Encrypted:	false
SSDEEP:	6:m/l/XYj018IrAWQ3nMBgJkKPqiNqVPm4EbK6t:kln1tBQ1f/
MD5:	B2CDEC588F854169CD48A4946DAF5E6A
SHA1:	9A8EEB3BEFC57BD1AB596992C23CCC6D10DDF5EE
SHA-256:	A0FC817F98236F46AED1AF4AF8E88CFB6FAC250CEDF8521E415B19B4C9125452
SHA-512:	DCE79D1FC10467BB9390F299FDD20E36BA7A1E3920C485065083916722D2B930BEA0503541FBB64C87749C06D9FB318A92C7A4DD414B62227AC328237C3C2E3
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/d(Z.i&/.....4.m...G..G.c/.M...I....H..O.J .w.A..Eo.....S.....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):	5.345357947169151
Encrypted:	false
SSDEEP:	6:mEanYiMs8pMTWtgDm9j8IcNupgLrOK6t:MrEgIc8pn
MD5:	ACC9791FAA971B6AE6A4140B18029C2D
SHA1:	01285EF25FF6292172BDA65A2EE36AFCF7CD11C5
SHA-256:	F2A9716C073E460690575D2881C5E992BE0CB0F115DBD5C7A98DEFA7EE75FEC7
SHA-512:	A3E42567686D8B2B0B4AF5349E6AD3F84A8AE72F73C245AF75EB00FD66E1F76CB395CF7D80F9729C57EF3D426A963886484237CA335DCF607575BF772F05DD5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....._keyhttps://twitter.com/i/js_inst?c_name=ui_metrics .https://twitter.com/..c.i&/.....D...L...9..g.....-...m...oN.B.A..Eo.....9..f.....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):	5.88810535357424
Encrypted:	false
SSDEEP:	384:Lv7WNNNSI4j7uiEkPLMMU2JToRScG96ELORg:LvKAdmiEkPLM+ZokcTELOG
MD5:	79E1044BF7DF3F4963CF0FE55B847CE5
SHA1:	683B47092D60BAC179A76ED75C728F8A34AD592D
SHA-256:	C2F064FD0E1CBF75AA0502CF66DB05D8E23F1DAE4A3D8B5E1A2CC35A9E9DCC2D
SHA-512:	73BB94031A615A9CE3ECCE2A7DD6A379F7FC57097111B0506F1FDA21698FABF2204C5F871E47E017FB6A02FAB139829A9A44347FCF3CDDC9DEF9B61CFB5C75D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f.....p...._keyhttps://www.census.gov/etc.clientlibs/clientlibs/granite/lodash/underscore.js .https://census.gov/....i&/.....3.Yt.I..G.&.e..B.W4..9..1.. 4Qu].A..Eo.....\Z.....A..Eo.....'.(o....O.....K...o{4.....`.....(S.<..`2.....L`.....(S....`:.....L`\.....Rcv.....Qd~.....idCounter.... .Qez.....indicatorObject...QdB.l.....keyPrefix.....Qd./.....reNoMatch.... Qf&.....reUnescapedString.....Qd.....argsClass.....Qd.....arrayClass....Qd.N.....boolClass.....Q d.....dateClass.....Qd.p.k....funcClass.....QdV.. ....numberClass...Qd61.....objectClass...Qd.F.....regexpClass...QdZ.cW....stringClass...Qd>.....objectTypes...Qen4d .....stringEscapes.....Qb..?c....root..Qd..S7....baseIndexOf...Qe.)B.....compareAscending..Qe.....escapeStringChar..Qc...#....slice.....Qc.j....arrayRef..Qc..aI....oldDash.....Q cf.s.....reNative..Qb...\....ceil..Qc..w.....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):	5.617275203451089
Encrypted:	false
SSDEEP:	3:m+lPk/l08RzYkwIAd0CW/KNGKYGR8AWhEFnLxKS9Cal/lHCynXunNK81SXD7C/Mc:mZtVYkvwyGRZnN19rgyneYrczbK6t
MD5:	5BC55082C4807FD8BFFFE58499F98749
SHA1:	668552F30A0A7A118C35DF7D7630BB9DEF840DA0
SHA-256:	F94CD2A3C9C7ED368D52FA46DE7A04A37ADAFD98BC77FAC4FA2B43AE58CCE392
SHA-512:	95A1EB6A3DAF8422B8F9FF5C6038E7BDF550934A492A13BEED8B67B6C6D84167A86246A748935A6B159CFD09461EEAB1216C7CF8AB7558CA99CDBC95DDEDDBD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8590095ca51749a2_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.....1...._keyhttps://static-exp1.licdn.com/sc/h/4zwn84zqft7j8zx33rolrjq6b .https://linkedin.com/.!t.i&/.....{.....3...S.....Z.....L(.....m.&..D.A..Eo.....D.....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):	5.51331852492675
Encrypted:	false
SSDEEP:	6:mhYj018IrAukGQAgOMPIgjbYLFig8/hK6t:s1tRnQ/7TYLe7
MD5:	0F4C1D453AE046DA31EAB6AC5C4BB54D
SHA1:	4BDE9442CCDEF7C0D64F93BB4FF2598A9DA1650A
SHA-256:	24F81F3710C8C241A07AA26A890C5FDBDB0842B9ED3285EFDE66D65DD45DE430
SHA-512:	366CB4FA4A73ED235F10E104CF7131AD8DC4AE39BB902C459C41BC36237A4DE4DD9FE8F5D2CBA73702DEE7C89260ECD025D4A9B5AC8870187EC98CE4941D71D
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&/.....r*._..\.O*f..^.../.LN..5E.U...A..Eo.....!.....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):	5.6965728007877345
Encrypted:	false
SSDEEP:	6:mSYk+f2pomdMGw1VwhmJ2uIgB3IGH4LZK6t:L++amdnkJZlIGHkT
MD5:	C11CF7E81A642C984B0F3E45C828C549
SHA1:	20371475435364AE4B05BA417892805EF6AB1B5B
SHA-256:	D3D8F163AEEC48C8E9002F3665292A4228F176EC3BDEB8484F2661F290F17328
SHA-512:	BAB4DAEADF801B74EE0BA70F3C8FEC8D62E225EBCA04367C21C5ECDF64C892F32BB88A5B160C5ED13379E5A7407A3BF2A5DDA07B2B06DBD3754CAB9DC1DBE261
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&/.....zu.....C.I.GI:.....8.~....[x.?..''...A..Eo....._.....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
Size (bytes):	4485
Entropy (8bit):	5.943525077819969
Encrypted:	false
SSDEEP:	96:NiHi/fttFQX4pp46/4yUAogPwHJT4JaFW8ncUJROY3UnA3yjKuJR:NyyVtuxyi+wHmocPY3yz
MD5:	D5782FBFB7226F0FD89A19E68A41BE35
SHA1:	5ACB3C0021E5CB81C37C7C1E6B42714CDFEF9E93
SHA-256:	696438B5D5BEA7650D5ACE2821D8CBA86AAB6777100B901AE8E34569945A83E7
SHA-512:	487748063DB2C3CB55C8FF3060C125C420E3473C7C997C5BFFC3EB649E4710B24572576AC536A3172D74355CA6B5EDBC9C91D5CB13CF95EE7CEC03F153677
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....C.C...._keyhttps://www.census.gov/etc.clientlibs/census/clientlibs/analytics.js .https://census.gov/wg..i&/.....L.....&...)...P..1.t|O.?2....A..Eo.....n.....A..Eo.....'..%....O.....&.....(S.....`.....L`.....L`>.....Qc:.p4....curHost...Qer.....govDomainList.....Qd.....fileExtList..(S.....Ia.....QeR.Cz....isInternalLink..E.@.-....PP.1.....D...https://www.census.gov/etc.clientlibs/census/clientlibs/analytics.jsa.....D`....D`v...D`.....D...`....&...&....&.(S...Ia....D.....QejW.....isDownloadLink..E....d.....&.(S...IaY.....Qd..q.....isExitLink..E.d.....&.(S...Ia..... Qf.....bannerAlertLinkClickE.d.....&.(S...Ia.....Qd.$.....linkClick...E.d.....&.(S...Ia....i....(Qh&.....bannerAlertCloseButtonClick.E.d....$.....&.(S...Ia..... Qf.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8b610968227cbc8e_0	
Category:	dropped
Size (bytes):	290
Entropy (8bit):	5.683030008437678
Encrypted:	false
SSDEEP:	6:mrTtVYj018IrAMUscQQc0HNy1x61GMGgsCB89h0K6t:IT/1thUsjUHyCBL
MD5:	4FF3B56B1AF1577277F454AB5A73FEF0
SHA1:	72BC3CA61306E85A8B52587BD967121B78E8EBD7
SHA-256:	215A64C66EC05101E2EC6DA73070D5AC61C973C01447A01B02DB67FB6DE33384
SHA-512:	FCB836250BFD1590F5B825EE152CA05C3719990247664486102C8816BE3A56BC998738DE7C4F024D81B5488CE689AD795E26DCED2D050D9586B9113279471C71
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/4.Z.i&/.....N.".G.b_..\....0%.[1.:Z)e.....A..Eo.....K.@.....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):	5.557017891582787
Encrypted:	false
SSDEEP:	6:mnKYj018IrAE8G1lMNAFgLk1zCveQMrWK6t:Q21tgG1701zCnj
MD5:	2437B1FB7022AF7B0DB8675DEB114736
SHA1:	A9A42C1971EED871D776FDF199CB3B276360B84F
SHA-256:	807FE19165DA8B9FF7A3EDA839ACEA54DBC0ABDDC71BE9D4DF5A6F86EBBAAE06
SHA-512:	4E1FD1116123342FDF3D63AD7D5DC727FFEC7172F5322F35107D5769DE764E7545A7E8995EEE360CDC13A04B5C5F54D0BC92A9C525B483DBAB2253EDB43D8A0
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/p'Z.i&/.....]^!..=:.{.Zl.6..^..HF~l5J ...q.b.A..Eo.....O].....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):	5.734530731931535
Encrypted:	false
SSDEEP:	6:md+oYk+f2pomWptt/ahmJ2KwrgMrffHsFhr8nK6t:lA++amgt/akJO77fM4p
MD5:	48D0C02AC17D18F1AFBC65CCC1A57EFF
SHA1:	5D7CC5324E2F30B0145465364CDC56E305846EFE
SHA-256:	A2DFE4ECE33913A55B7A8310BF2F3FFDD8682C0E73830A591BEEC22E1F4919D7
SHA-512:	CB6C6B01F4A61724A3BB839769967ACDF9678F4B253AF81B340B4988FF194CA911FD879BEB7A3DBF29A86C5A179766C7060F6493DDB9D622C3CEDEC72D1E1DD
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&/.....v.....L.)A. .... (."......k.....A..Eo.....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):	5.568698745771859
Encrypted:	false
SSDEEP:	3:m+l77Zv8RzYrSLbGtGyrsSN2IKKoT9LRHKEBM+LK7GLXWGVLnvll/lHChXzLENtd:maZEYGLKcLQ2IKt9PjBg+LrFK6t
MD5:	102FD3EDCD4CFA293CBD0434BEFE5981
SHA1:	8B5F36EF53A15B66C8AB25BD4DD2B072D6B22B2A
SHA-256:	9A362E1A77736145326D070D9E2FA3C99F15B606DEAE2AE10DA02E076AC1E03B
SHA-512:	8CA6CF76AA7B6CC04440AD74C58D843A154EBB42D14F80004CF402CEF95C0A5E7E214F94C1BE721B6042F6FC62FB6A367E8B0D71A0F6A68B2C4E0BE789C7FD30
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8defe3daa4bc95df_0	
Reputation:	low
Preview:	0\r..m.....c....#9....._keyhttps://www.census.gov/data-tools/demo/hhp/runtime.689ba4fd6cadb82c1ac2.js .https://census.gov/...i&/.....b>L..l.....?.....yh..(|.A..Eo.....9x.:.....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):	5.558163257846036
Encrypted:	false
SSDEEP:	6:mByEYkvwyEbA30VfNbgENTZISTS3tY9bK6t:4bvwy/ENNTNNI4EKN
MD5:	8FFB7B4F1C82C185B6D355818591A92A
SHA1:	CB9FF8E5EEB0E61C4FD33BF906829113F6CA53EF
SHA-256:	90B8BF7D29B2D677E10C2F2FC3BDFA55E6A2BD10A807680E1D7E57B07D03E33E
SHA-512:	923910E22ECCD2D3AF143785D690EF1869C487983B2DA7A0F463019487F8B39A6E3C35FE10C42737EA0EB69ED48002D941DF35F06266206F88A76B15AEA83998
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.....2...._keyhttps://static-exp1.licdn.com/sc/h/58ikgnh04in2ngtxjdu5jjic1 .https://linkedin.com/Z.t.i&/.....z.....vA...X..$t.b.^...'....'.[...A..Eo.....M.Gk.....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):	5.730467826758859
Encrypted:	false
SSDEEP:	6:mAHYk+f2pomWQr62VwhmJ28IgfeKtSLebunMK6t:h++amN6lkJLSiSLeie
MD5:	975FB4577703E07F586E13E0C9028B28
SHA1:	331909ABB44A652953B7519A5AFCAF21B7EB37EA
SHA-256:	D3D15E4AA0C77882C83873B9237F4B93837BE428A7235630A3B4023C747C9D3C
SHA-512:	7F4D1CCD6F5352FFAD5BF2DB4EB3601A415DF6BF03F4950C4A9474F8773E5E02F3089FDFB0EC2E15B149616918C9FA03AB986033DF36CB7816A0A122368AC8EA
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&/.....:v..... .....jC....u'*Z...B.yty...2.).A..Eo.....M.....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
Entropy (8bit):	5.568727863089258
Encrypted:	false
SSDEEP:	3:m+ls/HtgOA8RzYj0KKKXlMMIrAKTzKXF3OolMRub4Jl/lHCIkn/tdO04w7WmufzP:mWEYj018IrAK+OiMlgT1QnK6t
MD5:	1B21A04B07E63BA155F9CED047FFC1B9
SHA1:	C49BE50B5FC73AE2FCEF62D7C3D9014895A7BFA5
SHA-256:	2C1102720E5AD95C78EBA04EB08422384B694D84D8EC977CC925F13ED96AFC2A
SHA-512:	95D0F9B33739AE9C4AECE66F1AE5BBB25688EDF96515F0A2DAAF8DDEAE43B8A63D01625DD6FD725BAEB411A0F58D83EE045ABC1928C5AFD91A8FCA25CA05D187
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/Z~Z.i&/.....G..J..u..z.D.....&;7v$'....E..A..Eo.....U&.....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):	5.354142652787218

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99c7340fa3da6419_0	
Encrypted:	false
SSDEEP:	6:m2SEYGLKcoRMQSncRMQ6dvKnRMQ6dtZBxgAnrOYoe29hn7K6t:hSZhSni6dSN6dt/Znr4e29ht
MD5:	11C33CBCB3B78B6C0016FF8D4004EB86
SHA1:	5605DBA2B7E4F22E5910AD798CF99E97AD9AF6E1
SHA-256:	4B85C605B2E97895CE39AAF1A5562BBDCADFE58E059156DB49681DB8D0E22E7F
SHA-512:	736529217AA7C0952779D18F116BD42A1CCE397204E96DFE3AAEDCA54F670B5776F5941E792B821E92E3A74D7A2C55C3785D0243789E56F102D099C758F86B52
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v.....0M...._keyhttps://www.census.gov/populationwidget/population_counters/population_counters_controller.js .https://census.gov/h6V.i&/.....?.....j.Ly..u~.b .....+7.6."c....,.A..Eo.....-.....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):	5.428148685833429
Encrypted:	false
SSDEEP:	6:mm9YGLKcpK0IGKWNlaHgO0N7kBe5UTK6t:urElucW
MD5:	959E20BDAE25532DD10B029B62D760E3
SHA1:	9153F71E7A182C17FDA024BCCB4787A4AFBD3083
SHA-256:	0280491225C6884C9166A02C517F7FF04155383C8F1956F6F45EF91FCE720278
SHA-512:	30466704BC6B8CC78F34DB7EA440E4798951F192DCF6218E03C6EA467B334FC577EF457B23FDA70264CF8A3BAFD525C9ED10DFBD8E9A809DCC467B67F3342A1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...~....._keyhttps://www.census.gov/main/responsive-header/js/typeahead.js .https://census.gov/o...i&/.....&.>...L.wK-..m.....\....F.qO.A..Eo.....G+t.....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):	5.419486186220956
Encrypted:	false
SSDEEP:	6:m3YGLKcNQKtENFPZqHgQXjJVVTQGNTfFr3Ea/bK6t:nEQr1mTBTQGFfVEqN
MD5:	2CA19A0D743AED5303763FB881230F18
SHA1:	93FEEAB4A6534C613AF6464D365FC4E4002930DB
SHA-256:	B870FEA99D35CCF348DC668F45B307556F8EB162E3CF7CD03FAC24ABED63502C
SHA-512:	6908D36900D9726A0B3BF359D8F3CDA42551D294EB82771C4A3E135CAD0D12F113E2B9D683317F0AB007F31C71A83240184388189921416 5DF72DF9DF212A7BA
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.....z.!.....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):	5.7496992784388
Encrypted:	false
SSDEEP:	192:VpnF7CBw8agYXDw0ejxrvVnKfukwpmceh+fx2rMG3le2zaosxxjq5FlcMYxuxn:/wxrAfufmfWfGYhxFS4
MD5:	96E7E2C63841808E182AB5190DB42198
SHA1:	31A0DA739E56F2FAEBF79EFCD1B7B9BA461AC241
SHA-256:	713775142A58670D47E20330F470C29B97869CEC61C80588498C1E5E12CD07A1
SHA-512:	6F88C458A2A944B6B7C91558212319865D00C4C6826D9211310EED8C7C4670576AE40B2F8CFC3CF4A54730A4A209764626366A772958EBDA293CA9E1077BAF84
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a365c7ddd6fa6bff_0	
Preview:	0\r..m.....Z...E....._keyhttps://www.census.gov/etc.clientlibs/clientlibs/granite/utils.js .https://census.gov/J...i&/.....v.M..j..>\...M.+....!.....U.I.A..Eo.....A..Eo.....'.....O.....(..N.....(S....`2....TL`&....(S.h.`.....L`.....Q.@.....module....Qc~-k*....exports...Qc.Lfn....window....Q.@.6{D....Granite...QcF@?.....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&n.....SELECTOR_INFINITY.....Qd.*u.....infinity.....Qc.!.....CHARSET...Qd.}.5..._charset_.....Qczd.....STATUS....Qc.....:status...Qe.,.....STATUS_BROWSER....Q.@".G.....browser...Qd.we^....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):	5.594504675023007
Encrypted:	false
SSDEEP:	6:m7rnYGLKcLQ2IKsXi3BMygQl/nAbfFUp3K6t:cr66KQA+
MD5:	23923E9E3365B931802C81330392BB93
SHA1:	693AC1357E1C05408CA6C257C88509A8DF73889E
SHA-256:	35B4679B0CB17710EE1F0C3B5559EE80C66FAB81C68A6BFFCC00C40CF7554821
SHA-512:	7978560B72F77CBD3E6FF0D729B631931D1B005578BB964F2E5FE1C0F6CF122860AD7352F607FFC555AD43253D89C2177F7BF90BA08FFA0DB65B4317C7788803
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...}..N...._keyhttps://www.census.gov/data-tools/demo/hhp/main.79647588e103ae3fb146.js .https://census.gov/....i&/.....C.....,X.I.c|/.....J[y..^*..5.*..~8..A..Eo.....V.....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):	5.557194173778523
Encrypted:	false
SSDEEP:	6:mm26EYsyZcvXsqL7BfZWSlbbg6XlZe1De//n3ZK6t:dPO7poyXlZJ3T
MD5:	419ED584234EB4A2786C4A1A8B2DD11F
SHA1:	55A18F05A08935C60DEFF6256D8BD520817EA5C2
SHA-256:	7BFA2DBF8AB0014F3FDD8ED8C47655769E4FB6F7C1D984C2F0AF7E4394D7B1E6
SHA-512:	DBE104494FCC52E983BFB1F0BA6FDD43B8965106F1675225C6DFD714C51C3AE02CB5173B60D2F2C5D45D15849C97AA8A02F86C60078ABD3DF89E52D9DE74FA7
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&/.....qNd.....M..O...'...d.T.WC...A..Eo.....R.hv.....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):	5.414157114064089
Encrypted:	false
SSDEEP:	6:mW/XYGLKcpK0IiLElQOEXt+lHgnH0xDWP40/ZK6t:T/qrw1tH0xAr
MD5:	879AEA9C463A6A2A4645125A72D0444A
SHA1:	0C8798201E6521A0A344EC4DF6FA830477A54D89
SHA-256:	17F97347F7852178201229D129F65FA5EDA22AEE1750725A1097C4CB619077A7
SHA-512:	E0282114614818D99F616BD3778D8A8853E863B74A1828F3DCB707ECD3DC257250A76B089BE5D646DB7BE92DE7A98446A8250AA18DCC782BF4D4830EF922A7F
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.....ho.0.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a830cf2055d86cb7_0	
Entropy (8bit):	5.4072241424522565
Encrypted:	false
SSDEEP:	3:m+lKP//la8RzYrSLbGtGwNQWkGPWFvDGLXWGWeQi1/l/lHCjtQrXVGUPZuyhMmwj:mN9YGLKcG5ZWeQygWrXkzyhwHK6t
MD5:	01FEAA800F7D37926B19EB331F833112
SHA1:	AE5B768874BFF0C31B619EFB64B128C7E11F29C2
SHA-256:	67B77A5B1C312AB69149C77BEA1E8DFCC6FDBF8152BAB6DCA29C3966F85C9E47
SHA-512:	77C244AA16D98BA5B046E65DA567155CE3234C374E073C285A13A7B047A28680A7D7D44B3494E5CDFFD5FA4FDD5BA8EE8FA92C0E2F7AAFD0BE1C9B4E6F7CC9AD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...U.P....._keyhttps://www.census.gov/main/resources/js/census.min.js .https://census.gov/.;H.i&/.....j>.....3.....F.~.k....+Q.4...C.A..Eo.....K".....A..Eo.....

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):	6.0045504475995966
Encrypted:	false
SSDEEP:	6:mbXYGLKcNQK1UQTjJ7ZZFg8X+BO4jMK6tiK6GwszQcQ6Ydf0+BO4jll:qqEQK3J7PSYtblzQDVJYO
MD5:	DF8065ACA8AB0655056BFB232925B499
SHA1:	375D00D1F80ABB53D0FCBCAE9D07D7DE03A478A9
SHA-256:	A8BD43D1D259A2FA252E02EC25213C45E2015A678BD63E97A2DF1653787D2AC0
SHA-512:	D08A11482E87091BF62B95F1E0330162C66DB4BA02ECA46226557DB901E5104DE9754C3B8CD085A9A5A2652B9FB95FB76C04A0985CBA289E1E3F294ECA2978A
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&/.....Z.....\.....d.L.....Gk.Bf....^w.A..Eo.....t].....A..Eo.....i&/.....577D6B56FAC71FCB9653458F09AB6FE28574B0015E784AC0B791698B05E949DE.\.....d.L.....Gk.Bf....^w.A..Eo.....PS..L.....

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):	5.762776747284409
Encrypted:	false
SSDEEP:	24:Ht8mlj5ZthIpNZt7RZtkeZtmFpZtFEcZtS4r:HVIlZs3ZVRZmeZUFpZfEcZk4r
MD5:	6601DB5B300B9AFA8120FD553F97F6F0
SHA1:	D671F41CDC812F9648F23A575106A73DD5D2EE59
SHA-256:	867074DD698D31E01BC7C063B54542431D3FBE24EA0A50E9AEA32C7F1BF4C51A
SHA-512:	CA05C6A1951698DFBE53FCC38C1FDA7C3E67569801BCD978A885EFB0329F665F05D50D4DF1256E1F4A8B92F3509C962C049D1AB8485AEDE3764D9CEA5A94DFA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x....& ....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement.min.js .https://census.gov/v...i&/.....*..b....O..$E.`....V..7.....A..Eo.....A..Eo.....0\r..m.....x....& ....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement.min.js .https://census.gov/....i&/.....~).....*..b....O..$E.`....V..7.....A..Eo.....E.....A..Eo.....0\r..m.....x....& ....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement.min.js .https://census.gov/I.:.i&/.....8.....*..b....O..$E.`....V..7.....A..Eo.....A..Eo.....0\r..m.....x....& ....._keyhttps://assets.adobedtm.com/extensions/EPbde2f7ca14e540399dcc1f8208860b7b/AppMeasurement.min.js .https://census.gov/[...i&/.....R.....*..b....O..$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):	5.7463666564000775
Encrypted:	false
SSDEEP:	6:m49Yk+f2pomX8N7yhmJ2+ugQXWSIrNentK6t:rl++amX8okJrC2M
MD5:	82A5E395402CFE5E1D956EA1B1033F44
SHA1:	063918F0BFE3DC74464C36C0B03FDB428589A4E6
SHA-256:	70C80CF89F646F5CD70AFE52A1E415F93059D6D91D72A9F5991B2219A6A30218
SHA-512:	68E3411AF4E4C56C63A714318C4B029AB84C392CE1D507D683866C015E85776B4F53753A9E0A03573A72B9419410D607D8C097747CCAA2BBABA04B8C82708F2F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\adf7722569fd0bc6_0	
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/..0.i&/.....xw.....7.6I.#....1.Y.z.....D6...#-Go...A..Eo.....A..Eo.....

Static File Info

No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/23/21-17:25:11.222519	TCP	2515	WEB-MISC PCT Client_Hello overflow attempt	49994	443	192.168.2.5	23.50.100.208

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 23, 2021 17:24:04.613157034 CEST	192.168.2.5	8.8.8.8	0x90e8	Standard query (0)	covid.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:04.616940022 CEST	192.168.2.5	8.8.8.8	0x14d7	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:04.619792938 CEST	192.168.2.5	8.8.8.8	0x5c85	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:05.150829077 CEST	192.168.2.5	8.8.8.8	0xb200	Standard query (0)	gov1.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:05.814764977 CEST	192.168.2.5	8.8.8.8	0x2653	Standard query (0)	uscensusbureaucovid.gov1.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:11.820945978 CEST	192.168.2.5	8.8.8.8	0x8e57	Standard query (0)	www.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:12.672265053 CEST	192.168.2.5	8.8.8.8	0xa71b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:12.672310114 CEST	192.168.2.5	8.8.8.8	0x7a52	Standard query (0)	assets.adobedtm.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:13.424407005 CEST	192.168.2.5	8.8.8.8	0x90d2	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.291460991 CEST	192.168.2.5	8.8.8.8	0xdca9	Standard query (0)	cm.everesttech.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.294248104 CEST	192.168.2.5	8.8.8.8	0x8b6b	Standard query (0)	uscensusbureau.demdex.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.466326952 CEST	192.168.2.5	8.8.8.8	0x7888	Standard query (0)	censusbureau.tt.omtrdc.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.660044909 CEST	192.168.2.5	8.8.8.8	0xf4b9	Standard query (0)	s.go-mpulse.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:17.419409990 CEST	192.168.2.5	8.8.8.8	0x8dad	Standard query (0)	c.go-mpulse.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:17.577023029 CEST	192.168.2.5	8.8.8.8	0xe8ca	Standard query (0)	dap.digitalgov.gov	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 23, 2021 17:24:17.780915976 CEST	192.168.2.5	8.8.8.8	0xdf51	Standard query (0)	censusbureau.d1.sc.omtrdc.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.172835112 CEST	192.168.2.5	8.8.8.8	0x26cb	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.367460012 CEST	192.168.2.5	8.8.8.8	0xf24d	Standard query (0)	www.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.684077024 CEST	192.168.2.5	8.8.8.8	0x10d	Standard query (0)	kqiticdijx3nayh234za-f-6bc069541-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:40.691433907 CEST	192.168.2.5	8.8.8.8	0x50c4	Standard query (0)	685d5b1b.akstat.io	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:41.302171946 CEST	192.168.2.5	8.8.8.8	0x611d	Standard query (0)	kqiticdijx3nayh2343q-f-afc6b30b3-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.119404078 CEST	192.168.2.5	8.8.8.8	0xc64c	Standard query (0)	data.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:48.109519005 CEST	192.168.2.5	8.8.8.8	0xd1c0	Standard query (0)	kqiticdijx3nayh2347a-f-0071a8c97-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:48.110733986 CEST	192.168.2.5	8.8.8.8	0x6f84	Standard query (0)	kqiticdijx3nayh2346a-f-6fe3f05b4-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:50.984380960 CEST	192.168.2.5	8.8.8.8	0x683a	Standard query (0)	kqiticdijx3nayh235aq-f-2cacd6b69-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:52.887387991 CEST	192.168.2.5	8.8.8.8	0xf130	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.327528954 CEST	192.168.2.5	8.8.8.8	0x2d29	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.002032042 CEST	192.168.2.5	8.8.8.8	0x292c	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.090568066 CEST	192.168.2.5	8.8.8.8	0x7b87	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.401209116 CEST	192.168.2.5	8.8.8.8	0x8d2f	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.401793957 CEST	192.168.2.5	8.8.8.8	0xab43	Standard query (0)	api.twitter.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.403609037 CEST	192.168.2.5	8.8.8.8	0xf8e8	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.466705084 CEST	192.168.2.5	8.8.8.8	0x8aee	Standard query (0)	video.twimg.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.468034029 CEST	192.168.2.5	8.8.8.8	0x8ff3	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.865344048 CEST	192.168.2.5	8.8.8.8	0x1c52	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:59.135149002 CEST	192.168.2.5	8.8.8.8	0x5317	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:59.726768970 CEST	192.168.2.5	8.8.8.8	0x8005	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:00.316745996 CEST	192.168.2.5	8.8.8.8	0xdc19	Standard query (0)	platform.linkedin.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:02.589318037 CEST	192.168.2.5	8.8.8.8	0x5756	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:10.872440100 CEST	192.168.2.5	8.8.8.8	0x2c36	Standard query (0)	gis.geo.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:11.153191090 CEST	192.168.2.5	8.8.8.8	0x51b6	Standard query (0)	server.arcgisonline.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:11.535604000 CEST	192.168.2.5	8.8.8.8	0x3810	Standard query (0)	kqiticdijx3nayh235kq-f-34ab7faf7-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:12.530859947 CEST	192.168.2.5	8.8.8.8	0x909b	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 17:24:04.646109104 CEST	8.8.8.8	192.168.2.5	0x90e8	No error (0)	covid.census.gov	uscensusbureaucovid.vanity6.gov1.qualtrics.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:04.646109104 CEST	8.8.8.8	192.168.2.5	0x90e8	No error (0)	uscensusbureaucovid.vanity6.gov1.qualtrics.com	akamaisecure6.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:04.647541046 CEST	8.8.8.8	192.168.2.5	0x5c85	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:04.647541046 CEST	8.8.8.8	192.168.2.5	0x5c85	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:04.653048038 CEST	8.8.8.8	192.168.2.5	0x14d7	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:05.203960896 CEST	8.8.8.8	192.168.2.5	0xb200	No error (0)	gov1.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:05.848104000 CEST	8.8.8.8	192.168.2.5	0x2653	No error (0)	uscensusbureaucovid.gov1.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:11.854140997 CEST	8.8.8.8	192.168.2.5	0x8e57	No error (0)	www.census.gov	www.census.gov.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:12.705307961 CEST	8.8.8.8	192.168.2.5	0xa71b	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:12.705611944 CEST	8.8.8.8	192.168.2.5	0x7a52	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	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 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	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 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	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 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	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 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	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 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	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 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	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 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	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 17:24:13.460427999 CEST	8.8.8.8	192.168.2.5	0x90d2	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 17:24:16.324340105 CEST	8.8.8.8	192.168.2.5	0xdca9	No error (0)	cm.everesttech.net	cm.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	No error (0)	uscensusbureau.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	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 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.18.85.49	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	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 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	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 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.49.107.116	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.19.195.165	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.203.33.226	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	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 17:24:16.329221010 CEST	8.8.8.8	192.168.2.5	0x8b6b	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 17:24:16.500988960 CEST	8.8.8.8	192.168.2.5	0x7888	No error (0)	censusbureau.tt.omtrdc.net		52.213.168.74	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.500988960 CEST	8.8.8.8	192.168.2.5	0x7888	No error (0)	censusbureau.tt.omtrdc.net		34.252.166.160	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.500988960 CEST	8.8.8.8	192.168.2.5	0x7888	No error (0)	censusbureau.tt.omtrdc.net		52.212.193.208	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.500988960 CEST	8.8.8.8	192.168.2.5	0x7888	No error (0)	censusbureau.tt.omtrdc.net		52.18.150.20	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.500988960 CEST	8.8.8.8	192.168.2.5	0x7888	No error (0)	censusbureau.tt.omtrdc.net		34.252.156.174	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.500988960 CEST	8.8.8.8	192.168.2.5	0x7888	No error (0)	censusbureau.tt.omtrdc.net		18.203.205.32	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.500988960 CEST	8.8.8.8	192.168.2.5	0x7888	No error (0)	censusbureau.tt.omtrdc.net		54.75.9.158	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.500988960 CEST	8.8.8.8	192.168.2.5	0x7888	No error (0)	censusbureau.tt.omtrdc.net		52.212.164.82	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.694881916 CEST	8.8.8.8	192.168.2.5	0xf4b9	No error (0)	s.go-mpulse.net	ip46.go-mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:17.453990936 CEST	8.8.8.8	192.168.2.5	0x8dad	No error (0)	c.go-mpulse.net	wildcard46.go-mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:17.612716913 CEST	8.8.8.8	192.168.2.5	0xe8ca	No error (0)	dap.digitalgov.gov	d27f3qgc9anoq2.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:17.612716913 CEST	8.8.8.8	192.168.2.5	0xe8ca	No error (0)	d27f3qgc9anoq2.cloudfront.net		52.222.174.63	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:17.612716913 CEST	8.8.8.8	192.168.2.5	0xe8ca	No error (0)	d27f3qgc9anoq2.cloudfront.net		52.222.174.129	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:17.612716913 CEST	8.8.8.8	192.168.2.5	0xe8ca	No error (0)	d27f3qgc9anoq2.cloudfront.net		52.222.174.90	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:17.612716913 CEST	8.8.8.8	192.168.2.5	0xe8ca	No error (0)	d27f3qgc9anoq2.cloudfront.net		52.222.174.50	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:17.814759016 CEST	8.8.8.8	192.168.2.5	0xdf51	No error (0)	censusbureau.d1.sc.omtrdc.net		15.236.176.210	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:17.814759016 CEST	8.8.8.8	192.168.2.5	0xdf51	No error (0)	censusbureau.d1.sc.omtrdc.net		15.188.95.229	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:17.814759016 CEST	8.8.8.8	192.168.2.5	0xdf51	No error (0)	censusbureau.d1.sc.omtrdc.net		13.36.218.177	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:17.985904932 CEST	8.8.8.8	192.168.2.5	0x9c88	No error (0)	www-google-analytics.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.208719969 CEST	8.8.8.8	192.168.2.5	0x26cb	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:18.208719969 CEST	8.8.8.8	192.168.2.5	0x26cb	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.420557976 CEST	8.8.8.8	192.168.2.5	0xf24d	No error (0)	www.census.gov	www.census.gov.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:36.729543924 CEST	8.8.8.8	192.168.2.5	0x10d	No error (0)	kqiticdijx3nayh234za-f-6bc069541-clientnsv4-s.akamaihd.net	kqiticdijx3nayh234za-f-6bc069541.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:36.729543924 CEST	8.8.8.8	192.168.2.5	0x10d	No error (0)	kqiticdijx3nayh234za-f-6bc069541.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:40.409307003 CEST	8.8.8.8	192.168.2.5	0x66f9	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:40.734852076 CEST	8.8.8.8	192.168.2.5	0x50c4	No error (0)	685d5b1b.akstat.io	wildcard46.akstat.io.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:41.352667093 CEST	8.8.8.8	192.168.2.5	0x611d	No error (0)	kqiticdijx3nayh2343q-f-afc6b30b3-clientnsv4-s.akamaihd.net	kqiticdijx3nayh2343q-f-afc6b30b3.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:41.352667093 CEST	8.8.8.8	192.168.2.5	0x611d	No error (0)	kqiticdijx3nayh2343q-f-afc6b30b3.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:46.391901970 CEST	8.8.8.8	192.168.2.5	0xc64c	No error (0)	data.census.gov	www.census.gov.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:48.155771971 CEST	8.8.8.8	192.168.2.5	0x6f84	No error (0)	kqiticdijx3nayh2346a-f-6fe3f05b4-clientnsv4-s.akamaihd.net	kqiticdijx3nayh2346a-f-6fe3f05b4.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:48.155771971 CEST	8.8.8.8	192.168.2.5	0x6f84	No error (0)	kqiticdijx3nayh2346a-f-6fe3f05b4.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:48.160103083 CEST	8.8.8.8	192.168.2.5	0xd1c0	No error (0)	kqiticdijx3nayh2347a-f-0071a8c97-clientnsv4-s.akamaihd.net	kqiticdijx3nayh2347a-f-0071a8c97.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:48.160103083 CEST	8.8.8.8	192.168.2.5	0xd1c0	No error (0)	kqiticdijx3nayh2347a-f-0071a8c97.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:51.031363964 CEST	8.8.8.8	192.168.2.5	0x683a	No error (0)	kqiticdijx3nayh235aq-f-2cacd6b69-clientnsv4-s.akamaihd.net	kqiticdijx3nayh235aq-f-2cacd6b69.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:51.031363964 CEST	8.8.8.8	192.168.2.5	0x683a	No error (0)	kqiticdijx3nayh235aq-f-2cacd6b69.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:52.920510054 CEST	8.8.8.8	192.168.2.5	0xf130	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:52.920510054 CEST	8.8.8.8	192.168.2.5	0xf130	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:53.355691910 CEST	8.8.8.8	192.168.2.5	0x2d29	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:53.355691910 CEST	8.8.8.8	192.168.2.5	0x2d29	No error (0)	scontent.xx.fbcdn.net		157.240.15.13	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.026993990 CEST	8.8.8.8	192.168.2.5	0x292c	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:57.026993990 CEST	8.8.8.8	192.168.2.5	0x292c	No error (0)	scontent.xx.fbcdn.net		157.240.15.13	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.116657972 CEST	8.8.8.8	192.168.2.5	0x7b87	No error (0)	twitter.com		104.244.42.65	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.116657972 CEST	8.8.8.8	192.168.2.5	0x7b87	No error (0)	twitter.com		104.244.42.129	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.428829908 CEST	8.8.8.8	192.168.2.5	0xab43	No error (0)	api.twitter.com	tpop-api.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:57.428829908 CEST	8.8.8.8	192.168.2.5	0xab43	No error (0)	tpop-api.twitter.com		104.244.42.194	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.428829908 CEST	8.8.8.8	192.168.2.5	0xab43	No error (0)	tpop-api.twitter.com		104.244.42.66	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.428829908 CEST	8.8.8.8	192.168.2.5	0xab43	No error (0)	tpop-api.twitter.com		104.244.42.130	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.428829908 CEST	8.8.8.8	192.168.2.5	0xab43	No error (0)	tpop-api.twitter.com		104.244.42.2	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.442637920 CEST	8.8.8.8	192.168.2.5	0xf8e8	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:57.442637920 CEST	8.8.8.8	192.168.2.5	0xf8e8	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:57.442637920 CEST	8.8.8.8	192.168.2.5	0xf8e8	No error (0)	cs2-wac-eu.8315.ecdns.net	cs672.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:57.442637920 CEST	8.8.8.8	192.168.2.5	0xf8e8	No error (0)	cs672.wac.edgecastcdn.net		192.229.233.50	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.442755938 CEST	8.8.8.8	192.168.2.5	0x8d2f	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:57.442755938 CEST	8.8.8.8	192.168.2.5	0x8d2f	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.496759892 CEST	8.8.8.8	192.168.2.5	0x8ff3	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.496759892 CEST	8.8.8.8	192.168.2.5	0x8ff3	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.496759892 CEST	8.8.8.8	192.168.2.5	0x8ff3	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.496759892 CEST	8.8.8.8	192.168.2.5	0x8ff3	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:57.506005049 CEST	8.8.8.8	192.168.2.5	0x8aee	No error (0)	video.twimg.com	cs296.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:57.506005049 CEST	8.8.8.8	192.168.2.5	0x8aee	No error (0)	cs296.wpc.edgecastcdn.net	cs2-wpc.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:57.506005049 CEST	8.8.8.8	192.168.2.5	0x8aee	No error (0)	cs2-wpc-eu.8315.ecdns.net	cs531.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:57.506005049 CEST	8.8.8.8	192.168.2.5	0x8aee	No error (0)	cs531.wpc.edgecastcdn.net		192.229.220.133	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.892380953 CEST	8.8.8.8	192.168.2.5	0x1c52	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:59.173685074 CEST	8.8.8.8	192.168.2.5	0x5317	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:59.173685074 CEST	8.8.8.8	192.168.2.5	0x5317	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:59.776206970 CEST	8.8.8.8	192.168.2.5	0x8005	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:59.776206970 CEST	8.8.8.8	192.168.2.5	0x8005	No error (0)	cs1404.wpc.epsiloncdn.net		152.199.21.118	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:00.351689100 CEST	8.8.8.8	192.168.2.5	0xdc19	No error (0)	platform.linkedin.com	2-01-2c3e-0055.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:02.625159025 CEST	8.8.8.8	192.168.2.5	0x5756	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:02.625159025 CEST	8.8.8.8	192.168.2.5	0x5756	No error (0)	cs1404.wpc.epsiloncdn.net		152.199.21.118	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:11.190120935 CEST	8.8.8.8	192.168.2.5	0x51b6	No error (0)	server.arcgisonline.com	wildcard.arcgisonline.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:11.549792051 CEST	8.8.8.8	192.168.2.5	0x2c36	No error (0)	gis.geo.census.gov		148.129.75.137	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:11.582524061 CEST	8.8.8.8	192.168.2.5	0x3810	No error (0)	kqiticdijx3nayh235kq-f-34ab7faf7-clientnsv4-s.akamaihd.net	kqiticdijx3nayh235kq-f-34ab7faf7.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:11.582524061 CEST	8.8.8.8	192.168.2.5	0x3810	No error (0)	kqiticdijx3nayh235kq-f-34ab7faf7.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:11.956362009 CEST	8.8.8.8	192.168.2.5	0xa7a0	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:11.956362009 CEST	8.8.8.8	192.168.2.5	0xa7a0	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:12.564563990 CEST	8.8.8.8	192.168.2.5	0x909b	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

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 17:24:13.612317085 CEST	63.32.159.255	443	192.168.2.5	49739	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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 17:24:16.665019989 CEST	52.18.85.49	443	192.168.2.5	49746	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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 17:24:16.728564978 CEST	52.213.168.74	443	192.168.2.5	49747	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 17:24:57.154772997 CEST	104.244.42.65	443	192.168.2.5	49915	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		

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 17:24:57.155462027 CEST	104.244.42.65	443	192.168.2.5	49916	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 17:24:57.366478920 CEST	157.240.15.13	443	192.168.2.5	49914	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 17:24:57.467660904 CEST	104.244.42.194	443	192.168.2.5	49917	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 17:24:57.536668062 CEST	104.244.42.69	443	192.168.2.5	49926	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 17:24:58.493710995 CEST	104.244.42.194	443	192.168.2.5	49932	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 17:24:59.210381031 CEST	152.199.21.141	443	192.168.2.5	49942	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 17:25:02.666682005 CEST	152.199.21.118	443	192.168.2.5	49973	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 17:25:06.654557943 CEST	152.199.21.141	443	192.168.2.5	49977	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 17:25:11.885271072 CEST	148.129.75.137	443	192.168.2.5	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 17:25:11.940957069 CEST	148.129.75.137	443	192.168.2.5	50003	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: 6016 Parent PID: 3896

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' --start-maximized --enable-automation 'https://covid.census.gov/jfe/form/SV_3en1hX9u1RWIp38?Q_DL=SqN0lR2ri39yTOI_3en1hX9u1RWIp38_CGC_daprBTqzoTB4ekC&Q_CHL=email'
Imagebase:	0x7ff677c70000
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: 5156 Parent PID: 6016

General

Start time:	17:24:00
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=1616,5429937548656341176,3177274583310322343,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /prefetch:8
Imagebase:	0x7ff677c70000
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