ID: 433107
Cookbook: browseurl.jbs
Time: 10:20:51
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

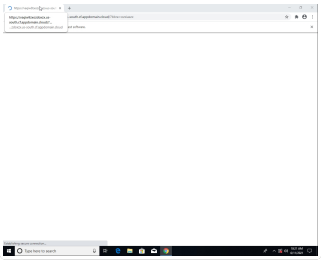
Analysis Report https://vaqiw9zxozdoxzx.us-south.cf.ap…

Overview

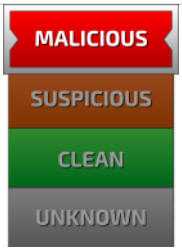
General Information

Sample URL:	http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx
Analysis ID:	433107
Infos:	

Most interesting Screenshot:



Detection



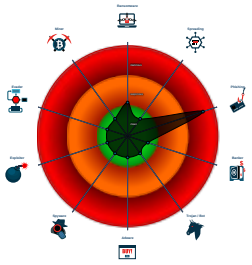
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish29
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4080 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5036 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1508,3517359519867941500,577729940254380 33,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1956 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish29

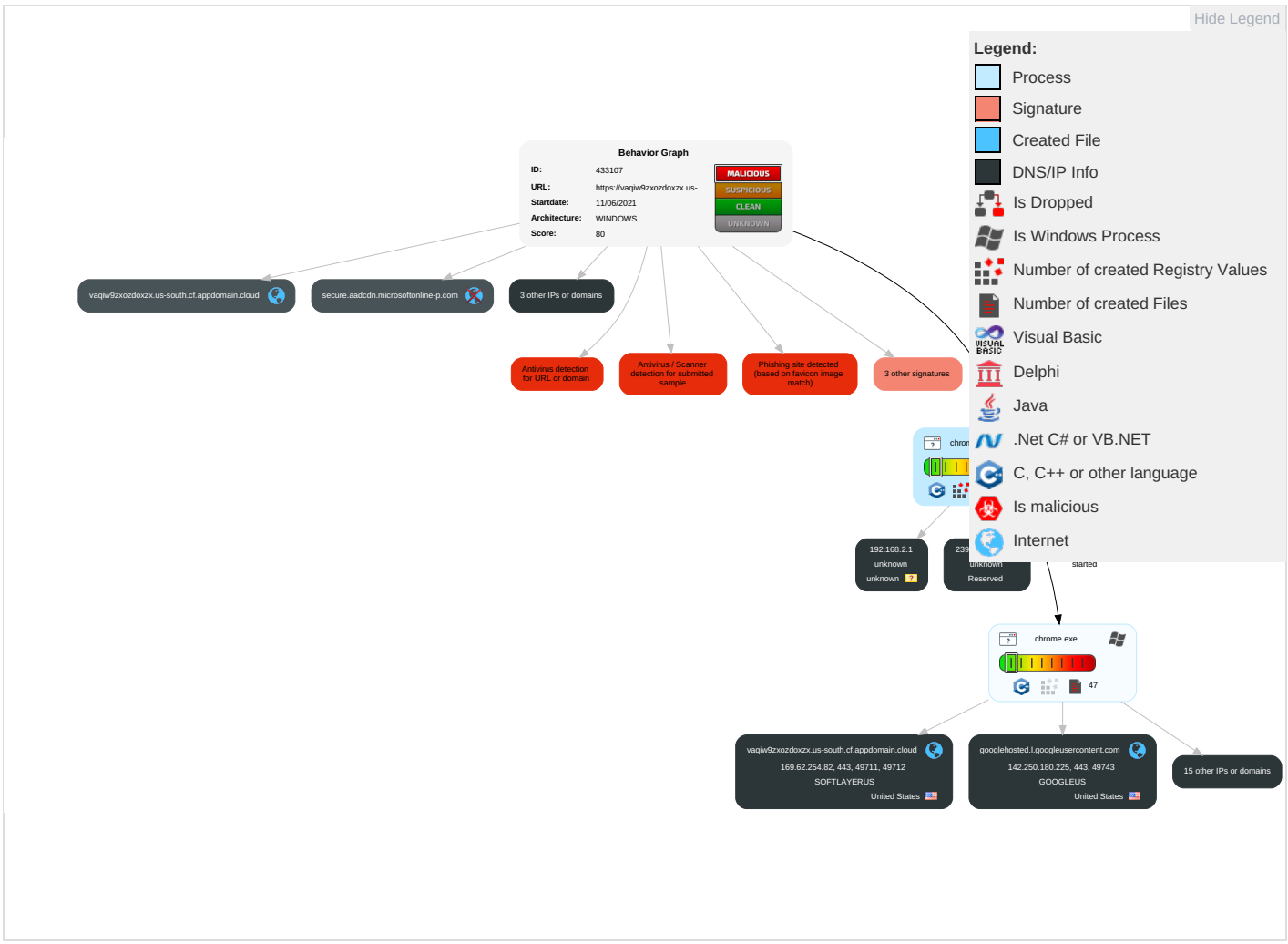
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

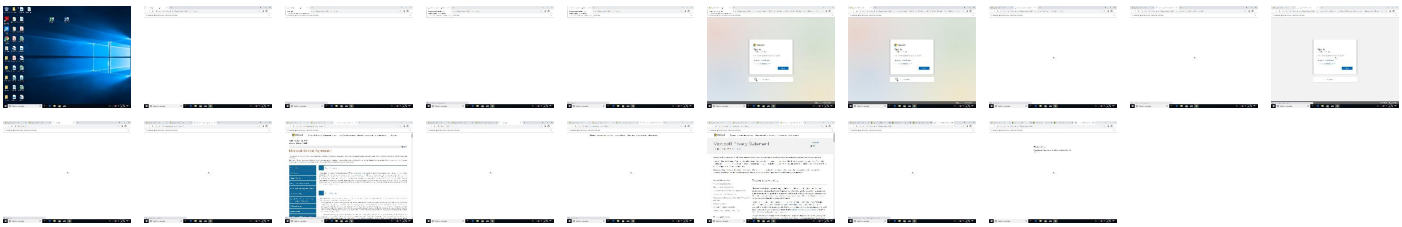
Behavior Graph

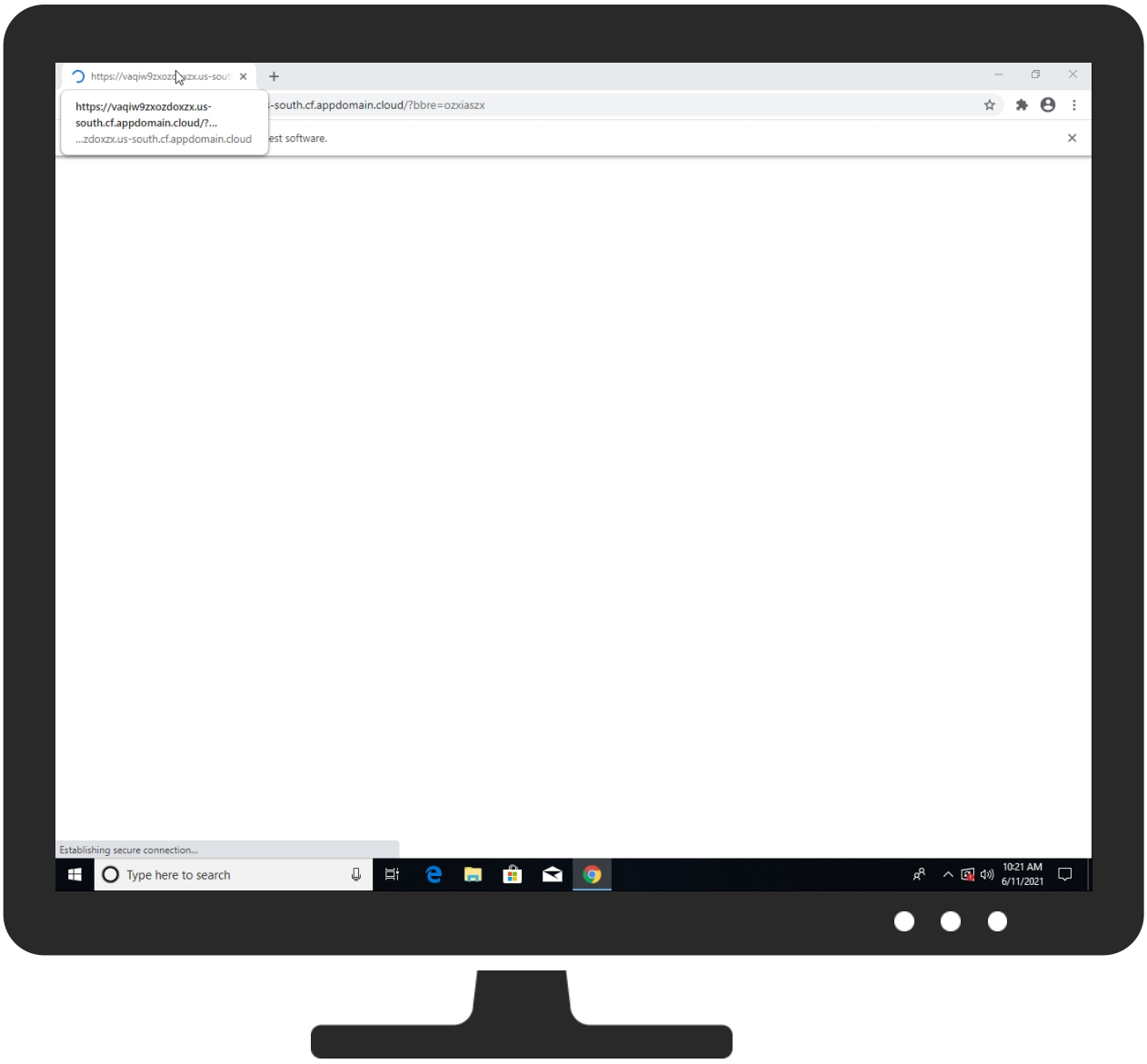


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx	0%	Virustotal		Browse
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
kifot.wancdnapp.page	0%	Virustotal		Browse
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
rikapcndbn.web.app	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/PpDUsrjn8IGBCAWytdv3ZxgET4	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/qjdgg12br68IWOAkxTFcUxNDjkK6vBXSQ14pglY-&!@ctNM8sAjZgEY5iLDn&!@bwModtqTQyV7pa0@&!-ysuJLX45IcP0KLhIxaQPE5U90CLI1XE3DDln3bffxyMcTU1SyZK8PyfndC0RXZuanMqxQ4unXZabg6dtpeTkxklXIRj1ItG-0SHYRldblkAj3Lq3FEirUZzFzqQo0mGQ4LAdWTMNAq0TWpgNOfeO6jrvgbbfZEa4YxTZTkDPRG/SFrnl6ZCu24tlNocmqA4ydRLNOJODPp218CSkziHWcwZALwBsLu1L1FctqkVigXJkj	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://appdomain.cloud/l.	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud	0%	Avira URL Cloud	safe	
http://https://rikapcndbn.web.app/ahygdvxzsa/themes/96cf99fc63f83319d09ad083f8a504cb.js	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx:x/&	0%	Avira URL Cloud	safe	
http://https://rikapcndbn.web.app	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/j	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/2	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/Sign	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszxSign	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/G	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/x0Lh7w4dQKuJ3sfdB8g-&	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico:x.m	0%	Avira URL Cloud	safe	
http://https://rikapcndbn.web.app/ahygdvxzsa/themes/17034c4caccdac15190faf36c3557a3dnbr1622646221.js	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud//#	0%	Avira URL Cloud	safe	
http://https://rikapcndbn.web.app/ahygdvxzsa/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301622646214.js	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszxxgu	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx:x/	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#PpDUsrjn8IGBCAWytdv3ZxgET4/#	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#PpDUsrjn8IGBCAWytdv3ZxgET4c	0%	Avira URL Cloud	safe	
http://https://kifot.wancdnapp.page/60b79dd6cc1251248c7a9396.js	100%	Avira URL Cloud	phishing	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszxy	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/qjdgg12br68IWOAkxTFcUxNDjkK6vBXS	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#PpDUsrjn8IGBCAWytdv3ZxgET4Sign	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/a~$	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.icoy	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx2	0%	Avira URL Cloud	safe	
http://https://rikapcndbn.web.app/ahygdvxzsa/themes/js/c0f5e0dd4f642062f92481ef2bb438191622646215.js	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/PpDUsrjn8IGBCAWytdv3ZxgET4Sign	0%	Avira URL Cloud	safe	
http://https://rikapcndbn.web.app/ahygdvxzsa/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301622646214.jsaD	0%	Avira URL Cloud	safe	
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#PpDUsrjn8IGBCAWytdv3ZxgET4	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://appdomain.cloud/N	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/K	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#PpDUsrjn8IGBCAWytdv3ZxgET4$&	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud	169.62.254.82	true	false		unknown
kifot.wancdnapp.page	104.21.47.62	true	false	• 0%, Virustotal, Browse	unknown
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
bit.ly	67.199.248.10	true	false		high
rikapcndbn.web.app	151.101.1.195	true	false	• 0%, Virustotal, Browse	unknown
unpkg.com	104.16.122.175	true	false		high
googlehosted.l.googleusercontent.com	142.250.180.225	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
aadcdn.msftauth.net	unknown	unknown	false		unknown
aadcdn.msauth.net	unknown	unknown	false		unknown
assets.onestore.ms	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/PpDUsrjn8IGBCAWytdv3ZxgET4	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#/qjdgg12br68IWOAkxTFcUxNDjkK6vBXSQ14pglY-&!@ctNM8sAjZgEY5iLDn&!@bwModtqTQyV7pa0@&!-ysuJLX45IcP0KLhIxaQPE5U90CLI1XE3DDln3bffxyMcTU1SyZK8PyfndC0RXZuanMqxQ4unXZabg6dtpeTkxklXIRj1ItG-0SHYRldblkAj3Lq3FEirUZzFzqQo0mGQ4LAdWTMNAq0TWpgNOfeO6jrvgbbfZEa4YxTZTkDPRG/SFrnl6ZCu24tlNocmqA4ydRLNOJODPp218CSkziHWcwZALwBsLu1L1FctqkVigXJkj	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/	true		unknown
http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.122.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false
142.250.180.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
151.101.1.195	rikapcndbn.web.app	United States		54113	FASTLYUS	false
67.199.248.10	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
169.62.254.82	vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud	United States		36351	SOFTLAYERUS	false
104.21.47.62	kifot.wancdnapp.page	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433107
Start date:	11.06.2021
Start time:	10:20:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx
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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.phis.win@41/257@16/11
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx#PpDUsrjn8IGBCAWytdv3ZxgET4 • Browse: https://bit.ly/39oebGZ • Browse: https://bit.ly/2Jmn3lA • Browse: https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:22:01	API Interceptor	2x 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 GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5887976EDAA817EEF5159B09F6FCD000_35673150FB44DAA99337A19E2291E035	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.114664147004366
Encrypted:	false
SSDEEP:	12:JKtfIt5BWm+fgZq8Gmg7aZ+hSes7Ae8eR2S5:JioS/182I+kHR2S5
MD5:	A9E22CBE31893BCEEBB03B729F35273D
SHA1:	7EF1F664A2771B9EF594FF25D36827B38A991D80
SHA-256:	5982F832A9F639582F02911390593D017D76ADAB10C44091D4127C7499568421
SHA-512:	F288FA59A260A2A790714735DEA6922B86D836893021B3A00DFFBA179BB369B358BEC770349CCA91E754287000E4D665583CB5470E1E6F1F81EA63F8A93EBC9F
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....=.P.....J`.e.!.....20210610211247Z0s0q0l0...+.....l.....v....@-h;qj....=.P.....J`.e.!.....s.Co.sz.\M..o....20210610205701Z....20210617201201Z0...*.H.....].._.(j1....gM...1D....S.2..y{Aq...\.X..vl.....kPrb.t.s...}.>...S..OZe..ACq....x..0..GE.f`O..YXS_...B.....~$ M..v..z.rH...n.>..E.X.=..z.l.@.....$.i..M.Y.Id...^xs$.*p..3.m\X[...QL..o.....o..E;..*.I....}..D./.T.....v."...~9A.E#.}.$...TP.L.>Z#

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
Size (bytes):	471
Entropy (8bit):	7.1947173395046935
Encrypted:	false
SSDEEP:	12:JY035FZJ9VQEc+VjeYMp4OkF0oMiusrAC/:JY033ZVQEFVVOosK/
MD5:	EB0C469CBC4EEBD58F2538ECF8EEA03C
SHA1:	6362CBB2AD3A2900E775B5B147AA702E5DBC6A57
SHA-256:	969F3CF553E8B94BC6ABE251CD0F5C56FDD268F092B5B038B5638B5A89383963
SHA-512:	B5B605A0C6AB08FDAB4DCA48194E70271ABB8DB06900141034201EF60726004EC8251A6512A4AE28D01F275A4685A877DB5029D7380DE0E397ADD910A99E452E
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....>.i...G..&....cd+...20210610215359Z0s0q0I0...+.....(..A..B..G@B.X....>.i...G..&....cd+....y.D.... .a_.k.....202106102153 59Z....20210617215359Z0...*.H.....P..j.5r._-.W.).....<....#..+.14..{s..... "..fw3.D..q.[..{An..yF#`.a....."A..q...B....T.[.G.Nz.{z.~paZ1[)P.....z/....[.q.=...._.....y...I...X....g..AW?..>E...0.0..?..&}..Q..c.pl/...q..CG..N/..-.....%dI...v...+...)Kba.....|U.. .Q..G.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5887976EDAA817EEF5159B09F6FCD000_35673150FB44DAA99337A19E2291E035	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.8579970764071456
Encrypted:	false
SSDEEP:	12:SbmxMiv8sFq3lCvM710Bf2QeDjBbmxMiv8sFq3lCvM710Bf2QeDi:SbmxxvM4vw1AoFbmxxvM4vw1Aoi
MD5:	4CBA7A8FC5F91B44AA2A1BABB0AEE79C
SHA1:	7928E2AC04FF41C3384F4729515C81EEAFA31098
SHA-256:	2E5FE70855B0717AC6AE9404C4A59396492EC9BEA173E6D70C85A3C4B7DA426C
SHA-512:	3547292CF79E4CE1D2CC0E1AD1D36DA0A3E2489B4725B56C4DAF37A38FE72159F5EED63F8EACFFA1FEB77BDA75C9D600A6E500B13C99F99CB70693368A595203
Malicious:	false
Reputation:	low
Preview:	p..... .....^J.^..(..... .....\=^.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M .C.G.g.U.A.B.B.R.J.9.L.2.K.G.L.9.2.B.p.j.F.3.k.A.t.a.D.t.x.a.u.T.m.h.g.Q.U.P.d.N.Q.p.d.a.g.r.e.7.z.S.m.A.K.Z.d.M.h.1.P.j.4.1.g.8.C.E.A.q.N.7.H.P.i.Q.2.%.2.F.4.c.3.r.d.X.E .3.u.H.G.8.%.3.D...".6.0.c.2.8.0.4.f.-.1.d.7."...p..... .....^J.^..(.....(;^....I..c.....I..c.. .....\=^.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w .T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.R.J.9.L.2.K.G.L.9.2.B.p.j.F.3.k.A.t.a.D.t.x.a.u.T.m.h.g.Q.U.P.d.N.Q.p.d.a.g.r.e.7.z.S.m.A.K.Z.d.M.h.1.P.j.4.1.g.8.C.E .A.q.N.7.H.P.i.Q.2.%.2.F.4.c.3.r.d.X.E.3.u.H.G.8.%.3.D...".6.0.c.2.8.0.4.f.-.1.d.7."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.819322841027361
Encrypted:	false
SSDEEP:	12:fPbmxMiv8sF1JbqDkwJr0yrkIbmxMiv8sF1JbqDkwJr0yrC:LmxxvnFqYwJhmxxvnFqYwJi
MD5:	D642135A80A9635CF341A671A798E977
SHA1:	FCA01E9E41688BD2A97381F4771460C9969F19CB
SHA-256:	58488CBAE8D3E7F65B8A7860FE4381FB944CECAD789A0B9965A33F04D38A4AB6
SHA-512:	5803E6E77206319FC54341E50873A68F264A7DA2AEE9256AD7606F4C9A05103371020FF74B97EBCB61226B4D17D7BA23CC3BF074EB9ED6F8EF147F629CD9E378
Malicious:	false
Reputation:	low
Preview:	p..... .....OJ.^..(..... .....p[W^..oJ.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g. M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.x.5.q.U.S.w.j.B.G.V.I.J.J.h.X.%.2. B.J.r.H.Y.M.%.3.D...".6.0.c.2.a.b.e.c.-.1.d.7."...p..... .....OJ.^..(.....5..C^...u.F.c.....u.F.c.. .....p[W^..oJ.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c. o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G. g.g.C.7.2.N.k.K.8.M.C.E.A.x.5.q.U.S.w.j.B.G.V.I.J.J.h.X.%.2.B.J.r.H.Y.M.%.3.D...".6.0.c.2.a.b.e.c.-.1.d.7."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\005f033d-7fa8-4056-b6f6-9ce72d9ac0bf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7505706786351767
Encrypted:	false
SSDEEP:	384:lHHAoCVrSBeIVtP0LNIrBvEg37I6THOHGvyr9iEixr2q+drZEm9qxy4w07OqeYNQ:pqOJ5mibnkeXuwaYvHy0KmIwto
MD5:	B182AC99E60AFE9CE68AB2F064AC3A40

C:\Users\user\AppData\Local\Google\Chrome\User Data\005f033d-7fa8-4056-b6f6-9ce72d9ac0bf.tmp	
SHA1:	5786E9EBA61955F5419A858808BFEDCF13E739F1
SHA-256:	CDDD9157226EF3DCD2DD215A90C0377C1B66861E212B3A88C3CCAC17ADFFC631
SHA-512:	7587DA6F6A3675B65D43649B4258B4B07A098291AC9CA61C633DBAA511060974BE88FD5FF4EB8FEB1671CE88662648FD2B5315BB4F6D9A423B79848B3DA8591
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\5d149a2a-d9ad-47a6-827b-fab45036f556.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):	172394
Entropy (8bit):	6.080006049873029
Encrypted:	false
SSDEEP:	3072:FxydLgVDqfsAtDzQFU36fdYPL8JPbFcbXafIB0u1GOJmA3iuRz:fKgIRXv6fWPL8VZaqfIlUOoSiuRz
MD5:	D539A6B94FC06D1A723D95895EC7BCFC
SHA1:	3CB340842808677B2E6C770D992D06879998A7BC
SHA-256:	B1120761BD2D1B5E8BD82E8C849BD1063492B0B3EE1FBCDF627E6C7D660A92DF
SHA-512:	9366DB77EFD43240FE5CB805D36C200B398AFFCFF5EA954D2FD6A0C4F3FD4E8277FC5A73D9BC4727D45681C4BA6B90F596D116B1B6ACF97D569943A5AF5D7E 7
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":1.623432104421123e+12,"network":1.623399706e+12,"ticks":99407339.0,"uncertainty":4562887.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\847fb939-b0cb-4d68-886b-d20708c15355.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.750009788597753
Encrypted:	false
SSDEEP:	384:LHHAoCVrueZ0LNIrBvEg37I6THOHGvyr9iEixr2q+drZEm9qxy4w07OqeYN114BJ:5OJ5mibnkeXuwaYvHy0KmIwtA
MD5:	BCB8322D04C486E85ACBAD30C1C530F7
SHA1:	19CAF82ECF683CC9B734FCD01118195C138E2F27
SHA-256:	C5376C0C8E462E00A198A40FF37560F0FAE5EDF04051F470F63D6BC45F20E7D0
SHA-512:	1719AC58F30A51AEB5C17938AA6488D43BEE168DCEB743EEB7CCB5ED906E02FA2AD4176A77E177AE855E11725F9815FD7E15C9A5A191507D82AA00E302EEC3C3
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\8a562679-66f1-4ad0-b46c-680a5936f723.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	95428
Entropy (8bit):	3.7503448996727493
Encrypted:	false
SSDEEP:	384:VHHAoCVrSBeIVtP0LNIrBvEg37I6THOHGvyr9iEixr2q+drZEm9xrxy4w07OqeYw:5qOJ5miInkeXuwaYvHy0KmIwtG
MD5:	10FA75F01AF5D1B72A5670A5975711EF
SHA1:	C358F4838770FA4C1F5228D9BEF57F4AA6D903C4

C:\Users\user\AppData\Local\Google\Chrome\User Data\8a562679-66f1-4ad0-b46c-680a5936f723.tmp	
SHA-256:	F43437E087D0CA1CDD03500FE8F7BC95B38ED083A4CF693F5A1963A9DF5F3F6E
SHA-512:	61F98298640673155406 7ABDF210188626C476B548A1BE8395EB0A918D190876875FAF6C886EE04BC417A57E08BBC179429979BD75478C238357545F4D435B2F
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\90e06b9a-3f9a-4d88-aca8-feb7e971ef33.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):	172395
Entropy (8bit):	6.080007835763176
Encrypted:	false
SSDEEP:	3072:KgwdLgVDqfsAtDzQFU36fdYPL8JPbFcbXafIB0u1GOJmA3iuRz:pEgIRXv6fWPL8VZaqfIlUOoSiuRz
MD5:	00131D1F3CDD0E727167C73EF8D91F96
SHA1:	0F8A5EEEDE4A8BB2B4D1CE94D000A9632CDF159E
SHA-256:	1D5D36C5F5BB9B3FA887108480D7C5BCD0B9471104AC6D6B619194A299BC2B67
SHA-512:	A1CECD9BFC85905D093A880722EE9EF965D92DE514F6AE41474C1D19AF9D64731193494C18B7663A67C659CD1D51268136B2DD66AA27AC52905F100C1FE4325
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":1.623432104421123e+12,"network":1.623399706e+12,"ticks":99407339.0,"uncertainty":4562887.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016520807"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0c85b975-e0fa-4076-a08f-51aa0bf79f2d.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):	5.5362810302686105
Encrypted:	false
SSDEEP:	384:cVatqLlhTXT1kXqKf/pUZNCgVLH2HfD1rUmzUHGzTnTuU4sgam4e:iLlpT1kXqKf/pUZNCgVLH2HfxrUm8GX2
MD5:	79F43B65DF5BCEF2AD6CFF1B71898089
SHA1:	DFBD341E1EBDE9BD5263D38C96A5BF555F9ECB6E
SHA-256:	1891DED35FCDA9F402E9B9A6EF24CAF6DDF87CE2483AC7B6DAEC036D0BFE472C
SHA-512:	0CB591F38CF6592CF0ADCE6AFAD8AE4CBE3A61FC4CAC91398E8F97DCE18DC44E39343D4429623BDB4AD2E7D98B5B7EF24898659B665C09771BFF5C7E212FB68
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0c85b975-e0fa-4076-a08f-51aa0bf79f2d.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13267905701478630","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\10692dd9-eaa1-48a3-9583-e7fe66d5208c.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):	19007
Entropy (8bit):	5.567356529675862
Encrypted:	false
SSDEEP:	384:cVat3LlhTXT1kXqKf/pUZNCgVLH2HfD1rUxUHGusdm4P:PLlpT1kXqKf/pUZNCgVLH2HfxrU+GuWB
MD5:	9B583243546D527CD323635C6FEED623
SHA1:	248B9604DACD7D0E4AA3AA9FB232562C9B11660F
SHA-256:	71D6A69356586D8341804F5D6B06625A803FB4D8C673A8E20C6136ECEF42E648
SHA-512:	197FC8C14B4791012910D1A56A8FCB284DD62CE15A7CC358A1623CA5AEC8A430681A5B8EC64B44B2FE40C81BF7C6669995F5ADBDC41E5600696AC5A707DEC83
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13267905701478630","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2422099a-e303-431b-adb8-aa2fc191bcaa.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):	24055
Entropy (8bit):	5.534019128124798
Encrypted:	false
SSDEEP:	384:cVatqLlhTXT1kXqKf/pUZNCgVLH2HfD1rUEHGAUHG5TnTuU4s6vm4k:iLlpT1kXqKf/pUZNCgVLH2HfxrUIGDGL
MD5:	84AF48CE78A14C6302C2054725A8625D
SHA1:	4AA35C172E906954370C721F4F250F88C0ABD014
SHA-256:	F4C5D2C2015095361ADBEFBE3922BB8C705CF410F964705FA895E743AE2A680F
SHA-512:	0184CF4B7EA8468EEC8C16FD2FC98FB4817687A78DA8EEC1C4F62450B5F5AC49F861E3D09E9114FA025B70E92D151293E4AA02EC479E78E1CDDD89FFA2AC3F06
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13267905701478630","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2da71a3d-c92b-48c6-b624-67ba1e492584.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):	3560
Entropy (8bit):	4.866592958270876
Encrypted:	false
SSDEEP:	96:JTnOCXGDHzwF4zgtPrO6NOdo5gjFV0Fi+UVmLmVeVjEGshH:JTnOCXGDHzwFAgtPrO6N+o2j30FTaa4n
MD5:	430C51A411DEEC2BA08A6198E708789D
SHA1:	19F7228F74406D2C17DD78C3081D97D99E314158
SHA-256:	0E244327C0FCF993E60069472DAC851C573EEB78975A5CEA15CBF98DA52793F7
SHA-512:	1111555F56FDEE1DA491FDA9D004B96D858FBA6EE7E3149A63409D2D923E949CC2A31967D4E603F9331DFF4D31992793DE6B88C763D0232C097833B2F53C9F75
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2da71a3d-c92b-48c6-b624-67ba1e492584.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270497704302018","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270497704318548","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","suppo

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\667cb605-3081-42ff-8910-4a7fed0a53d7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\73c849b0-9b0f-48d4-a2d6-0aa7587498ea.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):	5792
Entropy (8bit):	5.189280811496716
Encrypted:	false
SSDEEP:	96:neC+GC2Rv2s8GcVTok0JCKL8j5Mk51rbOTQVuwn:neCC2ReRGc84K85Mk59
MD5:	73A09AE67549719E3BAEB5EF5DD86A2A
SHA1:	704B90A2A46C837C92572456E7B1349E6AF08E5B
SHA-256:	CE2FDE7D75391E6481DF8B8ECD91BA5FA7561E081152CAC85627CCCBB8B27CE9
SHA-512:	7F2D7F2CA4404B3123D737BA8D99D4FF1AB9521D9EC03212D2FF541DEA61FB3E5F221775938075FBB3BE78C4CB195A884D71FBE2EBE2C29621CE03E321B1DD9
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267905701763236","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7d47f57b-5ea1-4bd8-9923-4a8213d326d1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1708
Entropy (8bit):	5.574082766021675
Encrypted:	false
SSDEEP:	48:Y5VwUuI6UUhLUeseKUewqPeUer2UefjbwU0wUFJU68Uenw:5UuBUUdUe3KUGPeU9UEjkUZUrU68UD
MD5:	0CBCC195819B1F641849FD965F992609
SHA1:	5E3BDE47F93B2D6A04FFA95CD998DD2221533583
SHA-256:	43490BC5FB0CEADBA8565AEFD01CD36D55799DADD6B0E2F63E65DE2F1DA7804E
SHA-512:	A19C4D4D237FB1089B97F37DD4B7B187497B394F10BE011B2FA37DD0F2339B39ACD743A69AED21986697B5894ABE155E9170CC46FD67188202EE3106D19BB4C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7d47f57b-5ea1-4bd8-9923-4a8213d326d1.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1639212108.592752,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623432108.592755},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1654968108.41168,"host":"e3SziuwfuO2UvuBno+qkR1ObHAzZmSUoJhrc7dbP1Uo=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623432108.411684},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.192952408390994
Encrypted:	false
SSDEEP:	6:mwGaH+q2PWXp+N23iKKdK9RXXTZIFUtpDGadZmwPDGaVU3NVkwOWXp+N23iKKdKT:aaeva5Kk7XT2FUtpKad/PKaaz5f5Kk73
MD5:	93398632F5C58FA955EB29501B9A94D9
SHA1:	B3F49353D3DDFBD888319A51802C4318A515144F
SHA-256:	7D521C4116C0BCB1A036546341FE5D83D1FD95F75AFC99AFC2C8E385D48BB599
SHA-512:	1B8FC0C16FDDD61E38E9C028E578DFD9EEF4E5F269C38A9AF8FFDA7499BCB23392563B93930F43CD23F3E4CBB2F01213C8437D487E54E56EB23B84E8941294D2
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:51.365 1af8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/06/11-10:21:51.367 1af8 Recovering log #3.2021/06/11-10:21:51.371 1af8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.186174694400208
Encrypted:	false
SSDEEP:	6:mwGaXQd+q2PWXp+N23iKKdKyDZIFUtpDGaXSpZmwPDGaXSdVkwOWXp+N23iKKdKy:aaXQYva5Kk02FUtpKaXi/PKaXO5f5Kky
MD5:	C1D6F658D9ED6D604F9546196B6123FD
SHA1:	965BB9DA7253A570352D94466AE7B8A96C156622
SHA-256:	F46CD800D9C78809BCDDDB6556237540F55EA6059EA779A3EEF202EDB85EB43B
SHA-512:	D16E95344E1717081BB436BB9E29C787FD23AD15EFFB553CB656ED445299B3CC52475530C42A36475C6137E6337FA31A1371D87AE2AAE76C2535064B70363A1C
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:51.355 1af8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/11-10:21:51.357 1af8 Recovering log #3.2021/06/11-10:21:51.357 1af8 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\094e2d6bf2abec98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.583736491268686
Encrypted:	false
SSDEEP:	3:m+lP9Ola8RzYJb9yKIf8QPKxWStHWFvDFYtR72GelHCgs/lxl58tyGdDmQXlpK5M:m3VYyK08fNH1DDgSyL6KK6t
MD5:	3A49CEA667AE83FE2C8E8245A4FC8F73
SHA1:	8F0316E56379E7A12AD619EFCC3D8C9D42ADF22B
SHA-256:	4ED46194FE244E2B95D290A9C149AEC06A751A0A77A4168457F2683B98522556
SHA-512:	C8860BE933CC29A95CCD04AE638EC22806D38E466CF9B773DC0FA5D7628EFEE1C28FBAED2F42BD4A6223F5D494ECA588D1C64508B9496C9F97A58F376B6CC03
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js .https://microsoft.com/...../#/.....=.z-.7.K]..~..=..9.....8...A..Eo.....X?.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1090860740f0bc96_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1090860740f0bc96_0	
File Type:	data
Category:	dropped
Size (bytes):	14147
Entropy (8bit):	5.707488300050843
Encrypted:	false
SSDEEP:	192:v0B5rgSGJEAKTYK0N5BNVKGNqkE1iKyLuVSprIY7QJx+M3YO:MrsH3/N/NbOkVS40Y7QJBYO
MD5:	C0266161260F1FB994E1FB3A1B4D504D
SHA1:	792D9300E22A8665208FA629BCD60405E9AAF8E6
SHA-256:	19195C192D0323711A062AA1340B5A1D51014DA4A6B411995BC86A5FBD2F5458
SHA-512:	5793A2A0742890A7E7FF66977B17B7753853A7F452E317A51C67BF3330BA49D577D6B7A3CADBF5F00296AAD6992646638F179B763AA71B36F66C87DB35C0C274
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c.....n...._keyhttps://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js .https://appdomain.cloud/.(...#/.....gZHD'.J.....\D*.T.K...B..vp....A..Eo....U.....A..Eo.....'..7....O.....5..(.....(S.<..`4.....L`.....(S.I.`.....L`.....Q.@.....exports...Q.@.....module....Q.@.....define....Qb.Q.W....amd...Q.@..u.....VueI18n...K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.].....\..&.-...%....(Rc.....I`....Da.....e.....`...p...@.....@.-....TP.A...E...https://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js...a.....D`....D`2...D`.....`....&...&....&.(S.m..`.....9.L`.....i.Rc.....P.....Qb.].....t.....Qb.....e..Qb...]....r.....Qb.*.s....n.....S...Qb...:....o.....M...Qb.....s.....Qb...^....l.....QbRc.....c....R....QbZ..-....f.....QbjG.....h.....Qb..[.....p.....QbF..-...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\15bbcddad0bfbf89_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.903078031975226
Encrypted:	false
SSDEEP:	6:m8+VYSHT8NWQA8SSNkVjjW/G1BC338m4gK6tNj0o9NEKc3RTurUG1BC338m4E:K7z8NWQ93NuQGm338CfIzUQGm338E
MD5:	C455D2243FA161F02E789E1E126F44F1
SHA1:	BDDF0F7C7EEE3936DED20739531AC168E58D38F7
SHA-256:	CE20C09628F8C665DD602BDC25C2E596D29A1AC37E34A940648B2FA790650976
SHA-512:	B32CE958BC152DA43F91A4F9AFBB44B1C08EC6DAE67EA16BA0753EB689D5100956D3803F8FEFA004155FDD4ED404D9F1F159E679936CE46AABF899097DEB02A0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^...%26C...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js .https://appdomain.cloud/.....#/.....!RV...u.^~;.....sc..:5.c..A..Eo.....e..s.....A..Eo.....#/..x..6428D88CAD211309052E7F07CD235DC13FD1C65FC75D9A4D31AFB7E26469BA7B...!RV...u.^~;.....sc..:5.c..A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\16c3089330ff7ee0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	255
Entropy (8bit):	5.718093917793761
Encrypted:	false
SSDEEP:	6:mzXYacBT2fb0lnD+79XxWbKzWdSZdyOMWZVT8m4O/ZK6t:uUBT241D+79v7Hwc98mpr
MD5:	48C18D7D2A4399AFF6072F223DE4879B
SHA1:	16E085B0DD915FB4AF749EB4F95C65B04B19363D
SHA-256:	A1129F6661A6435738678413D5ABBEE52C42FF07DD0611BD4F05623D6884F5E3
SHA-512:	D66261A4B01CC99AD69357B9700BE85361F2DC0CA868422D7745F1DD1F947716473F364012CFD9D9289DF7E88C55267EDEA294BF0D3007117D6A69DC9C48B95
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{...JXy....._keyhttps://rikapcndbn.web.app/ahygdvxzsa/themes/js/c0f5e0dd4f642062f92481ef2bb438191622646215.js .https://appdomain.cloud/N.)..#/.....A.....#>X)...|.pE7..G...yQ...N...^KH;1.A..Eo.....I{.n.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e2f53894c97faa5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.734482696531105
Encrypted:	false
SSDEEP:	12:XKEBT24vxVVFUnLN+p9KEBT24vxVVNuzNQT:JV7Venx+pnV7VNuJQT
MD5:	203CAFBC7A7A6DEBC4EC0A7D827F5949
SHA1:	22A2BBAF45F1AD9D371E83693C6747DDF056482F
SHA-256:	7A9C1B6C03518D456A3D86426A395CB99AFDE18533FFDB572300FFC4D7F85177

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e2f53894c97faa5_0	
SHA-512:	FA697C84958E38E6CBD4903C694EFAC8FCBC029510757B60448F11E84FA837DFC65E5F493874053AFB55D6ED4AB6BDF8E566ECF90DFC4FC8C0856D5FC10FB85
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{.....z....._keyhttps://rikapcndbn.web.app/ahygdvxzsa/themes/17034c4caccdac15190faf36c3557a3dnbr1622646221.js .https://appdomain.cloud/.....#/.....F.....?....@.g.K?.W~...;..R...e }..3Z.A..Eo.....W.....A..Eo.....0\r..m.....{.....z....._keyhttps://rikapcndbn.web.app/ahygdvxzsa/themes/17034c4caccdac15190faf36c3557a3dnbr1622646221.js .https://appdomain.cloud/l....#/.....?....@.g.K?.W~...;..R...e }..3Z.A..Eo.....+1;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\328b75cf02d95d5e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.685003685432698
Encrypted:	false
SSDEEP:	6:mcYiRDHwA7eIAX3TH5R2D5yOSowDgjn5/m4HshK6t:XDHXeB3L5gDxwCm6s7
MD5:	06A972395C5F26A9976C36FEEAB6D176
SHA1:	B1C6D97DFC9429B6EE045AF2E33E623D45D87C6D
SHA-256:	E035EE57A7AEC19F440C3BF01982056ABEC9CE5AED7E1FFEC400C737099176D6
SHA-512:	F1C9FA4CF1802FBC97F7E5E076D31B905331578228287A6E71D79D758CD164D22E9159188471F56DC2AF1CEA56E444D352A1B98B6DFCB6A8E997319C156DCD0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...?....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=8c84dc53-9dee-f42a-46b1-5a93c0e43d70 .https://microsoft.com/N(...#/.....1.....U..0.....\.oQ.8gD.r*{.....A..Eo.....X.:.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\48f565ca8f495c25_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	37160
Entropy (8bit):	5.806601180834401
Encrypted:	false
SSDEEP:	384:3Ox0tnyN1C5H8lbHsUR7C7n863ON2Uz/ARne3G+H7jQ5UBvwvHJYlroYtcAcIX:3ACne1C5HPHsOU85MUbAg2fUL+Y3Z
MD5:	17F15D37645B832C8D7AD62D3A142F31
SHA1:	47D51E99A786DFAD3D0AB0554A6C67CA13F62D3F
SHA-256:	E48CFFC2AE3BB6D263D28226970508C04CBA3BE969FA120AD319ABF45E381652
SHA-512:	3486C5A2996BFF168AD80CEFAF041FA6920375DC6AC666D33F58FC63D0D2FA7B4C4DB16DD03ADFAD8F5642B32597239AC0E6F610D9C3865EA8BC3DBAEECB6A55
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....W.f...._keyhttps://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js .https://appdomain.cloud/.....#/.....J.....`.....u...T,..p...S._U2.au.7....A..Eo.....3.....A..Eo.....'.....O....h...z.a.....(S.<..`4.....L`.....(S.l.`.....L`.....Q.@.....exports...Q.@.....module....Q.@.....define....Qb.Q.W....amd...Q.P...G....VeeValidate...K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.].....\..&.-...%....(Rc.....l`....Da....2.....e.....`...p...@.....@.-....`P.q.....R...https://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js..a.....D`....D`0...D`.....)...`....&...&....&.(S.....`p#.....L`B.....Rc.....`.....S...Qb.*.s....n.....Qb...]....r.....Qb.....s.....Qb...V....d.....Qb..[.....p.....O.....QbNc.....x.....Qb6.C....w.....QbRK..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d80fc69098d2f00_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	651
Entropy (8bit):	5.409595434243996
Encrypted:	false
SSDEEP:	12:XsDQLzkGFhhykPpoMKl0xUDjNC1Ngw97weyY0p5FSDsC/aWbH:Xs0hQklxUDRCTFyY0MgC/au
MD5:	7A40B47F610DB26B9FEC42B2883D0FF3
SHA1:	D4336EFFC246A711CEEE0492737F0D73845E9172
SHA-256:	9552C57C60AEF1DA4610162290E49BDBD1DDDBF6F7B3E523D5D52C3A749CDB48
SHA-512:	9F18CC56350CCF8F2B1547D2D1A5D2915D960D1A13D31BF37A9FD8336C57A3EC029608D9FC7CD620B31D187650CC3EDCB5FB6D36D53DDE2CB2A1C71D41DC30
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/6a-234a32/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1 .https://microsoft.com/.....#/.....+.....]-=....1...M.j....t.O.....E..A..Eo.....k4lf.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6ea6b0fd83aa1e1f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8643
Entropy (8bit):	5.617228046958892
Encrypted:	false
SSDEEP:	192:pHwFr/cLhO9fCgiu+hT6K6POv2QkRbjsquZ0UovCHJnf:p4ULhO9athuNvgTovCHtf
MD5:	F1DCD221C38C5B13694EC54CCCF64728
SHA1:	8D79E2499C454C03B94A442F791B28EAFCC61B18
SHA-256:	FA129E75046535224F4EDD0277C255F223D505011E64EC01D53AEF246DEF9ECC
SHA-512:	9771968902176E61E2716196D1E3E82CDF267ACBCCD4952CD4B13C9D606E6D79E10BD13F0CF155D3DA7EE410FD51E7828C319FF148E8FCD9B531F5CB2C1045A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[.....5d...._keyhttps://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js .https://appdomain.cloud/.f...#/.....8Sw2G/.?.,6.a4t....l..}.lU...A..Eo.....r.. .....A..Eo.....'..)....O....@ ..`vW.....L.....(S.<..`4....L`.....(S.l.`.....L`.....Q.@.....exports...Q.@.....module....Q.@.....define....Qb.Q.W.. ..amd...Qb.o"K....Vuex..K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.].....\..&.-...%....(Rc.....I`....Da.....e.....`...p...@.....@.-....LP.!.....=...http s://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js...a.....D`....D`,...D`.....`....&...&....&.(S.%..`.....L`.....Rcp.....0.....Qb.].....t.....Qb.....e.....Qb.*.s....n.....Qb ...:....o.....Qb...]....r.....S...Qb.....s.....M...R....QbRc.....c.....QbZ..-....f.....Qb...^....l.....Qb..[.....p.....QbjG.....h.....Qb...V....d.....QbF..-....m.....Qb"D.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\753172e1420a85e5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	50218
Entropy (8bit):	4.987573259515028
Encrypted:	false
SSDEEP:	1536:aLLu72+Bo7ABvnqKbDkmm6dGwjA7G+4qmrmqjkQ+TIYgrwv:Mu72+WABfq+5Zk
MD5:	61DA1B1B68AD3C2F0670634469173A4E
SHA1:	31E2B5D561765E62273ED6A7C1FD7BF42A950037
SHA-256:	D7D996B22381EC5CA9E918EDB4A3A87742B4B6C27ABADB9AADCF57925EDF0DC7
SHA-512:	EBC6231B027DEBDBC8AD4F9627D34F9DE83A19E52BE602F7FCB3871BFF88997431E2069BDC839CA5BAAD9BD7660FA5DDAC0FFD78A0FE2B49965CC14018B4F4F7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{....._keyhttps://rikapcndbn.web.app/ahygdvxzsa/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301622646214.js .https://appdomain.cloud/j+...#/.....5... ..../.....z..~h=...]W.&.,..l3. {6.A..Eo.....A..Eo.....'.zy....O.....Op.....h....1.....d.....(S....`..... L`.....(S....`.....8L`.....@Rc.....Qb>. .*....$yun..Qb..l.....$uyn..Qc.....$utnbr..b....d.....I`....Da.....(S...`.....L`....I..Qc~.s.....parseInt.q...Qd.....fromCharCode.....K`....D{ .....i.....&....&...7..&.]...&.]...&...8 ..&..#j.....&.(...&.%.@..&.Y.....(...&..$&.Y....4.....,Rc.....`.....a.....e.....G.....@.-....lP.....]...https://rikapcndbn.web.app/ahygdvxzsa/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301622646214.js...a.....D`....D`>...D`.....`....&...&..!.&..q.&.(S.,..`....]..K`....De.....&.%.*....,Rc.....I`.....QbJ.....$ut

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\781980b07f1bb38f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.6739220768269
Encrypted:	false
SSDEEP:	6:mql9YiRDHwA7qYsDpNdNFvNgD+xAmR0QK4mK6t:RTDHXqn/xNgD+xOQE
MD5:	4B9FB554D66B266B91F5BCDD5780DDE8
SHA1:	3233215FA03C46843B73E2931D7FEE6B1E509BA6
SHA-256:	D0619EBCD8174EC33D060F07BD04B4476C4602AC39363B47EF12DFC35C4D8749
SHA-512:	814A2364D53A5ABB2FC7E6A57401FA77EDD9EC766F4654FCF3BBF3ADA304A0005B30D82A611999BF404E0572349AEF1494134AC65F0779947859A1BC8FA8FD33
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...0.v....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4 .https://microsoft.com/....#/.....5...a..... S...s5.O..8O....F$.|3F.A..Eo.....|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7df541af6f0604ae_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	31166
Entropy (8bit):	5.6035153883629345
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7df541af6f0604ae_0	
SSDEEP:	768:o8P/dsiEZ7SkqdWsizZ+QWqvUFmHQ5GXzq:LP6PhDqdWs0wGIzOm
MD5:	8F4BD621969FD141BDDAD174D0927EBB
SHA1:	F5B7259E99AC9CE9D6F5C0DFF02076127C774ED7
SHA-256:	0B4A2311B40702D22A530F31D96ABB47BFAA2B57D1979A95B7EED85EE5C43F3D
SHA-512:	AAAADED90A4F30580E7A9C1E49E09D280BD137645C3B2D571B539D7C032575FBAC88CF6FA6B49A672BBDCAF574B6C309D98D7B49D39001F13E71C06C9ADCE21
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...^....._keyhttps://unpkg.com/axios@0.16.1/dist/axios.min.js .https://appdomain.cloud/.....#/.....t.c.i.<.1....N...V....)...S..?.A..Eo.....+g.....A..Eo .....'.....O....(x.....(S.<..`4.....L`.....(S...`.....L`.....Q.@.....exports...Q.@.....module....Q.@.....define.. ..Qb.Q.W....amd...Q.@...W....axios.....K`....D}.....s.....s.....&.\..&.-...%..H...s.....&.(.....&.|.&.^.....&...s.....&.\..&.-...%...\..&.-...%.....(Rc.....I`....Dat..... ..f.. .....`...p...0.....@.-....<P.....0...https://unpkg.com/axios@0.16.1/dist/axios.min.jsa.....D`....D`$...D`.....`....&...&....&.(S....`.....L`>....(S.`.`x.... L`.....@Rc..... ...Qb.].....t.....Qb.....e.....Qb...]....r...b$.....I`....Da.....(S...`.....L`.....!..$..a.....a.....QbBC.O....id..C..Qcv.].....loaded..H..a+..Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\88dc8e2097326454_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96664
Entropy (8bit):	5.817309422172258
Encrypted:	false
SSDEEP:	1536:kzPCtyEySRJ/9EMGGyogjNWlYE+n1bhgroip3cCw:qPc/yCmMGGynNjEC3Soc3O
MD5:	C19F5A02EE7AFD997C0F7A2CD6A7EE11
SHA1:	5D2BA72AD65DD161246BA3199D0EF77F50299EDA
SHA-256:	41C2E03BB0DD5205B2C587CF3168ADA920849E43CFCE00E2CE94A58BBB70B9FA
SHA-512:	B2259EB54C76FF2E67CDA6C88007050644E11607D7635927429FF595A55B01EFC5D65F2B57F2D42D33699FA14DFEDE52805F8EC7162E78D6588784E90595DFB8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....}]0....6428D88CAD211309052E7F07CD235DC13FD1C65FC75D9A4D31AFB7E26469BA7B.....'..R....O!...@x....B.....X....".....(..... .....l.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....j.....Q.@.....module....Q.@.....exports...Qc...\.... document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa..../...I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.jsa.....D`....D`....D`.....M....`....&...&..!.&....&.(S....".`.E.....L`.....Rc`.....(.....M...Qb...V....d.....Qb.....e.....QbZ..-....f.....QbjG.....h.....S...Qb6d|.....j.....Qb".q.....k.....Qb...^....l.....QbF..-....m.....Qb.*.s....h.....Qb...:....o.....Qb..[.....p.....Qb...]....r.....Qb.....s.....Qb.]....t.....R....Qb"D.....v.....Qb6.C....w.....Qb....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8dc6cc7af937d5e7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	484
Entropy (8bit):	5.733041468099351
Encrypted:	false
SSDEEP:	12:euBT24zQruIpsS1JVguBT24zQruIVKS1JDV:eOV5IP1JVgOV5I11Jh
MD5:	CE225F78C8734DB117917BA3CBFC56B4
SHA1:	DA26389C3C0FEB81DF9F486EB4AB6ABECFDB7438
SHA-256:	A767B2F6FDE614FA6CAFB972A02C591B724FF175286DAE78F1EB811EB328FE72
SHA-512:	E46F08D56C527306122918F03DEF22DD39AEBC663FE485E2FA908BC8B9073EF91F5A53E9349C9AE2218AEC7096D39922D3A33FBC39B3E720B0B2A8735307CA5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n.....`....._keyhttps://rikapcndbn.web.app/ahygdvxzsa/themes/96cf99fc63f83319d09ad083f8a504cb.js .https://appdomain.cloud/.@...#/.....[`..s.8....DU... .MM...8.v....A..Eo.....=.....A..Eo.....0\r..m.....n.....`....._keyhttps://rikapcndbn.web.app/ahygdvxzsa/themes/96cf99fc63f83319d09ad083f8a504cb.js .https://appdomain.cloud/+<#..#/.....[`..s.8....DU....MM...8.v....A..Eo.....:.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3c2e2c260a7099_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.316842894519256
Encrypted:	false
SSDEEP:	6:mXYI4McTDsJegD8Alkt/61TrlEro//hK6t:e+TDsYgD8HktC130or
MD5:	E045EE4A3B95EF83165ED3F077135F77
SHA1:	8729E1347387E4C4C9D89107287798CB568681E8
SHA-256:	F85140F5E86BED6503F7FCC5834E2D06B73722B1EA2C19383D6B6DFBB02E1134
SHA-512:	61629E032BABE5FA5542B131A5EAF66C4B8B260A023701EBF6F48CB1CC74FEB162F70EEFB6B3EE00C3F7BEF7A9E26C2D5AFDAA8AA7011E926300CD2D3C7C2FDF
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3c2e2c260a7099_0	
Reputation:	low
Preview:	0\r..m.....V...|.L\...._keyhttps://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js .https://microsoft.com/....#/.....<.S....l....*.W.U\..E?`..r.A..Eo.....Z..... ...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b90ea9ec3c36916c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.675874722185327
Encrypted:	false
SSDEEP:	6:mEnYEmyq3OSKOAAR4NVzoZK6tWEnYEmyq3OSmAwhR4NVDu5/lbK6t:ZNcrNR6poTTNcr6hR68T
MD5:	7A81799CFFAF764EF79947C44302F952
SHA1:	1D59DB2D431298A618D8D6CCF3CB97ADEE6B312E
SHA-256:	AECA813229C8F33406962C118DB505A044DDD273AB878BB9E63AAAACC1AF6BE5
SHA-512:	E907B3DE35CBD34EA6B1020B78ADF228FF25DA38AF0B66F5E3C58D6614C5BBD9DBE5220B69E365B22A020FBC9297A882E9B6BB8D50A484036446FE3D302F6B 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://kifot.wancdnapp.page/60b79dd6cc1251248c7a9396.js .https://appdomain.cloud/.....#/.....m....."....C}k5..`{..M..ov...%.[.A..Eo..... ...A..Eo.....0\r..m.....V....._keyhttps://kifot.wancdnapp.page/60b79dd6cc1251248c7a9396.js .https://appdomain.cloud/`....#/.....j....."....C}k5..`{..M..ov.. .%.[.A..Eo.....q..K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bcba23f2a537c6bf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42901
Entropy (8bit):	6.212284927419107
Encrypted:	false
SSDEEP:	768:6jxFTawkOYO0UVJ/Z8v9oigvzbaLWfzkU2205xuaxKnogFHmt9H4eXATPctZylhG:ITawnYO0UV1Z8vG9naLWfzkU220/YnvS
MD5:	61D02DC730272BEF6B0569C98ED1F31C
SHA1:	B44968EFFC21314228F5C35E7FE859AEDAAE1CD7
SHA-256:	8EB2CF42C4F0EFDA359E2154689AC60477DC92E6F774FDF08198BC86358FF6F4
SHA-512:	8B7FB378AEFAE8D6B3E88C3D25EBF62326EE51DBE6E73F871EA0E4BA61608085B798056461FFA950D783513676CEE9BF6B2509460E93332E2BBC51F87C7F6598
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....9....._keyhttps://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.js .https://appdomain.cloud/.....#/.....z1f...F....dj...r.XL.T.;s.`t. .A..Eo.....W.QP.....A..Eo.....'.A.....O.....;X.....p.....0.....(S.<..`2.....L`.....(S.8.`*.....L`.....0Rc.....O.`....l`. ...Da....f$...(S....`.....M.L`.....dRc.....M...QbRc.....c.....Qb...V....d.....Qb.....e.....QbZ..-....f.....QbjG.....h...f.....l`....Da....b$.....(S.....Ia.....a..@.-. ...\P.a.....O...https://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.js.a.....D`....D`6...D`.....`J...&...&....&..Q.&..1.&.(S...Ia....c.....d.....@.. .....&.(S.|..`.....L`.....Qb...1....call.....S...K`....Dy`.....%..Tw.....&.....E.....7&.&...&.(...&.Z.....!...&.%.*..&...&.%.e....&.0...%..&..E.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c7ac401a91b7fb3b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19447
Entropy (8bit):	5.689278867685485
Encrypted:	false
SSDEEP:	384:r8r5FZpD+Atc0IYfMzXU1id5LnxEjNFouN2LNjUko5w/V9H:r89zpSGc9YfMzsixaNFqzH
MD5:	2374B745E0751464DFFB3CF7BA123BD2
SHA1:	E3E0B5901555BB74CE091F50C56CEECAC0F8A232
SHA-256:	020BFFF4524C9335969F46883AADF5D0E4CBB784D17FD5BC4366CEC7291A06BF
SHA-512:	79CC7E8C329029E8E54883D0921489B3D88FB01EBA22120813D3445AD2190910664A0A08E1D301FD8ACD816B277BCBD286E173A79BC20A1FAADE8A475A996B1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....*^....._keyhttps://unpkg.com/vue-router@2.7.0/dist/vue-router.min.js .https://appdomain.cloud/K[...#/.....E....6..$P.|....c9.Nx....@...%.e.A..Eo... .....*X.....A..Eo.....'.Z\....O....hJ..O}.....(S.<..`4.....L`.....(S.l.`.....L`.....Q.@.....exports...Q.@.....module....Q.@.....def ine....Qb.Q.W....amd...Q.P"..(....VueRouter.....K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.].....\..&.-...%....(Rc.....l`....Da.....e.....`...p...@.....@.- ....HP.....9...https://unpkg.com/vue-router@2.7.0/dist/vue-router.min.js...a.....D`....D`*...D`.....a....`....&...&....&....&.(S....`<.....L`x.....Q.Rc.....Qb.].....t.....Qb.....e .....Qb...]....r.....Qb.*.s....n.....Qb...:....o.....S....M...R....QbRc.....c.....Qb.....s.....Qb..[.....p.....QbZ..-....f.....QbjG.....h.....Qb...^....l.....Qb...V....d.....Qb..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e2a64377b8c73d51_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e2a64377b8c73d51_0	
File Type:	data
Category:	dropped
Size (bytes):	87720
Entropy (8bit):	5.639706563527665
Encrypted:	false
SSDEEP:	1536:UKFU2v62QPM1BBRTdXPS//CQ7ZUperEBUHDC6cDV+pyRP5KkdHLPJ:xS30rpXPzcXHrcDxRP519
MD5:	AFD66710172EB2741735D99A82186C94
SHA1:	EBFF9904E840F83C6CE511D364E6BF6D2BC2FFAC
SHA-256:	4C2A8ED402A93AEC9259C489AE397025233E3B167C160919FF58CE87385C6DAD
SHA-512:	8EDA5173AE33F770D9277F55CE30D9BAE6FFDE1CFBAC0B0EB7104C5ACC0CD51684E265FFBB8401D90E27595FE41120D10D55D0ADDEA588B79463D5371D887 86
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...>,.H....37993BF524D58221B98C5AEE06F93B58E5686857EB261CE6C5B5208DE90C380C.....'.D.....O....`U.....5..... .....(S.<..`2.....L`.....(S....`....Y.L`(....a.Rc.....Qb.*.s....n.....Qb.]....t.....Qb...]....r.....Qb.....e.....R.....S...Qb...:....o.....QbZ..-.... f.....QbRc.....c.....M...Qb...^....l.....Qb.....s.....QbjG.....h.....Qb..[.....p.....Qbb.....`_.....Qb"D.....v.....Qb...V....d.....Qb.....y.....O...QbNc.....x.....Qb6d|.....j.....QbF..-....m... ..Qb.M<.....A.....Qb".q.....k.....Qb..B.....E.....QbRK.....O.....Qbv..\....S.....QbF.....l.....Qb..W.....R.....QbZ..f....z.....Qb.....W.....Qb..\5....B.....Qb..a.....L.....Qb.....U.....Qb.$.n... .C.....Qb..K.....D.....QbNn|.....M.....Qb.l.....T.....Qb.k2.....F.....Qb..!.....N.....Qb".h6....P.....Qb..c\....Z.....Qb*e.....q.....Qb6I.....V.....QbZ..'....K.....Qb"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f07074a526b61413_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	339
Entropy (8bit):	5.888586112163311
Encrypted:	false
SSDEEP:	6:m+lVY0OCZI5B5LZzySxU6a5zOj6P4PcK6tnGaKQ5rSzOj6P4u:3VnI5BLCKjulGISKj2
MD5:	9E36005E575C135A40E25D0D524FE494
SHA1:	6EC658EBD49E792D1950BD804DCF531F32EB4FD2
SHA-256:	4F98142842A88FB94C456878D3A64373EC14589E3228204CA197B0F30102CE96
SHA-512:	947F11BD02B12DF33C2593DD4BF934CFC6FCBA6C392D3268AB3C9E9BFF98BC09C421AE8D71A54D991E773B9F13E8F78CB4FA61990A634F0775EDDFADBEB47 AE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K...z.{....._keyhttps://unpkg.com/lodash@4.17.4/lodash.min.js .https://appdomain.cloud/....#/.....Y.....d.....=b3.....L.OB&z..LR|Bt...A..Eo.....8.....A..Eo.... .....#/..V..37993BF524D58221B98C5AEE06F93B58E5686857EB261CE6C5B5208DE90C380Cd.....=b3.....L.OB&z..LR|Bt...A..Eo.....>`..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f428b9f7917ec10e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	63106
Entropy (8bit):	5.842397724623211
Encrypted:	false
SSDEEP:	768:VUXw2ij3hgFfV0yqkLc+WjnnC3eEzMfqFWNXa8aib43Z9BggYlOM8qJ:e32hglV0yzvWE0nXacb43NggYhjJ
MD5:	76F079E05E8E13A64E15FAE8EC7D0EB8
SHA1:	0225A0DA610EB9D9DFC7E28B174CCC6248DC8EFE
SHA-256:	E25E59CEF489C3CABB1C309DCF6CAA656E94B6F3A8ECBC8FE1CA9BDE6DBC413C
SHA-512:	96C2FABBF0EC4C3F9452BC92FE45866465612341CF5D238645D8EF0CDBACABD9F163D63ABD630D14E5FFF4871383FC982B1D3238C64618755991C1604678A11
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....8...._keyhttps://unpkg.com/vue@2.6.11/dist/vue.min.js .https://appdomain.cloud/.....#/.....=...7N....|.....%.[.A.o..`XOOX.A..Eo.....A..Eo..... .....'..m....O.....c.....!..|.....(S.<..`4.....L`.....(S.x.`..... L`.....Q.@.....exports...Q.@.....module....Q.@ .....define....Qb.Q.W....amd...QbvG9.....self..Qb.....Vue...K`....Dx.....s.....s.....&.\..&.-...%..3...s.....&.(.....&.]....%.....&.\..&.-...%.....(Rc.....l`....Da..... ...e.....`...p...@... ..@.-....8P.....,...https://unpkg.com/vue@2.6.11/dist/vue.min.jsa.....D`....D`(...D`.....`....&...&....&.(S....!.`.C.....}.L`:.....i.Rc0.....Qb..... e.....Qb.].....t.....Qb.*.s....n.....Qb...]....r.....S...Qb...:....o.....M...Qb.....s.....QbRc.....c.....R....Qb...^....l.....QbZ..-....f.....Qb..[.....p.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f46ad1d2652b0b43_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.530770465025965
Encrypted:	false
SSDEEP:	3:m+lSxla8RzYJb9yKlf8QPKxQBHWFvDFYtRyVKv1lHC6/yq5EzDHz4mFdpK5kt:mfYyK08fUH1Dfy6aq5EfzrFLK6t

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f46ad1d2652b0b43_0	
MD5:	4A7F92B7027504C711C1D5D9ECD52B92
SHA1:	133023B0A40020157B5948C515726BE573001D94
SHA-256:	C9BDF2C0F9D89E508036A023B649655585F37A5ADAA2BB2717E01498109446B6
SHA-512:	C00CF571C0C1386FEE03638347A65F943CD8A5455110DC184148A1B97CCDD756489486A89173AA5E577FC8AC27AFD37E26861079891C6D1BABAB7FCFE3BD135
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...T....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js .https://microsoft.com/....#/.....f....cB..cWhT..6..(..$....G..A..A..Eo.....x..... ..A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fd9925bdad311f6d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	650
Entropy (8bit):	5.429083230145612
Encrypted:	false
SSDEEP:	12:ltDQLH6kGFhhykPpoMKl0xUDjNC1Ngw97weyY0p5FSDrQe:ltkShQklxUDRCTFyY0M3z
MD5:	D4E00BF316E886B3E28B53BEB42FD7B1
SHA1:	B07F2CC10D95FC8389991DC8AA0246A8DFBDEDCB
SHA-256:	D6ACFD62CAA7A517F9ED3A66F0366F4B9E52C533283A7F045621B1F692EAC0E2
SHA-512:	A958A2C410EADBE460B946EFFA664CBBB5D2C909E6EB9C973CA2FEF1E0E70A66AC4BA0981575C1D87711235351C9C0317D2AD25890F8FCA823BFE6461B55FFC4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....% .3...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872 /d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0 /b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/6a-234a32/e0-3c9860/91-97a04f/1f-100dea/33- abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1 .https://microsoft.com/B...#/.....):.l&.A.....G.,_0..p.~.A..Eo.....".....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ff3254c380ce1732_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1103
Entropy (8bit):	5.0018071206882775
Encrypted:	false
SSDEEP:	24:MjXJaGN4zXk16FHPtJ8dtUUuzi19EJkuLUkl5E/9RLFePpZSw:M9aGQXi6OdCzLJk+UkeE1nePpD
MD5:	DB8B41CDF354FBAD9F106065826E5627
SHA1:	DE1D027943BC90F4FC56F6C5D18776ABF1563F44
SHA-256:	BD4F27CC3A17D65E714DCB9C126D69B39363365E1F39F0C9F9C840306146481C
SHA-512:	CE8F526AC59D40821455B80BA5581AB0A02B8E6CD0AB19DCBE6A1340C597028A69CF5AB777743668E1FA3DC376B3F2C6DEAD3E55F6FEF7E811C63100BE8561E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....'....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=0502864a-b6ef-2f14-9f8e-267004d3a4e0_c5ea3348-55af-729a-2641-14f0312bacf3_742 bd11f-3d7c-9955-3df5-f02b66689699_cb9d43d2-fbae-5b5c-827f-72166d6b87fc_49488e0d-6ae2-5101-c995-f4d56443b1d8_7dea7b90-4334-c043-b252-9f132d19 ee19_38aa9ffb-ddb5-75be-6536-a58628f435f5_e3e65a0a-c133-43e7-571d-2293e03f85e6_4ca0e9dc-a4de-17ba-f0de-d1d346cb99e2_06310cd8-41c6-3b11-4645- b4884789ed70_5c27e8aa-9347-969e-39ac-37a4de428a8d_d6872b5a-5310-a73c-7cb3-227a3213a1c5_be92d794-4118-193f-9871-58b72092a5ac_64c742e2-b29c-b6c1- fdd9-accf33ec40bd_cf2ceca9-3467-a5b3-d095-68958eee6d4c_cec39dd8-f1d3-56f1-abfc-a7db34ff7b46_ec5fa2c9-3950-ff57-a5c3-1fa77e0db190_d19f9592-65df-bcc9- e30e-439b875c3381_76a3d06f-f11f-77ef-9bfd-6227ba750200_5e1caa45-461c-3b04-f88b-8cd50af16db5_c2dceda8-20b4-7d3f-13b6-9cac67d7df17_914fa41b-cc86-d3b0- 4e15-2fdfa357bcc7_40c6c884-da6e-7c2c-081f-4a7dfe7c7245_ae79ba96-1a9d-debd-a5b1-f3067213b9b8 .https://microsoft.com/....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	816
Entropy (8bit):	5.285473353292966
Encrypted:	false
SSDEEP:	12:0tedKG+/+O4/D3UnylnYU7KzF6BMg7rW46cgwZzyz7V4hk+:0sdd+/+9/D3Uny93s2S46cJl+
MD5:	84608439941C4DBA4C1B8B2CE4F2B12E
SHA1:	F7030E009B2CE7AE5491D6BFE92A1E7906F44186
SHA-256:	2BF03BDBAECC37938930B5A26B62B49AECCDAA91A4B8BFAA5D30465A6A7E6D43
SHA-512:	638DE24336AD88DAABA9DBBA53D824BF0FA108230DCCC3E12E80961558C2D71D9880A64F4F7692AD62E0E8F50FD696BF9B288E7BE09FDB0E7C6BB0B23B3EE58C
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Reputation:	low
Preview:	(.....oy retne.... .....j.....l.6<...@. ..#/.....^]...u.2@....#/...../..i..]@....#/.....k-N.....#/.....x.....#/.....2...T2..d...#/.....m.1..%...d...#/.....p.&,.<..d...#/ .....C.+e..j..d...#/.....B.r1u..<..#/.....~.0.....#/.....7.z.....#/.....Q=.wC...R...#/..X.....Td2. ...R...#/..{.....L.S/..R...#/.....7..#...R...#/.....&.tp.....#/..... ....@.....R...#/..8.....%\I..e.H.R...#/.....#/.....n.R...#/.#.....;...@...R...#/..M.....~...(..R...#/.....o.A.}.R...#/..{.....^}.Np..@ikt../.....-..0..x@ikt../...../ ...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q...._.KPu../.....+<P|...X.KPu../.....],..#/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.8226790333307651
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwadyS93sNEQIIQ3bo/2:TLyqJLbXaFpEO5bNmISHn06UwwI+/
MD5:	AEDF50E0CE737EC24CD3DBFDE5997F36
SHA1:	3E5D7DA3CE35FF20F14C7A9E42FDC9F5DA90F265
SHA-256:	FA71020C6EDD2A4603C672D1018F3FDF087C977A09C28D3888AE5317D6F6543F
SHA-512:	4D3D27004AAE2FB7F2205B4C771236FA3328D50E86677C17B9EF2C6D20608E9B7495EDB25EAFFF0B9A1F92D2FF6E9B1DD068A52FC72582FAAE0D7EFE8EA808 4
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9668589090231927
Encrypted:	false
SSDEEP:	24:uCcLgAZOZD/5qLbJLbXaFpEO5bNmISHn06UwP8:/8NOZ5q5LLOpEO5J/Kn7UM8
MD5:	F3A6373948B88027FA641A8EF00998E3
SHA1:	31FFD5B5955FBD400D4F50A0AA713F977154A838
SHA-256:	0DB04CC0206AEB57700537094958955C54FF33B8CD009147BEFCA6BA4DD06679
SHA-512:	01B0FC3A471F3ABAAE85408CE1597D57710CBDD9546992D4DF33158DF51AE354D666F2B61CB69CAC27099AA97DDE21294D425BB57F18449522D9933EF47D4E7
Malicious:	false
Reputation:	low
Preview:	.....R,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10760
Entropy (8bit):	4.076775094912804
Encrypted:	false
SSDEEP:	192:3/5/25i5Co2Llf+rjUD5C5k535ut5D5uvkH05e5i5a5uokHm5e5i5Ihh54X5a:vUccoEGra0+xUVgcUYYUgpGYYIhEM
MD5:	18B405E9964B787C4A12F78BCE7605B4
SHA1:	59095ED81362EBFFA48D5A326FA68922F3C6BCB6
SHA-256:	EA1616E91C5CF72C8A225575A118C29B91AA69F98459598E8EEC11EF9FBAEC7D
SHA-512:	AC00208B59C8C58A7FDA470C6EE56313CDD7F3F633FEF5F72BC38251C409366137C65A8043F6366E8555B125775CB8AB9E28B0B194E5A44B800F61792F59FCFF
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...22c3bd88_6d45_4b5b_b0a8_8dbd6d59ac36.....<..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....B...https://vaqiw9zxozdoxzx.us-south.cf.app domain.cloud/?bbre=ozxiaszx.....h.....`.....PC....QC....0.....H.....B...h.t.t.p.s.:././.v.a.q.i.w .9.z.x.o.z.d.o.x.z.x...u.s.-.s.o.u.t.h...c.f...a.p.p.d.o.m.a.i.n...c.l.o.u.d./.?.b.b.r.e.=.o.z.x.i.a.s.z.x.....8.....0.....8..... . .....B...https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiasz

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.194415948231102
Encrypted:	false
SSDEEP:	6:mwG7q2PWXp+N23iKKdK8aPrqIFUtpDGTZmwPDGXVFDkwOWXp+N23iKKdK8amLJ:a7va5KkL3FUtpKT/PKXVFD5f5KkQJ
MD5:	5A217A4C51D390DD8AA3CC490A825725
SHA1:	FB477550D5CEB21C2434B7F3B3339F2EEEA5CFA9
SHA-256:	5C146F164C1F572B2706B61CB3E142E54A9851E7B859125895D9A5E6506B04DA
SHA-512:	9AA3DDE858B0444E9D72BA0B9C0FDB4B530D2A2B7713C81075EB6EF602FA8F99E7C9591DE298B77C20474082B978A384A1B2FDCB11F97E8314A18583F707D0B
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:41.788 310 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/06/11-10 :21:41.789 310 Recovering log #3.2021/06/11-10:21:41.790 310 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4 C
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Reputation:	low
Preview:	.f.5................f.5..............f.5................f.5................f.5................f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.217173404640852
Encrypted:	false
SSDEEP:	6:mwG1+q2PWXp+N23iKKdK8NIFUtpDGS32WZmwPDGoiVkwOWXp+N23iKKdK8+eLJ:a1+va5KkpFUtpKXW/PKoiV5f5KkqJ
MD5:	18E1E3F4FB50977740BA73412D7896D3
SHA1:	E7F8DF78802639308EBC5912BBFFB211BC7CE81C
SHA-256:	2A9BDF2C3A6A7D9CB4A8282B5440D28EF4F439397B20DE1E4DB890A7B4117BA3
SHA-512:	224D1A3CF53B373276A904C5F7BCCB12E84F3B649D6EF4B9F50287EF1C035CFF805B73901ABE56C116AF50A027EFF708A6E78D5919E611FEFB10D1099CBF920
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:43.921 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/06/11-10:21:43.922 d5c Recovering log #3.2021/06/11-10:21:43.923 d5c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	2.360093547410948
Encrypted:	false
SSDEEP:	384:LcoWeC6coY7icg/IXycoWemx5gA3WcoY7Rng/IXycoWe4+x5gA3WcoY70V:gogpo33qoUx+eo8gqoO+x+eoZV
MD5:	16A7F766296E7A88B027A1735328B800
SHA1:	A25313C50CEA266A1721E1891C57FFCCEDB38ECB
SHA-256:	F0F87C2C48F4BCC9EB0FF4BDAA834465A034CCF549E5E0E4C7DF309FEDFFD8CB
SHA-512:	A364061AE2121F7446E37AD891E472118A6372B28761C4B4B2FAAF0AB761AA6D70F2BAA07EAF8EBE8CC219B42D741FA55B856A6E7C840DFF872CC26C69350923
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	46804
Entropy (8bit):	1.4896610672159047
Encrypted:	false
SSDEEP:	384:FIcoY7ncoWe6kx+gA3WcoY7mg/IXycoWeT:1oRoIkx9eoMqoF
MD5:	36A15B385A72972E57AEFF6DA6352052
SHA1:	E6E8F4EB70D8ABFE2B05C912E004381E44C77116
SHA-256:	883D7FB8E6EDDB884F290674366257FBC349D24A0D777194AA3CBD34F39D2731
SHA-512:	6B62F416DF045E0AA6D4829C7245F044976A50A344AB4CC3A8EFBBC4A64A58D495DF6B1C34764C0AA75151F2DCA5B4498EB2A35454479D8709E7A05797F04011
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Preview:	.........."..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.204261314846866
Encrypted:	false
SSDEEP:	6:mwGa3N+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpDGaT1ZmwPDGaTZVkwOWXp+N23U:aa3Iva5KkTXfchI3FUtpKaT1/PKaTn5M
MD5:	DB05D93305F405049BF4DFF694615185
SHA1:	B7AFB1819D482CBE528FCC0554A786D6A04A77A1
SHA-256:	B1C4477B372F48268B3D0610C1E49074412611FE8BA083F268D0C1946587908D
SHA-512:	732C81EAFABF8F973AEAD37CA7A8BCE34B48BE22FE135AFC6B3F8A39C188A5DB6D8CBAC57FC11787339E651ADB9DA4392EDF10DC39FC1C32EE367ADB332349AC
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:51.301 1af8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/06/11-10:21:51.316 1af8 Recovering log #3.2021/06/11-10:21:51.316 1af8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.205204430743204
Encrypted:	false
SSDEEP:	6:mwGaZR+q2PWXp+N23iKKdK25+XuoIFUtpDGa1ZmwPDGaZVkwOWXp+N23iKKdK25y:aaZcva5KkTXYFUtpKa1/PKan5f5KkTXp
MD5:	D0066FB4F5C3DEBDA56E675B50BE6327
SHA1:	A72868B02ECA862A33CD5C870A236A3DB6D54747
SHA-256:	7DE8146FB5067A89AD191FEE351CD8AD435496587C8A6F4C0D4B009AC8E48A6D
SHA-512:	80A36F3A4CDDCAD458331EB911BA016B8BEA064BAD5B801EEBE34DBF1CFBFF102D642A1BFD790EF09CCDA316C5CBC0E0711A36555FF7E5BB83D7330618EAAF3E
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:51.295 1af8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/06/11-10:21:51.297 1af8 Recovering log #3.2021/06/11-10:21:51.297 1af8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Entropy (8bit):	5.207129303677163
Encrypted:	false
SSDEEP:	6:mwGaP+q2PWXp+N23iKKdKWT5g1IdqIFUtpDGaRGZmwPDGa2qdFNVkwOWXp+N23im:aaWva5Kkg5gSRFUtpKaRG/PKa/T5f5Kg
MD5:	7D5EC7B0168421EA1C6B98FF89B20522
SHA1:	1DD5857B939E358D860D30C85CED3B1C16AC8A44
SHA-256:	63180E30529C574B19EFD600B50CE8352381B54D6F45FB659CCAEE9E7D465CE3
SHA-512:	317C4E01CD8EF7233F4532516BB65A78ED1E411DADB40E234BB29A055FA5D4FFC4D8756EFCC355E2D76032419940CA2FB73BE20A43C4BD51465E9251C50D215
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:51.286 1af8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/06/11-10:21:51.287 1af8 Recovering log #3.2021/06/11-10:21:51.288 1af8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	90112
Entropy (8bit):	1.171140272728057
Encrypted:	false
SSDEEP:	384:NgJco2b1coY7lg0p0f9co2yCg5D1coY7Sg0pVE9co2Z0XWg5D1coY7F:Rojov9eoR4oQUoV4os
MD5:	CFD7944D5D2FC8B073817E8333B49F2A
SHA1:	86A472D6E4022C2208E3F60698E95339DB37D0F5
SHA-256:	9DFC2D8EE899A6363F495FFD0C7E6E1F204AA683973B8598C430423C7AD06DA4
SHA-512:	23AD69D138F75B536467030DE1638FB459BE0134276BF8CE4FEF0C2F5D7ECC145A6F3702CF462925E0FDD4E5FADB35CE676F527FDF0B8409F903193868D578BI
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2444
Entropy (8bit):	6.238059655850886
Encrypted:	false
SSDEEP:	48:f/Eie/kgTUCp0ZgTe+fkTUq08+Sr5tpTcyvgP0l3jw5s3fC3nlB+1hA5EksL75HH:fsiedYCOaTe+8YD8+S5tpTcYpw5CK3lg
MD5:	15808B3962448A6247CC7E8230A545E0
SHA1:	E6D2C4F466720F6C43153A6E7245B58EFF1D027D
SHA-256:	857FA38ACEA8522F842C760881E2934324BE5D70A36AA80F35CA5568A1CDB12A
SHA-512:	93777A214D4021EE036E0B435C7325C9FB130364931433325CC0F416DFA2AA58CB5F0E23280ECF49D56C2141462687E427E308A4275A5A6AD37A9CA8BC0F8534
Malicious:	false
Reputation:	low
Preview:	.....".....J0shyrldblkaj3lq3feiruzzfzqqo0mgq4ladwtmnaq0twpgnofeo6jrvgbbfzea4yxtztkdprg..365..appdomain..bbre..bwmodtqtqyv7pa0..cf..cloud..ctnm8sajzgey5ildn..https..in..office..ozxiaszx.'qjdgg12br68iwoakxtfcuxndjkk6vbxsq14pgly.Bsfrnl6zcu24tlnocmqa4ydrlnojodpp218cskzihwcwzalwbslu1l1fctqkvigxjkj..sign..south..us..vaqiw9zxozdoxzx..with._ysujlx45icp0klhixaqpe5u90cll1xe3ddln3bffxymctu1syzk8pyfndc0rxzuanmqxq4unxzabg6dtpetkxklxirj1itg*.....N.J0shyrldblkaj3lq3feiruzzfzqqo0mgq4ladwtmnaq0twpgnofeo6jrvgbbfzea4yxtztkdprg.....365.....appdomain.....bbre.....bwmodtqtqyv7pa0.....cf.....cloud.....ctnm8sajzgey5ildn.....https.....in.....office.....ozxiaszx...+.'qjdgg12br68iwoakxtfcuxndjkk6vbxsq14pgly...F.Bsfrnl6zcu24tlnocmqa4ydrlnojodpp218cskzihwcwzalwbslu1l1fctqkvigxjkj.....sign.....south.....us.....vaqiw9zxozdoxzx.....with...c._ysujlx45icp0klhixaqpe5u90cll1xe3ddln3bffxymctu1syzk8pyfndc0rxzuanmqxq4unxzabg6dtpetkxklxirj1itg..2...$.....0.....1.....2.....3.....4...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	100580
Entropy (8bit):	0.662253528774531
Encrypted:	false
SSDEEP:	384:Wk1coY7GgJco28g5D1coY7Dg0p0f9co2iQ7:2opoY4o19eoc
MD5:	402506EC171331C30EC6AA256A8C8656
SHA1:	3DA79C8C52E0C4C71165A967B101C4EE3FB44208
SHA-256:	2FEA712B7B345118EF567E99A3959318063F08D42BE40C391EBEAAC12BA42072
SHA-512:	343AF4842274329104D96AEF683BD9A7D583291C8D6E5EF2014529A4E8B9D51438C510F3D1F9092A044C14107B11A2BDAE926CCD9BAF8BFBD11EA3A74EE2B96

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Malicious:	false
Reputation:	low
Preview:	.....4(..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3767
Entropy (8bit):	5.588996147929794
Encrypted:	false
SSDEEP:	96:Sb5JI5H5ai5s54a7OMWdbgBRubQ5fgGGrS0i5Z5s5p:Sb5JI5H5ai5s54yOtdcBRuE5fgHi5Z5C
MD5:	4F5592D764046438FC82DC04D362FAE2
SHA1:	34E1FCCEA5A593243E4D4392BDC13EC639941CA6
SHA-256:	2BE2AD13475D814AACDCF6BA31CB4C7A10BAD4C2CFE1EAB41974C7B7C3EF8434
SHA-512:	237BF3EB994FC2DBCB287E75B6E913AD20E43E7E237AF7D7F77A057D7154B4F638B190AF66C3BECF673CA75F3C203614626DDA93F7730C65A3AECC076CC60DB
Malicious:	false
Reputation:	low
Preview:	...=;..*.....8META:https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud.....@_https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud..browserkeyN.{"browser":{"detect_browser":"","detect_browser_detail":"","detect_btan":""}}.=_https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud..userkey...{"user":{"keepLoginLongtime":0,"AuthNBR":false,"AuthKeyNBR":false,"tk_nbr_uc_frv":"","br_nbrcheck":"","br_utcheck":"","testlist":[]}}.M_https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud.._canWriteToLocalStorage.?_https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud..nbrteststst...../.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.ldGenerator.cast.RequestIdGenerator..585470000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogMana

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.181244807745579
Encrypted:	false
SSDEEP:	6:mwG7D0Vq2PWXp+N23iKKdK8a2jMGIFUtpDG95BRSgZmwPDG/4wIkwOWXp+N23iKi:a7DMva5Kk8EFUtpKrB9/PK/E5f5Kk8bJ
MD5:	44BF77D898B17BFC15BB7822A4DC39F0
SHA1:	EE42C304F092941B1403EDB3A817F5DB40E1688E
SHA-256:	31EBE90184C1931F6C04EDB715F17C02E1AE26F4B7CA6CEEEC5F4FC969EEC1C9
SHA-512:	AAC28B2D2446D5C20D93ABAAB95BAABF6EED0C11AC98CB6F0F715D827AD937BA3CFAF5D7E1573B45294DFD730C0C2A7CDED9BC64A9030148B3F8AEBCC6FDB847
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:41.536 6d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/06/11-10:21:41.552 6d4 Recovering log #3.2021/06/11-10:21:41.573 6d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	1.3897398788642705
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOvRz0OqAuhjspnWOa1r9dT9oU9u597UWFnh9wEOqAuhjspnWOoKOn:H8SGUASUE9UDV
MD5:	E94AAC5BC0A59353E379A9446718C4BF
SHA1:	4365099DDB217DF29313F807B6A2DCE9E84794C4
SHA-256:	52384EEE1E56E8C8569C4A4C236F87F7846736A3EF42D2B4B09A7DCC3489017E
SHA-512:	B2A40A39A771E75F68A4782D91DA6D0251338EFCD0B5F731D4610B3C74FC17F3F58A48712A75B87DD295BAFD4B019AF3F470D65A427BB197C10EB69ABB2DF00
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38508
Entropy (8bit):	1.140849646745676
Encrypted:	false
SSDEEP:	96:MeyqAUOqAuhjspnWOpkOqAuhjspnWO9D1r9dT9oU9u597UWFnh9p0OqAuhjspnWj:4y8iBUAS+o
MD5:	B828C2E62BE596AA0A82BD93A726610A
SHA1:	87994A8C54167C5ED9746EB79F0DF0DA69453208
SHA-256:	765C8DDA21B305A0FD7F4E2B626984F8E829331102E44649A27033B4C3347C54
SHA-512:	0E40AD71D012DA269FF019A0A123286494FA5D6BFBF1FA2F41084916AF1164224C1AF92E13B9ECDD44CC7D90F7380EF7C8CC9DA7ACEAAEF6AA559B3D06B5E 95
Malicious:	false
Reputation:	low
Preview:	.....M..&..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.237597706114035
Encrypted:	false
SSDEEP:	6:mwG6cVq2PWXp+N23iKKdKgXz4rRIFUtpDG4pnSgZmwPDGXSIkwOWXp+N23iKKdKt:aVva5KkgXiuFUtpK4pnX/PKXF5f5Kkgi
MD5:	6BB5875E9CF986B624F81B18ADCADA8A
SHA1:	2D34DD17B3FDD9E46557C466E47D0B2021C129DA
SHA-256:	CA9EA83881A54BABA2A908CDA5C786B35178E3BF98C24D60F5200C08331B832E
SHA-512:	BC0A1F4959CE848720A37DCA78C4C9CBA2F0908F531F5874E1E9CFB817406FEF5E2EE92C830EDFFEA4ED9833D8C0BC26975EFCEACB3352EE88A89CC89CEFE 22A
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:41.854 6d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/06/11-10:21:41.856 6d4 Recovering log #3.2021/06/11-10:21:41.857 6d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.242249784224462
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUGgp+3A4x4wpBr:wIElwQF8mpcSO9cBsqUi7A1
MD5:	01B1573AF3A479B63C1BE68DA098ED0D
SHA1:	F7AD4EE16DB20111D304F3E8A3C96EDA24759A99
SHA-256:	B9975871F5D77BD1ABE214100746F02373EC870FD32C42E13E6459E90EF56339
SHA-512:	12757C0C0CC40CFD9D217A08269D3582E2B7B4FA725E80EDBBB293B79FC95A6B9C4EB6AF317AE3972AF87DAC938D4350D929DB240509EA84F99D8CE8159DA1 C9
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6286732214888799
Encrypted:	false
SSDEEP:	48:eQqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUj4:eQhIElwQF8mpcSw
MD5:	E424D3AB4352986B9C527DBC7DF6DDA2
SHA1:	59244A8EBD0ED56D48718522263802DAB8AED5CD
SHA-256:	51F24C4B76B2285146174DE4D5724D4EE8760C126E9381DC0E8A0AC6A217B9B5
SHA-512:	06E7CB2AF09197D7C878E500928B4F38A76E372E95B850C3C0E6C2C5C6A81F7B48FE296B9D9AD97E2113B3FBF350F0A4AAFED3D66730B8A25471DDDB5BB874 7
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.104005483552134
Encrypted:	false
SSDEEP:	12:5l1lt80ACkRGxbwJK+aA3JcC4Pxbm/v/v/Ftl2GjUXzk:758CkRGxbwJK+L3l4xbm/v/v/3lLlj
MD5:	D2BAA4C1B3F69E5777AF350D4A2B5A9A
SHA1:	149DE2A60F6C32F0A1EA1993ECBF498E0974F9DC
SHA-256:	AF16B6E42B3BEA8AAB9F698980638E814E317DFA1E10B5F3E45326B9F240439B
SHA-512:	651E6F836FD556749DAD68E964D801CDA9F3F2C8BFF7D9E1E62888F9E017B6CD476738EEB80D3728E052E5E4308F2878E8A18E15AD8C657EB4F4E3EB330ACC8 6
Malicious:	false
Reputation:	low
Preview:	..&f.....X.....next-map-id.1.cnamespace-22c3bd88_6d45_4b5b_b0a8_8dbd6d59ac36-https://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/.0&U.93..... .....map-0-ReadyFIle.{.}...map-0-nbrteststst..\.....next-map-id.2.cnamespace-2542e106_7c83_4d21_81b8_e34d28d70869-https://vaqiw9zxozdoxzx.us-south. cf.appdomain.cloud/.1.R.....R.....R.....a3.....map-1-ReadyFIle.{.}...map-1-nbrteststst.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.213203171806952
Encrypted:	false
SSDEEP:	6:mwGUN+q2PWXp+N23iKKdKrQMxIFUtpDGjZmwPDGc9VkwOWXp+N23iKKdKrQMFLJ:aNva5KkCFUtpKj/PKC5f5KktJ
MD5:	844172465FD6199EC7BBFE16902191D7
SHA1:	3DED27198E4E12FDCCF11512734E6F6C80C96A79
SHA-256:	72F80F5C3C2F2F1DE5F0D04403EE3BC88A2C30E2AF44091A678312C2D750ECCE
SHA-512:	3A63625C69C7ED5104D2BD9734B512D613952D7AC4CE6845040733EE475FCEFCE10D52E861AA95916DFC9A9B742CC0F641A87A21B2B64963F3227052D028AAE
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:41.697 458 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/06/11-10 :21:41.698 458 Recovering log #3.2021/06/11-10:21:41.699 458 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.144106424000205
Encrypted:	false
SSDEEP:	6:mwGUn4q2PWXp+N23iKKdK7Uh2ghZIFUtpDGquyJZmwPDGspv3DkwOWXp+N23iKKF:aI4va5KkIhHh2FUtpKryJ/PKsBD5f5KF
MD5:	E20AAE08F614E90C7DDFB9A974BFC55A
SHA1:	A11683070D3AEC6D9B2EF9D58BE11637ED81E84C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SHA-256:	BE7F67032F5CFA87F0370EBC28790BCF858B5BE6CDB3D8237B7435A1A5E64170
SHA-512:	F7F59D254E697EF309B097F9781C73AE3FEA29F07B74ED8F656C56456DA249E00EEF516D3DEF2D830FE8F0BC160A69264945C25B4C52590FED65FC316C329AE
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:41.478 1320 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/06/11-10:21:41.483 1320 Recovering log #3.2021/06/11-10:21:41.485 1320 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\24bd4fe3-51fa-48ec-af39-3edec79ba4b3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.27673328265777
Encrypted:	false
SSDEEP:	6:mwGZgE+q2PWXp+N23iKKdKusNpV/2jMGIFUtpDGZXrkZmwPDGZxVkwOWXp+N23i3:agva5KkFFUtpKprk/PKR5f5KkOJ
MD5:	4A7FC8A1F9DAEDE8E13CFDB23D513C2F
SHA1:	38F9BF09F99FC0F12A7E39C83BB445876AC73783
SHA-256:	B4B00D3219EB7E39EB24A75A6A57BC2F74B27F883B33965F36D11EDEC976C854
SHA-512:	F1BD1A155BB10AC3B9823D8B651216731F8A3B3207182AF29F3961E3DE8D6B429E02222A6BDD4C9A1DF479616AE87793D633586F48E4C0494BD8C0C719C909E
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:41.771 458 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/06/11-10:21:41.772 458 Recovering log #3.2021/06/11-10:21:41.773 458 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.295883799032229
Encrypted:	false
SSDEEP:	6:mwGhFN+q2PWXp+N23iKKdKusNpqz4rRIFUtpDGIZmwPDG8EtVkwOWXp+N23iKKdA:ahFlva5KkmiuFUtpKI/PK8ET5f5Kkm2J
MD5:	AA9028420D5CD143F7B78B71D393EFED
SHA1:	AFCCF63FE76FA914B396AF780BF0EAB72C4535AB
SHA-256:	A761F8EBEA88CD642FBF8AB94CF6B096BDC6DC9803D8CBBD4CA9187BA8FA0DDC
SHA-512:	D425E01CEEEFC5BB26F74790D1F786D92357E2B75E0A7653E6D7A170016C0D093EC53E0569DF9D8AA0D0F163AFDAF1CF91149229E6539C5E971552811155DDB
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:41.847 458 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/06/11-10:21:41.851 458 Recovering log #3.2021/06/11-10:21:41.852 458 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.249368323535494
Encrypted:	false
SSDEEP:	6:mwGlcRq2PWXp+N23iKKdKusNpZQMxIFUtpDGKZmwPDG2kwOWXp+N23iKKdKusNpB:aCRva5KkMFUtpKK/PK25f5KkTJ
MD5:	50DBD33F5E027E6427F074FAC79DD2E0
SHA1:	00A2DB7AED45F572E115AAC9A1A2F2FE568D3DBA
SHA-256:	F580440D15F048462EC6EAF5E3497D3620AC3D39CABDF494370B07D160D6F597
SHA-512:	D755F7083F3FB89C0CDF70629631EF02B82214C2682BF527C8B0776603FDA08C8A39348668563897504ED915580D308799F40BEBEE64C8C6C589B85D3B30ADD8
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:58.284 1650 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/06/11-10:21:58.285 1650 Recovering log #3.2021/06/11-10:21:58.285 1650 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\5d3799c5-1c93-4243-9e1b-c83897e62b27.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\5d3799c5-1c93-4243-9e1b-c83897e62b27.tmp	
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
Malicious:	false
Reputation:	low
Preview:	.'..(.....'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.223152773452582
Encrypted:	false
SSDEEP:	12:aCHnva5KkkGHArBFUtpKh/PKeD5f5KkkGHAryJ:aava5KkkGgPgoMeVf5KkkGga
MD5:	9A234FFD52DA98D2D59B0FB2B3ED8694
SHA1:	46FB7AD3E754FB96B6016D1C9EF3ECAE70E81C0E
SHA-256:	B6971D90F7F7B0F25D52C4C96FBDE8A04ED7E8310811E6884316DC29B78EBCF8
SHA-512:	94886A5BD728A7D8942BB2CB1C2574DF95AB33C3A0A63080FF2AAC5DFCD26ECF52FBC797839B9F255F3BBDB424151365DC6ADA6C14B08F36C879599F9EC22A7
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:50.948 458 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/06/11-10:21:50.953 458 Recovering log #3.2021/06/11-10:21:50.956 458 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.192068040821825
Encrypted:	false
SSDEEP:	12:abva5KkkGHArqiuFUtpKn/PKm5f5KkkGHArq2J:a7a5KkkGgCgoawf5KkkGg7
MD5:	223ACEFED532B296418AAB39454D8CA7
SHA1:	853DE85B26D2C86D051ABDE5A115F9BDEB53B54E
SHA-256:	4F463355418852624F52657553C1149424B6257352C25A5BC067FA2FE56DA03E
SHA-512:	E1F31EB0F7CCDFFFA7FBA0BAEC99573F8252399A253CEF30A135D629D5EB510EA5BA08ADBCB24C0FB31DD7A4D88D2A0391BFE0E1C5F3E598A24C37A028069995
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:50.960 1650 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/06/11-10:21:50.963 1650 Recovering log #3.2021/06/11-10:21:50.964 1650 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.205361740497342
Encrypted:	false
SSDEEP:	12:aBIva5KkkGHArAFUtpKx/PKr5f5KkkGHArfJ:aB6a5KkkGgkgo89f5KkkGgV
MD5:	8196C1D88B60A10180989FDEAC6C331E
SHA1:	6BD38287AC24323CD01A10CBEE83C22293BFA2CA
SHA-256:	6613E65D9A69B0538092A843C070475D5A1AA5C337CD45FF341B7BF5CEBA91FB
SHA-512:	041402B6BA854DCD55226CFC146E1B46EDE342062A08A6F6B778FD94976D548C7523096956E88ECA788A9E42E3438384DD2381CF2C0ECF67258B45DFF2F5CC6
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:22:06.191 458 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/06/11-10:22:06.193 458 Recovering log #3.2021/06/11-10:22:06.193 458 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.225654346230102
Encrypted:	false
SSDEEP:	6:mwGqNpM+q2PWXp+N23iKKdKpIFUtpDGduZmwPDGTRMVkwOWXp+N23iKKdKa/WLJ:aCpM+va5KkmFUtpKI/PKTRMV5f5KkaUJ
MD5:	410F8685D393E4625F5E82C5CEA7E6DA
SHA1:	FFED0E030591EB399267A0E0A136D64590AF78F8
SHA-256:	D0A4945012F6D1395D4AEBCC59E8784DFCAC9845276FA954AEED1BA3854C5FB2
SHA-512:	6AD1256129EAE6FCE77D615A3247F80CB720C52C1988C4CE5BE979183786FF6756B8B42D367FC1CF1B95C40D0EA9544182D714FD85380E7D79EC653875BE30A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Reputation:	low
Preview:	2021/06/11-10:21:41.483 f6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/06/11-10:21:41.486 f6c Recovering log #3.2021/06/11-10:21:41.488 f6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.347582159259179
Encrypted:	false
SSDEEP:	12:a+64va5KkkOrsFUtpKw5/PKV5f5KkkOrzJ:a/Ka5Kk+gowkHf5Kkn
MD5:	38172D3FCE26DF9F761C8271C3AC8890
SHA1:	74E4D7DF11A9EFB818E357621176A54052AB6E2A
SHA-256:	FDC932782FB815492F16FC3DEF88EDBFF56578AFA6E0947736755A058105400F
SHA-512:	20591E67D715CF1D4B26C436D04722E10E1371A8EC5400A6335F8BB564C8A71265CB8A3563B54B2E5756D93B74001C076BCFD03554FD0BF9A990B023C947DE73
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:53.136 458 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/06/11-10:21:53.137 458 Recovering log #3.2021/06/11-10:21:53.138 458 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	180
Entropy (8bit):	5.821613294445431
Encrypted:	false
SSDEEP:	3:6yeql/NHWZv3TrzZgbMvWlNvg/lgJlbI1rv/0PHAvllxaaRtaZtmoeL8lwBggq/D:Xsv3vzObuiNvZMHfjFRtom9L0wag+RQo
MD5:	F4E05587594347CDFB00763FD479F36E
SHA1:	A611BD83DBEB0E4C6A19812F7F0EE1D435BCEE9F
SHA-256:	DA22E77D3F0C7D816604828AF92ED8C867D9DD640731A82784449C587812F7E0
SHA-512:	FA79DB98F6C4F48CE905325B65178E8EDE4F00028DE9B5B7A8572F4F3460D9B42C09FB6CC0E5B35CB7E60CA81DC4E11A959E0063D356FD2E1934F6923FA1712D
Malicious:	false
Reputation:	low
Preview:	....^q./.;n{....m."d.V.....s..J.....dr..R-.....).H..(y.....9./.....}..p.,L.....b...-..1.....j.HxS.....@.....T8...a.....:.7.....4....w".....T..0N{

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\31c088d6-60c9-4612-8d45-1bcd70612ddd.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Reputation:	low
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E.....I...k}....{.m.t.CP.....E...\.....=H..,A..,J..;P.....nnp}nnp}.....~~~.....!...!---2---2.. .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P..Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e.....nnnzXXXa.....RRR\.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168B6
Malicious:	false
Reputation:	low
Preview:	F.....r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a0736c6a-43d8-46b0-afa8-f6650bd8b580.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b958bc37-a341-4d59-8ea9-6f1b4bf6b8d0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.536146476185522
Encrypted:	false
SSDEEP:	384:cVatqLlhTXT1kXqKf/pUZNCgVLH2HfD1rUmzUHGGTnTuU4sTm43:iLlpT1kXqKf/pUZNCgVLH2HfxrUm8Gyp
MD5:	DAF66A6B2C026F0997EA97C9034A9384
SHA1:	44728B7213C901ACDBC33819F2167D3D22A47560
SHA-256:	DA11FB1C2DD95DF757F15ECA5CEA1EF49C22036C518982BC3DC87C8CF494F2DB
SHA-512:	D0262927BB6E6144642BA7276E330169CF25C81E2B6B55714C8F93C11B7E7AE8E40B8E335EEF3C8640BEBA95FB99C41EF944A4DC76FBD2A2396CEBD27C81F61
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13267905701478630","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c5bd3cd5-73e0-4e2d-9580-f9de8ea07559.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):	2379
Entropy (8bit):	5.585952357053246
Encrypted:	false
SSDEEP:	48:YnU6VwUuI6UUhqUpeUVUsvzUeseKUewqPeUer2UefjbwU0wUlURUenw:OUdUuBUU8UpeUVUQzUe3KUGPeU9UEjkr
MD5:	687D2C145E54651080FC34DFC372ED50
SHA1:	C2816ACAFBC33D5A859385518AAB3CC64A4FBACB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c5bd3cd5-73e0-4e2d-9580-f9de8ea07559.tmp

SHA-256:	EE803F22CDA03E7E37C61FF2C43E1E9407C61133BEBF11CCBD9D2BA0F0DB1D63
SHA-512:	19C19B923ADDDD305A61F6A78ACC5FFAFED4C0D81D81A00D23362F8F11ACE13E6AC6ED11F40FD80ED1CE3FE8E9552B5F2E8AFDC1DE47085F6D7F3414549C9 A76
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1654968130.892763,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623432130.892768},{"expiry":1639212108.592752,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623432108.592755},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1654968127.549932,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623432127.549936},{"expiry":1654968127.721011,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623432127.721016},{"expiry":1654968130.286941,"host":"e0dnev3n5m4rUz3lgUGIx3llwf0kSf/EB+PPIf8u0SI=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d3ba0114-7af3-4080-9c94-51bd8b6693a6.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2210
Entropy (8bit):	5.587633207604886
Encrypted:	false
SSDEEP:	48:YAUAVwUuI6UUhYUrueU0zUeseKUewqPeUer2UefjbwU0wUlURUenw:5UfUuBUUOUrueU0zUe3KUGPeU9UEjkUU
MD5:	1A9820B994ADD2659056A78DF6E753CB
SHA1:	54C2CA02B46B7A02EE38D2C8D60EBA79D930CEA7
SHA-256:	344F873296F115D1D0C3660F22A497B92740A5F6B33F093BA0F859D755B545A0
SHA-512:	A60F4BC53E428DE670D8C8679EACF2A1B462E2D251447C401F16BC50B086F261D312D00075E7548C47B1DDA18656D72E654B1F64C5EBEE93FC99199E3909DCD
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1654968125.751306,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623432125.751311},{"expiry":1639212108.592752,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623432108.592755},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1654968121.963532,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623432121.963535},{"expiry":1654968122.31542,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623432122.315425},{"expiry":1654968108.41168,"host":"e3SziuwfuO2UvuBno+qkR1ObHAzZmSUoJhrc7dbP1Uo=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d5a6c12f-6955-4d9a-8b1d-b358e27d45ef.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):	5757
Entropy (8bit):	5.191683433361813
Encrypted:	false
SSDEEP:	96:neCUGC2Rv2s8GcVcok0JCKL8j5Mk51rbOTQVuwn:neCI2ReRGct4K85Mk59
MD5:	B7AF28FD3119A5CE48AC4E9B433B36DC
SHA1:	2AC5FB19B626E3B634F92DB845D8559E48C2C437
SHA-256:	525DFFA58CDFE40C2F4FC8445A109DB06C1FD908B292B77C6E4982F2687AD6A2
SHA-512:	B9438162CC9EB79E367FB1449891BF5E80B198225FC5F8021B6D14B2461D766948C9CC2D5CA088E1961933DF6B0F934E7DD788F92D55D1112B1805FCA9385C63
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267905701763236","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.256224724432833
Encrypted:	false
SSDEEP:	3:tUKUUGux/AgZmwv3GUGuwBWH1V8sGUGuwam5H1WGv:mwGiJZmwPDGYVVvDGFVtv
MD5:	35FF8C7FA6EA5EE24BB7BE72EF515A6E
SHA1:	D640C4AC39D7A77793ED52B90F922DA66F1D1BBD
SHA-256:	9ACDB403FB0650C55F88F26FB18FEA7C9A5102C69548D9E9A9382509501EA6B7
SHA-512:	E89DCDF9F496C3D8F49A3E195920D497A239979537251BB5272E0668A2D7BB92ECF2BA99AB6778FFC835E28791318DA0327F87517EF9F53CD0675DA5F6246331
Malicious:	false
Reputation:	low
Preview:	2021/06/11-10:21:50.069 1700 Recovering log #3.2021/06/11-10:21:50.115 1700 Delete type=0 #3.2021/06/11-10:21:50.116 1700 Delete type=3 #2.

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 10:21:44.742712975 CEST	192.168.2.3	8.8.8.8	0x33e9	Standard query (0)	vaqiw9zxoz doxzx.us-s outh.cf.ap pdomain.cloud	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:45.967994928 CEST	192.168.2.3	8.8.8.8	0x6de9	Standard query (0)	kifot.wanc dnapp.page	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:47.394701004 CEST	192.168.2.3	8.8.8.8	0x8ef1	Standard query (0)	rikapcndbn .web.app	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:47.777570009 CEST	192.168.2.3	8.8.8.8	0xdc3b	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:48.371387959 CEST	192.168.2.3	8.8.8.8	0x36ba	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:48.756665945 CEST	192.168.2.3	8.8.8.8	0xc745	Standard query (0)	vaqiw9zxoz doxzx.us-s outh.cf.ap pdomain.cloud	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:50.261620045 CEST	192.168.2.3	8.8.8.8	0xc132	Standard query (0)	aadcdn.msf tauth.net	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:50.264712095 CEST	192.168.2.3	8.8.8.8	0x794a	Standard query (0)	aadcdn.msa uth.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 10:21:50.730576992 CEST	192.168.2.3	8.8.8.8	0x5dd8	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:51.090691090 CEST	192.168.2.3	8.8.8.8	0xbb25	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:51.359282970 CEST	192.168.2.3	8.8.8.8	0x705b	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:51.749191046 CEST	192.168.2.3	8.8.8.8	0xb30a	Standard query (0)	rikapcndbn.web.app	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:51.750915051 CEST	192.168.2.3	8.8.8.8	0x6867	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jun 11, 2021 10:22:01.810045004 CEST	192.168.2.3	8.8.8.8	0x462b	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jun 11, 2021 10:22:03.999022007 CEST	192.168.2.3	8.8.8.8	0xc534	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jun 11, 2021 10:22:09.240757942 CEST	192.168.2.3	8.8.8.8	0xf550	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 10:21:44.810460091 CEST	8.8.8.8	192.168.2.3	0x33e9	No error (0)	vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud		169.62.254.82	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:44.810460091 CEST	8.8.8.8	192.168.2.3	0x33e9	No error (0)	vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud		169.46.89.154	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:44.810460091 CEST	8.8.8.8	192.168.2.3	0x33e9	No error (0)	vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud		169.47.124.25	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:46.032021999 CEST	8.8.8.8	192.168.2.3	0x6de9	No error (0)	kifot.wancdnapp.page		104.21.47.62	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:46.032021999 CEST	8.8.8.8	192.168.2.3	0x6de9	No error (0)	kifot.wancdnapp.page		172.67.145.59	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:47.464116096 CEST	8.8.8.8	192.168.2.3	0x8ef1	No error (0)	rikapcndbn.web.app		151.101.1.195	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:47.464116096 CEST	8.8.8.8	192.168.2.3	0x8ef1	No error (0)	rikapcndbn.web.app		151.101.65.195	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:47.836323023 CEST	8.8.8.8	192.168.2.3	0xdc3b	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:47.836323023 CEST	8.8.8.8	192.168.2.3	0xdc3b	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:47.836323023 CEST	8.8.8.8	192.168.2.3	0xdc3b	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:47.836323023 CEST	8.8.8.8	192.168.2.3	0xdc3b	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:47.836323023 CEST	8.8.8.8	192.168.2.3	0xdc3b	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:48.432876110 CEST	8.8.8.8	192.168.2.3	0x36ba	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:48.432876110 CEST	8.8.8.8	192.168.2.3	0x36ba	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:48.826855898 CEST	8.8.8.8	192.168.2.3	0xc745	No error (0)	vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud		169.62.254.82	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:48.826855898 CEST	8.8.8.8	192.168.2.3	0xc745	No error (0)	vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud		169.46.89.154	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 10:21:48.826855898 CEST	8.8.8.8	192.168.2.3	0xc745	No error (0)	vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud		169.47.124.25	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:50.323972940 CEST	8.8.8.8	192.168.2.3	0xc132	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:21:50.323972940 CEST	8.8.8.8	192.168.2.3	0xc132	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:50.331280947 CEST	8.8.8.8	192.168.2.3	0x794a	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:21:50.793101072 CEST	8.8.8.8	192.168.2.3	0x5dd8	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:21:51.160412073 CEST	8.8.8.8	192.168.2.3	0xbb25	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:21:51.160412073 CEST	8.8.8.8	192.168.2.3	0xbb25	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:51.420875072 CEST	8.8.8.8	192.168.2.3	0x705b	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:21:51.810030937 CEST	8.8.8.8	192.168.2.3	0xb30a	No error (0)	rikapcndbn.web.app		151.101.1.195	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:51.810030937 CEST	8.8.8.8	192.168.2.3	0xb30a	No error (0)	rikapcndbn.web.app		151.101.65.195	A (IP address)	IN (0x0001)
Jun 11, 2021 10:21:51.812408924 CEST	8.8.8.8	192.168.2.3	0x6867	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:21:51.812408924 CEST	8.8.8.8	192.168.2.3	0x6867	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jun 11, 2021 10:22:01.860080004 CEST	8.8.8.8	192.168.2.3	0x462b	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jun 11, 2021 10:22:01.860080004 CEST	8.8.8.8	192.168.2.3	0x462b	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jun 11, 2021 10:22:02.516469002 CEST	8.8.8.8	192.168.2.3	0x9ffe	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:22:04.072796106 CEST	8.8.8.8	192.168.2.3	0xc534	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:22:04.074491978 CEST	8.8.8.8	192.168.2.3	0xddcd	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:22:09.317626953 CEST	8.8.8.8	192.168.2.3	0xf550	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.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
Jun 11, 2021 10:21:45.160593987 CEST	169.62.254.82	443	192.168.2.3	49712	CN=*.us-south.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, 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 Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 10:21:45.165524006 CEST	169.62.254.82	443	192.168.2.3	49711	CN=*.us-south.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, 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 Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 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		
Jun 11, 2021 10:21:45.320746899 CEST	169.62.254.82	443	192.168.2.3	49713	CN=*.us-south.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, 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 Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 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		
Jun 11, 2021 10:21:49.195230961 CEST	169.62.254.82	443	192.168.2.3	49733	CN=*.us-south.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, 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 Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 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		
Jun 11, 2021 10:21:51.946666002 CEST	152.199.23.37	443	192.168.2.3	49750	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 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		
Jun 11, 2021 10:21:51.949444056 CEST	151.101.1.195	443	192.168.2.3	49748	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed May 19 23:19:33 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Aug 17 23:19:32 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

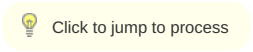
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 11, 2021 10:21:51.949588060 CEST	151.101.1.195	443	192.168.2.3	49749	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed May 19 23:19:33 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Aug 17 23:19:32 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 11, 2021 10:22:00.116656065 CEST	169.62.254.82	443	192.168.2.3	49761	CN=*.us-south.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, 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 Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 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		
Jun 11, 2021 10:22:01.835863113 CEST	152.199.23.37	443	192.168.2.3	49772	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 10:22:14.176748037 CEST	169.62.254.82	443	192.168.2.3	49828	CN=*.us-south.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, 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 Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 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		
Jun 11, 2021 10:22:17.141892910 CEST	169.62.254.82	443	192.168.2.3	49834	CN=*.us-south.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, 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 Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 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		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4080 Parent PID: 4232

General

Start time:	10:21:40
Start date:	11/06/2021
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://vaqiw9zxozdoxzx.us-south.cf.appdomain.cloud/?bbre=ozxiaszx'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 5036 Parent PID: 4080

General

Start time:	10:21:42
Start date:	11/06/2021
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=1508,3517359519867941500,5777929940254380 33,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1956 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly