ID: 345054
Cookbook: browseurl.jbs
Time: 16:30:40
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

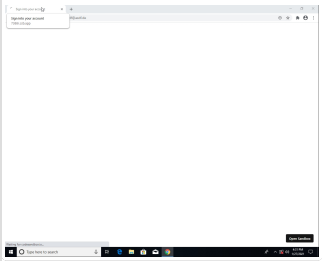
Analysis Report http://lib.tnua.edu.tw/goto/https://7388r....

Overview

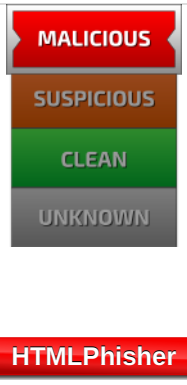
General Information

Sample URL:	http://lib.tnua.edu.tw/goto/https://7388r.csb.app#asdf@asdf.de
Analysis ID:	345054

Most interesting Screenshot:



Detection



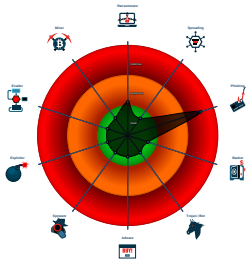
HTMLPhisher

Score:	76
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 HtmlPhish_10
- Phishing site detected (based on log…
- Form action URLs do not match mai…
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5944 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://lib.tnua.edu.tw/goto/https://7388r.csb.app#asdf@asdf.de' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4968 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1584,11749481043944155124,6311535833497222460,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1668 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

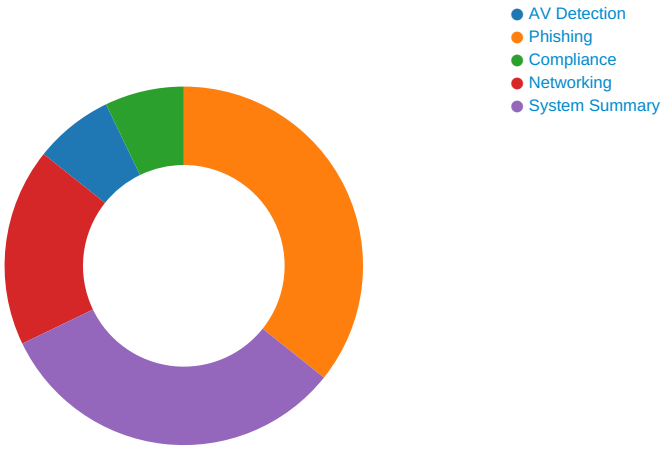
Yara Overview

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 HtmlPhish_10

Phishing site detected (based on logo template match)

Compliance:

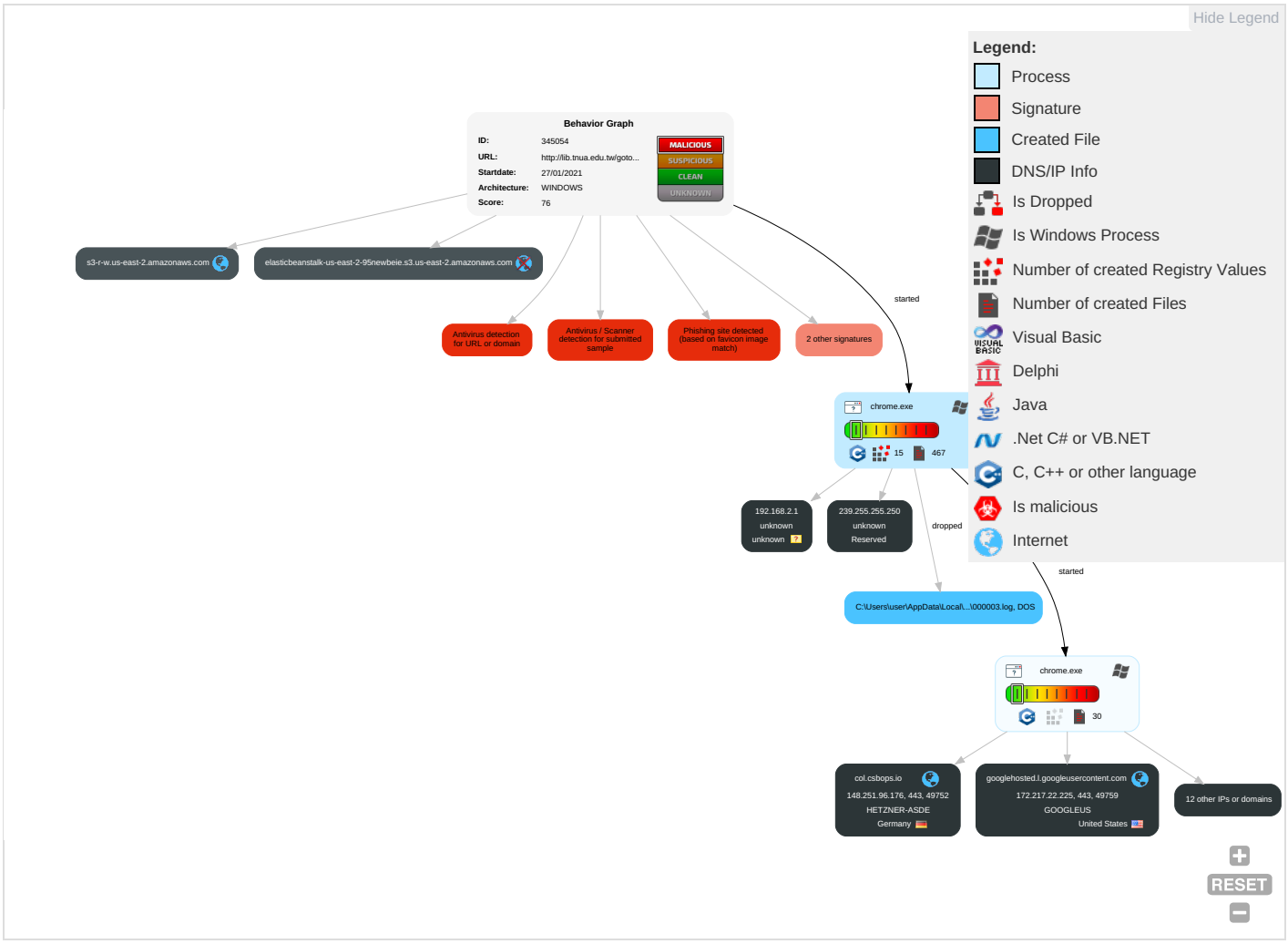
Creates a directory in C:\Program Files

Uses secure TLS version for HTTPS connections

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	Impa
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	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

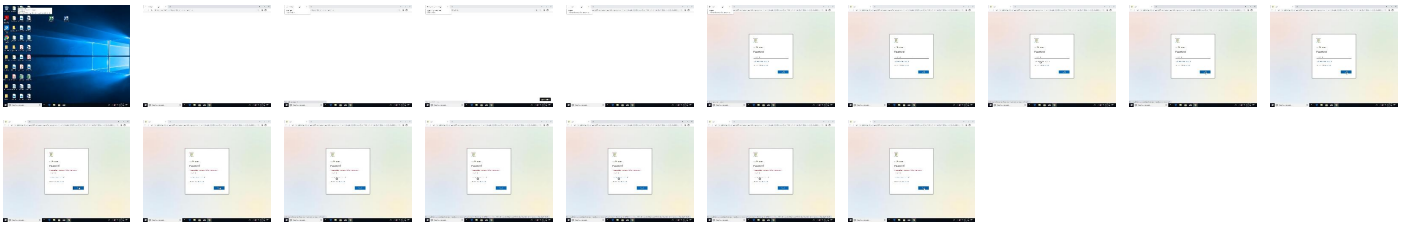
Behavior Graph

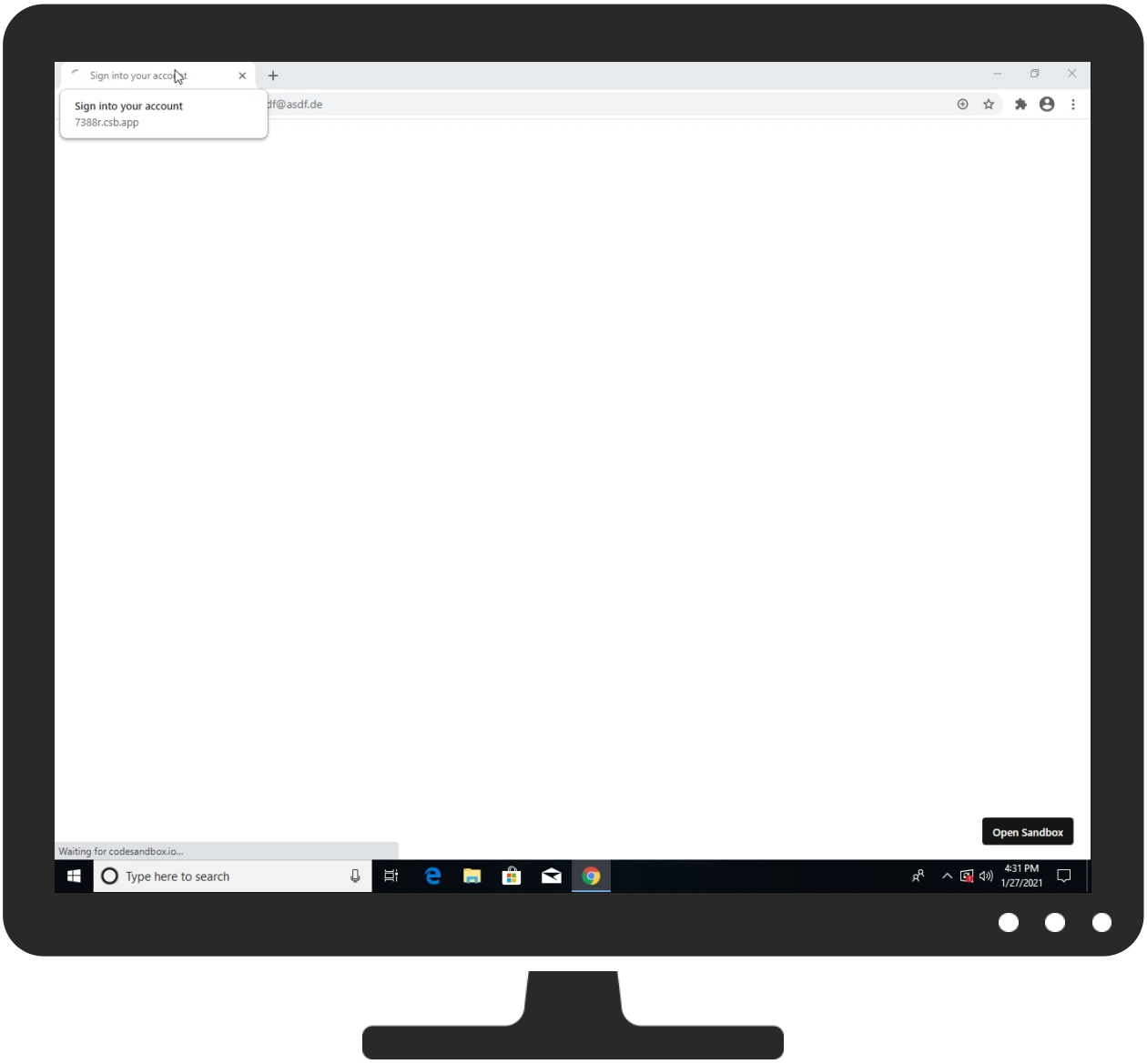


Screenshots

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://lib.tnua.edu.tw/goto/https://7388r.csb.app#asdf@asdf.de	0%	Virustotal		Browse
http://lib.tnua.edu.tw/goto/https://7388r.csb.app#asdf@asdf.de	0%	Avira URL Cloud	safe	
http://lib.tnua.edu.tw/goto/https://7388r.csb.app#asdf@asdf.de	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
lib.tnua.edu.tw	1%	Virustotal		Browse
col.csbops.io	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://7388r.csb.app/?#asdf@asdf.de	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com/index.html?auth=30%40ohixyzo80aNC4yMTIxXzIzNTgwNF8yNTQ1MzcuMDU4NTkwMDAwLCNGI1MjMTcxNDEjRQ%3D%3D%3Aver-UID=8c60cf39e11d1659051190bdc1f1a8a8#asdf@asdf.de	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com/index.html?auth=30%40ohixyzo80aNC4yMTIxXzIzNTgwNF8yNTQ1MzcuMDU4NTkwMDAwLCNGI1MjMTcxNDEjRQ%3D%3D%3Aver-UID=8c60cf39e11d1659051190bdc1f1a8a8#	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://7388r.csb.app/sandbox-service-worker.jsaD	0%	Avira URL Cloud	safe	
http://https://csb.app/D	0%	Avira URL Cloud	safe	
http://lib.tnua.edu.tw/goto/https://7388r.csb.app#asdf	0%	Avira URL Cloud	safe	
http://https://7388r.csb.app/0	0%	Avira URL Cloud	safe	
http://https://7388r.csb.app/?#asdf	0%	Avira URL Cloud	safe	
http://https://csb.app/8	0%	Avira URL Cloud	safe	
http://https://7388r.csb.app/frame.html?_sw-precache=358bc62ccbd9155c9f01d203199f04da	0%	Avira URL Cloud	safe	
http://https://7388r.csb.app/$$$	0%	Avira URL Cloud	safe	
http://https://csb.app/-	0%	Avira URL Cloud	safe	
http://https://7388r.csb.app/	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://7388r.csb.app/favicon.ico	0%	Avira URL Cloud	safe	
http://lib.tnua.edu.tw/goto/https://7388r.csb.app	0%	Avira URL Cloud	safe	
http://https://7388r.csb.app/?	0%	Avira URL Cloud	safe	
http://https://7388r.csb.app/$$$$$$inactive$$$	0%	Avira URL Cloud	safe	
http://https://7388r.csb.app/frame.html?_sw-precache=358bc62ccbd9155c9f01d203199f04daH	0%	Avira URL Cloud	safe	
http://https://csb.app/	0%	Avira URL Cloud	safe	
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.	0%	Avira URL Cloud	safe	
http://https://7388r.csb.app	0%	Avira URL Cloud	safe	
http://https://csb.app/o	0%	Avira URL Cloud	safe	
http://https://36cv9.csb.app/index.html	0%	Avira URL Cloud	safe	
http://https://7388r.csb.app/sandbox-service-worker.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d26p066pn2w0s0.cloudfront.net	143.204.11.11	true	false		high
codesandbox.io	104.18.22.207	true	false		high
prod-packager-packages.codesandbox.io	104.18.23.207	true	false		high
s3-r-w.us-east-2.amazonaws.com	52.219.100.16	true	false		high
googlehosted.l.googleusercontent.com	172.217.22.225	true	false		high
lib.tnua.edu.tw	203.71.172.211	true	false	• 1%, Virustotal, Browse	unknown
7388r.csb.app	104.18.27.114	true	false		unknown
col.csbops.io	148.251.96.176	true	false	• 0%, Virustotal, Browse	unknown
elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
logo.clearbit.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://7388r.csb.app/?#asdf@asdf.de	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com/index.html?auth=30%40ohixyzo80aNC4yMTIxXzIzNTgwNF8yNTQ1MzcuMDU4NTkwMDAwLCNGI1MjMTcxNDEjRQ%3D%3D%3Aver-UID=8c60cf39e11d1659051190bdc1f1a8a8#asdf@asdf.de	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high

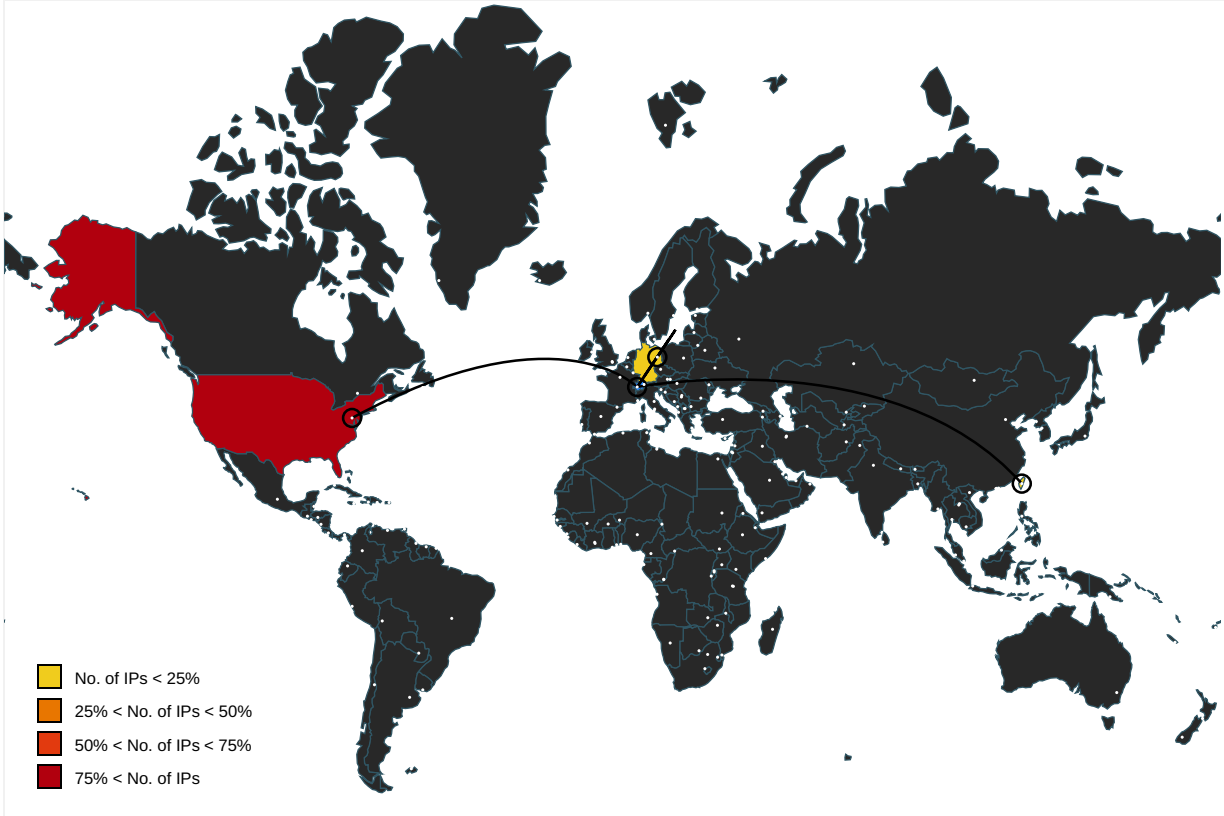
Name	Malicious	Antivirus Detection	Reputation
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com/index.html?auth=30%40ohixyzo80aNC4yMTIxXzIzNTgwNF8yNTQ1MzcuMDU4NTkwMDAwLCNGI1MjMTcxNDEjRQ%3D%3D%3Aver-UID=8c60cf39e11d1659051190bdc1f1a8a8#	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://lib.tnua.edu.tw/goto/https://7388r.csb.app	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com/index.html	000003.log3.0.dr, 184390d23e1bf4f4_0.0.dr	false		high
http://https://codesandbox.io/static/js/7.a39df6d6b.chunk.jsH	cb22034d7c8bc530_0.0.dr	false		high
http://https://7388r.csb.app/sandbox-service-worker.jsaD	2cc80dabc69f58b6_1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://csb.app/D	dbecaed5c01c2696_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://codesandbox.io/static/browserfs8/browserfs.min.js	9a84336bbf206ea2_0.0.dr	false		high
http://lib.tnua.edu.tw/goto/https://7388r.csb.app#asdf	History-journal.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://codesandbox.io/static/js/7.a39df6d6b.chunk.	000005.ldb.0.dr	false		high
http://https://codesandbox.io/static/js/76.c312409fb.chunk.jsH	134c91c98518603b_0.0.dr	false		high
http://https://codesandbox.io/static/js/72.2c983ea22.chunk.jso	000003.log3.0.dr	false		high
http://https://codesandbox.io/static/js/vendors~app~sandbox.3a7b80a48.chunk.js	bad56957642addd2_0.0.dr	false		high
http://https://codesandbox.io/static/js/72.2c983ea22.chunk.js	000003.log3.0.dr, 71155808921bfc20_0.0.dr	false		high
http://https://7388r.csb.app/0	000003.log4.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://7388r.csb.app/?#asdf	History-journal.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com	Current Session.0.dr	false		high
http://https://codesandbox.io/static/js/default~app~embed~sandbox.39603aef6.chunk.js	184390d23e1bf4f4_0.0.dr, dbecaed5c01c2696_0.0.dr	false		high
http://https://codesandbox.io/static/js/vendors~sandbox.ee783573a.chunk.js	24f0ea9236843cef_0.0.dr, 184390d23e1bf4f4_0.0.dr	false		high
http://https://csb.app/8	bad56957642addd2_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://codesandbox.io/static/js/common-sandbox.71780db40.chunk.js	edce4b4068efcfbc_0.0.dr, 184390d23e1bf4f4_0.0.dr	false		high
http://https://7388r.csb.app/frame.html?_sw-precache=358bc62ccbd9155c9f01d203199f04da	184390d23e1bf4f4_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com/0ridjsskfrivncxmssjf.ico	Favicons.0.dr	false		high
http://https://codesandbox.io/static/js/vendors~app~codemirror-editor~monaco-editor~sandbox.e68dd7bee.chunk	52567c5dc82a84ca_0.0.dr, 184390d23e1bf4f4_0.0.dr	false		high
http://https://code.jquery.com/jquery-3.3.1.min.js	17af122e5462afff_0.0.dr	false		high
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com/	Network Action Predictor.0.dr, 17af122e5462afff_0.0.dr	false		high
http://https://7388r.csb.app/$$$	index.txt.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://codesandbox.io/static/js/76.c312409fb.chunk.jsQDY	000003.log3.0.dr	false		high
http://https://csb.app/-	2b34a4a96b383c83_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://codesandbox.io/static/js/7.a39df6d6b.chunk.jsc#7	000003.log3.0.dr	false		high
http://https://7388r.csb.app/	000003.log4.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	29c850d9-9905-47ac-90ad-fa7859b5efa4.tmp.1.dr, c25ecedc-fdc1-4244-ad4b-ef66ded4d381.tmp.1.dr, cce6abd3-2504-455b-9fef-4752af18a5fa.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://codesandbox.io/static/js/watermark-button.d47e1de20.js	184390d23e1bf4f4_0.0.dr, 7238af54101ad45e_0.0.dr	false		high
http://https://7388r.csb.app/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com/0ridjsskfrivncxmssjf.ico%	Favicons.0.dr	false		high
http://https://7388r.csb.app/?	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://7388r.csb.app/$$$$$$inactive$$$	index.txt.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://codesandbox.io/static/js/sandbox.81e0de32a.js	184390d23e1bf4f4_0.0.dr	false		high
http://https://7388r.csb.app/frame.html?_sw-precache=358bc62ccbd9155c9f01d203199f04daH	184390d23e1bf4f4_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://codesandbox.io/static/js/7.a39df6d6b.chunk.jsm	000003.log3.0.dr	false		high
http://https://csb.app/	24f0ea9236843cef_0.0.dr, 7238af54101ad45e_0.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://codesandbox.io/static/js/76.c312409fb.chunk.js	000003.log3.0.dr, 7b92c1431104de88_0.0.dr	false		high
http://https://codesandbox.io/static/js/72.2c983ea22.chunk.jsY	000003.log3.0.dr	false		high
http://https://codesandbox.io/static/js/76.c312409fb.chunk.jsY	000003.log3.0.dr	false		high
http://https://codesandbox.io/static/js/7.a39df6d6b.chunk.js	2b34a4a96b383c83_0.0.dr	false		high
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.	000005.ldb.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://7388r.csb.app	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://codesandbox.io/static/js/7.a39df6d6b.chunk.jsX	000003.log3.0.dr	false		high
http://https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com/index.html?auth=30%40ohixyzo	History-journal.0.dr	false		high
http://https://prod-packager-packages.codesandbox.io/v2/packages/	ab425f50d67661ba_0.0.dr	false		high
http://https://clients2.googleusercontent.com	c25ecedc-fdc1-4244-ad4b-ef66ded4d381.tmp.1.dr	false		high
http://https://codesandbox.io/static/js/72.2c983ea22.chunk.jsH	02ffbff9939db27c_0.0.dr	false		high
http://https://codesandbox.io/static/js/76.c312409fb.chunk.jso	000003.log3.0.dr	false		high
http://https://codesandbox.io/static/js/sandbox-startup.81d8a90a0.js	1f763c5512ce4f99_0.0.dr, 184390d23e1bf4f4_0.0.dr	false		high
http://https://csb.app/o	7b92c1431104de88_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://new.codesandbox.io/frame.html	2cc80dabc69f58b6_1.0.dr	false		high
http://https://36cv9.csb.app/index.html	000003.log3.0.dr, 184390d23e1bf4f4_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://7388r.csb.app/sandbox-service-worker.js	000003.log4.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://codesandbox.io/static/js/vendors~app~embed~sandbox-startup.10f5f18b4.chunk.js	184390d23e1bf4f4_0.0.dr, 563dfe3e2ee44651_0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.71.172.211	unknown	Taiwan; Republic of China (ROC)		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
172.217.22.225	unknown	United States		15169	GOOGLEUS	false
104.18.27.114	unknown	United States		13335	CLOUDFLARENETUS	false
148.251.96.176	unknown	Germany		24940	HETZNER-ASDE	false
52.219.100.16	unknown	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.22.207	unknown	United States		13335	CLOUDFLARENETUS	false
143.204.11.11	unknown	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345054
Start date:	27.01.2021
Start time:	16:30:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://lib.tnua.edu.tw/goto/https://7388r.csb.app#asdf@asdf.de
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:	15
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:	mal76.phis.win@30/215@11/10
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 40.88.32.150, 216.58.207.174, 172.217.23.78, 172.217.20.237, 173.194.187.70, 173.194.188.234, 172.217.23.35, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 209.197.3.24, 72.247.178.41, 72.247.178.8, 172.217.23.10, 172.217.23.42, 172.217.23.74, 172.217.22.234, 216.58.207.138, 216.58.207.170, 172.217.20.234, 23.210.248.85, 51.104.144.132, 72.247.178.49, 72.247.178.32, 72.247.178.11, 72.247.178.35, 51.103.5.159, 95.101.22.224, 95.101.22.216, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, r1---sn-4g5e6nsk.gvt1.com, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, clients2.google.com, redirector.gvt1.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, dualstack.f3.shared.global.fastly.net, r5.sn-4g5ednsk.gvt1.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, displaycatalog.md.mp.microsoft.com.akadns.net, r1.sn-4g5e6nsk.gvt1.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, www.googleapis.com, r5---sn-4g5ednsk.gvt1.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, clients.l.google.com, par02p.wns.notify.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:31:38	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF 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\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....l.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....l.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..l..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0908522464605643
Encrypted:	false
SSDEEP:	6:kKUHbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:X3kPlE99SNxAhUeo+aKt
MD5:	58C4D4994B051B641386DA59DA792A74
SHA1:	908F5DAF2514C4D7A486DBDA11FEA5E08F61220A
SHA-256:	70B7207017912DC06D1DE261C500753F65C4F9FF782D1C08C6EBA761393C4D9C
SHA-512:	371933965D8EC3AAD6E4492514BAFE500E656B8CD55009F55B4E2D1BD6D54A8E09EB246D85DDC3F9E4A1EEF2A36879102F8C267A1D8932C04D492F2863BC426
Malicious:	false
Reputation:	low
Preview:	p..... .....L.....(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\24088231-11b8-44cb-bd3b-7ab43f0cce8b.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):	163495
Entropy (8bit):	6.081278271334301
Encrypted:	false
SSDEEP:	3072:owF2w0rBlQ96umxmsP6tttYVj4UnsFcbXafIB0u1GOJmA3iuRQ:T41lAumJe8U6aqfIlUOoSiuRQ
MD5:	F8F783863E2337C8086AF011D78BEB8D
SHA1:	E0BC79994F5ADDB84C3D59EAACEB9FFFC759B60E
SHA-256:	7A9BAC3E312E23881C7A7C0B8B3D851F89BE22A8DA1F8E9F6747E7860233043F
SHA-512:	1EC63C52E5299F46B6C556E3EC98504CCAEDA776FCF0B6010BA9ECE503448FB6B4323059B635331F0CC008B5583BA5F3F3DE01E09BEEFAB743130AB2E88FA2D4
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":1.611793893530551e+12,"network":1.611761495e+12,"ticks":99514022.0,"uncertainty":4527453.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\5ed046cb-c87a-4378-bba4-142d12427331.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):	163495
Entropy (8bit):	6.081280515637355
Encrypted:	false
SSDEEP:	3072:tre2w0rBlQ96umxmsP6tttYVj4UnsFcbXafIB0u1GOJmA3iuRQ:BD1lAumJe8U6aqfIlUOoSiuRQ
MD5:	E407A26C29D947DF9D33ECEE54A4DDD5
SHA1:	DE50A123BD94762CB5E8438DF63FD1EFA931D0D3
SHA-256:	2232FBB115753CA8C9FC3594712EA88E5C23C7E17CDF19B5803EF6D022371D0C
SHA-512:	86B74488F8BB1498204FD18D1F130D75B193E8732474E365CAE5EA09FFB512B49276718AA79E6CBBAF39903EF7072FF14FD5DA7A6E6CED02AE31D161C5857CC
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":1.611793893530551e+12,"network":1.611761495e+12,"ticks":99514022.0,"uncertainty":4527453.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016513249"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\6cc5e2c2-3a75-4c3a-9b3b-845e7e5afa7e.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):	163495

C:\Users\user\AppData\Local\Google\Chrome\User Data\6cc5e2c2-3a75-4c3a-9b3b-845e7e5afa7e.tmp	
Entropy (8bit):	6.081278281054912
Encrypted:	false
SSDEEP:	3072:o2o2w0rBlQ96umxmsP6tttYVj4UnsFcbXafIB0u1GOJmA3iuRQ:Fp1lAumJe8U6aqfIlUOoSiuRQ
MD5:	324A13D6EC9A11915DECAFA6BF08EC73
SHA1:	80950C938A559D906CEB73023A16369EDF824728
SHA-256:	B51171ED0C28E75EF0194220BC9381E73D32C3442A26BBA6038481F731DE69CE
SHA-512:	D1983EA8B3A0CE0A2B1745E3067CB1ABEE96F31B307AB06F95380AC0C8558F8B2C5F471AF45675456ADBA508EB8F1FFCB6EC51546C9F4EB1C57C0F2CCE9BFI 0C
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":1.611793893530551e+12,"network":1.611761495e+12,"ticks":99514022.0,"uncertainty":4527453.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr 2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1 vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+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\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\13a4e645-0175-4073-bb96-e9cd67b10f44.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2f1a7a5a-7baf-4b03-8268-d36fa57ee0c2.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):	5554
Entropy (8bit):	5.021916386899527
Encrypted:	false
SSDEEP:	96:n2wSF3Ax4pcVQFok9ylJCmRWL8Uk/S1lbOTQVuwn:n2jex4pcityl4mYBkq7
MD5:	26F5545E676FA93DDA19A0BDADB02CCE
SHA1:	F4B17DC09DBB814C2616AEB2985233F69D343A7A
SHA-256:	A2289D6694AE054AF91BACB81C073834C56B7D089DBB63D090FA2DB85C7AA5DF
SHA-512:	BA634A86E045FBA669839775593F534E529F9C177768962F4F5C5D9AA3115EA6B39AC27F851A16DBA102275A0F62A66CF1E888521D41E9EC666329D83D4CA5D1
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2f1a7a5a-7baf-4b03-8268-d36fa57ee0c2.tmp	
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256267490794827","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3ab124b5-02e9-4da4-b7cf-849eb294bc01.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):	1374
Entropy (8bit):	5.585758244599624
Encrypted:	false
SSDEEP:	24:YI6H0UhRPEsU99GsTG1KUegD6Uoikq/HeUeXby2qUeXvq7wU9B2RUenHQ:YI6UUhRPEsU9UseKUegeUoHqPeUer2Uh
MD5:	226A778304DA86EB6D9387562437F164
SHA1:	6D95DBEF52260C21B5B1267DFC8B2720C35AF9C5
SHA-256:	604F7405545D095EDE78D70C278A357A24DFF9B18D31778E1436B5DE1F788E86
SHA-512:	5992F3F46E08F2E84B143D87B7C1C7AFA8E6E5FCA0C66FD08EAAED2AC500378BBD6EC972F1D3BEE847CE70092E52F326D2B49085A91CD15E431EDEFA3444BI F8
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1643329895.747376,"host":"i6A/hZj+yPBpXgblNhsMP8nKhrhEwM3Q9CRGI6U7FiU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611793895.747379},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1643329895.097583,"host":"qaDeFdT1UTirY0OQe+c5LKw+zjx6vF/+3vFh7CgrAOY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611793895.097589},{"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_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5c72dd94-bf2d-48f6-b4eb-e130ac62a04f.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):	6418
Entropy (8bit):	5.226182409370279
Encrypted:	false
SSDEEP:	96:n2wSF7Ax4+ROiMwnjcVQFok9ylJCmRWL8Uk/S1uckzX2bOTQVuwn:n2j+x4+Rf5jcityl4mYBkqpkz0
MD5:	45672076D4F3CE2B90FACE0BF121B167
SHA1:	C6AF8CE573832C2078D14729BC463C089A475EE3
SHA-256:	B51A7C7C1323A028883EFCFABDF49E1584C093353C8C98A0A34E59C23F119BEF
SHA-512:	DB1B8135E8A2D3C3417CFFBEBF0E88D3D1DF68B7E51DDAD5FF7BFA801B1AD067CD50702CDAE50914C709F7CC58F3AC23C140D93863BCBCA8980990E366C8 B7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256267490794827","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9ffb5d1f-061a-420b-a849-e864a9b16ee6.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):	22465
Entropy (8bit):	5.538911129874348
Encrypted:	false
SSDEEP:	384:fvat5Ll2uXS1kXqKf/pUZNCgVLH2HfDgrU4HGfnTXVC4L1:gLlTS1kXqKf/pUZNCgVLH2HfsrUsGfnV
MD5:	B9EC56203AF2E69421E50009F74DEC4E
SHA1:	18C46A9C1730102E7B65FD97364A134B95CC7890
SHA-256:	D586143CC3CCB44F275683754F5B3F496B9AE58E5B28F2B4901040F6194A563D
SHA-512:	479AB1525C42F45DFCAC2EAEFA7377A3C8EB38738BC5EE61AE7EA5CE63A3CCC47B325114808F56EC84617003589D86B14362F50EDA94CFF9420F10C322F67A2 C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9ffb5d1f-061a-420b-a849-e864a9b16ee6.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":"13256267490512005","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.267766316421092
Encrypted:	false
SSDEEP:	6:m1+UoBt+q2PWXp+N23iKKdK9RXXTZIFUtpS+UoQ5ZmwPS+UoDVkwOWXp+N23iKKU:HfBova5Kk7XT2FUtp3fg/P3fJ5f5Kk73
MD5:	B0CBF91AE2CBD83389A672239327743F
SHA1:	347B1C3B9E187203194B78B67B983BF93030C99C
SHA-256:	2C1CDCB547E7D8E4F53189DD74852AD83F28F2D72DDA1FAB0C470141B897DA1B
SHA-512:	9C68D4D73F884CE42C401A31D48BF2A6ABFF10807516ECBAD714204D0D62E96546170C49288A1359653310DA050A2A12D6DCF434C1FB06F473DE4A207DE4E33
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:38.423 1bb8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/01/27-16:31:38.466 1bb8 Recovering log #3.2021/01/27-16:31:38.467 1bb8 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):	5.263871639418335
Encrypted:	false
SSDEEP:	6:m1+UoWlIHt+q2PWXp+N23iKKdKyDZIFUtpS+UoN5ZmwPS+UoNtVkwOWXp+N23iKA:HfRHova5Kk02FUtp3fv/P3f95f5KkWJ
MD5:	353620C9CD1D5A81E122C903D3A024D5
SHA1:	59DD6FE1BC3A6805C8901E3CA1005C47FCB705E8
SHA-256:	F070CAE82DB52703ED6DDFF5CF60979542BDF4CAB0DB2E00BF50C2F3CF9718B1
SHA-512:	9C268C35C75D24710FA8B038DF41DB8952CAD6AD1E0FD6260C531870EA8FBA56E9900A6C1C6017B27A7A1F4ACDCD95AB5867CE669CEE174FEE2A6E7191C7A18
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:38.391 1bb8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/01/27-16:31:38.405 1bb8 Recovering log #3.2021/01/27-16:31:38.405 1bb8 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\17af122e5462afff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	253
Entropy (8bit):	5.562109196605627
Encrypted:	false
SSDEEP:	6:mR9PYeSSIEGExZLiJPLjdvtgcbTcnCK4LNhK6t:G9ZLIvE3LKZPbTA4N7
MD5:	1E2A1EF870871EACF5B7881D8EAA7D3B
SHA1:	99FAE36602A9D1F015DD72F623CFE2D430332A67
SHA-256:	4F1829E67830FD47872837056C883E768E0514C08E85EA8D391A33146FDE2500
SHA-512:	9E98D2A61A8EB7D88E8C2D526B3F53E8F9D49C31B5C92A1BCE92A2E0613F346C6F4972C3090FA5A7A9D7E8E9D31A2F264F4D2473A4D87CD7F0FA4D8F4C8AD5D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....y....$....._keyhttps://code.jquery.com/jquery-3.3.1.min.js .https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com/.]SK../.....b.....E5...+=.V.c..m.|mpO....s.z2R...A..Eo.....K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f763c5512ce4f99_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f763c5512ce4f99_0	
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.473076019222375
Encrypted:	false
SSDEEP:	3:m+lxNcqOA8RzYP2D1HGLMkBGKuKDYdIWEi6ghK7Q/nu0+1t/lHCfW/69fnRzEOUT:msqYeD1+WEi6ea0+1tgfh9fnz/IDK6t
MD5:	ABA2998C55930A680FB3F285AEB4BF07
SHA1:	5ACE53403BA29C2FEBC635D87C850BF6273F2D9C
SHA-256:	9F27E95AEA9584320F1621F91EFE7F19BADB098C44A7E72BC0FEDAF9DB815587
SHA-512:	31AA9ECD839A1A6C8608CF0E7629939B6A824ED648F31DDB22129A0F9A5775446668BCC88C2BFD2A6746BC789660DE14F39C5B76F3EEC9CFB554AF4E9B4B14 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....._keyhttps://codesandbox.io/static/js/sandbox-startup.81d8a90a0.js .https://csb.app/...K../.....:.....aS.d...r.,..&{M.h...).A..Eo.....W.P.....A..E o.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\24f0ea9236843cef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.532720518546365
Encrypted:	false
SSDEEP:	3:m+lz7C8RzYP2D1HGLMkBGKuKKBXldLAkHDP6SRQ/0k41t/lHCWgOB173cof6RmUZ:ma7PYeD1xUDiSxk4tgXO3jcRA2K6t
MD5:	AAC49DCEFBBDC9A4ADA6802F9BB7DF61
SHA1:	B34C7EC734C80433AEE58779B3111674A0701714
SHA-256:	B70019D73B470CDFC69FAB005AE3333B00811CE612C312DD21A6B1BC62C8CD8B
SHA-512:	0738EB0ABE0B94E31A1B2A4BA249A422A4E1AD3E5A469E3C34B97A3EC551135B63FF0A0F6802E18D0AAAD99466AB75BFDE3B76C820AB0838ECCAFEC6358408 62
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y...-.I...._keyhttps://codesandbox.io/static/js/vendors~sandbox.ee783573a.chunk.js .https://csb.app/...K../.....\.Q..#.q..^?=....a.qZ..8....q..A..Eo.....o..... ...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2b34a4a96b383c83_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.4435345240366315
Encrypted:	false
SSDEEP:	3:m+lj6AOA8RzYP2D1HGLMkBGKuKSLEW0rRQ/yAp+1t/lHCyrst6uOSZOoRLF4kvgv:m9YeD1jL4c+1tg4ndSwkAg4K6t
MD5:	0D62DE75EE67F5CF94833E3B182878E2
SHA1:	B5C99A68B1D32E989198C6C704208DAE7925392B
SHA-256:	DE46E0FE55F481470523D7A142B0D277AC1AE63EC75B34557758EE180D5D483F
SHA-512:	3B3A4C80A79D1167C36E065C5BB3FDE935229FF7C7C5E61E531713925FB24856A0E9978F10E955AEA618DEDCC7EDC2ED2E080B32F81132C3420F699200F57D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K...]<O+...._keyhttps://codesandbox.io/static/js/7.a39df6d6b.chunk.js .https://csb.app/-.%K../.....v...P...G0R.....M.!..7..P/...A..Eo.....h.T.....A..Eo.... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\52567c5dc82a84ca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.516478988129655
Encrypted:	false
SSDEEP:	6:mOqnYeD1xe/sgMB/ykxvuvBSFkl1tgOy3uRZohyALPbK6t:4D/qAacQSor2rN
MD5:	317180366E6A799D58F93E436E420ECF
SHA1:	83B7515CB050D0F365D13948887B96E236C6C310
SHA-256:	A8FE6D84A6373B46EE06674F0F2160B0655113FABA494FDCC50E72E3FB59C006
SHA-512:	44C5961BFC2E932620AB11D7A9FF1859BF212F4CC275CAFC649DDA37700EC8C7911AFE41011B57087E8FD90672C7B4958E7ADF71AD4896D78CEB087B6501C9 D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\52567c5dc82a84ca_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}....z:T...._keyhttps://codesandbox.io/static/js/vendors~app~codemirror-editor~monaco-editor~sandbox.e68dd7bee.chunk.js .https://csb.app/..K../.....N.....MwT.-@q....Ks.3...y 2U...A..Eo....._./u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\563dfe3e2ee44651_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.539168011819969
Encrypted:	false
SSDEEP:	6:mUagEYeD1xSY/WEiWFSvtgXGl08V/6r/K6t:p8D/S3Cy9T2
MD5:	60E4B4E5D4DDA0DE8E381B5630473F86
SHA1:	6C3C53D76F6048AD6A9CCC77D07C80210E9A7D11
SHA-256:	7730628AF9A4F8FC5140A7E69287168590C0B9647544AAA6DDC299393BBD2ED9
SHA-512:	DA0F92D212E95869417FCBBE93D75032CC72F5DD21F31B78093B16A7666A428B58848528B4F3273BC8F1B276F109543C6C242B62C31660AB015F16A407F3AA14
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....._keyhttps://codesandbox.io/static/js/vendors~app~embed~sandbox-startup.10f5f18b4.chunk.js .https://csb.app/...K../.....2.....x.b.l...a...qS....w.....+b....A..Eo.....A.v.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\71155808921bfc20_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.525573643908135
Encrypted:	false
SSDEEP:	6:mFllXYeD1jX3ZUN6yJgTIaYdqO/fInK6t:kllBD5X3ezcLYdqO3Ip
MD5:	3FAA0617235D3842C84FF89710EA662A
SHA1:	34A4EFD39179DC711189A2E560C429F9ED55F14F
SHA-256:	8B6718EDF31FA503BD1059B6C6E230716453D0E909B1B0A0DB11803B8AE76E91
SHA-512:	75E99E166D8F8BF24B9AA63C550D7D03D1F505D96579D185AC41C6C58ACC2B053E3661BC796BB26D54BDE1E3CDCA11BA62006E6B469BE350D8124B552B4BFDDF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L...4by....._keyhttps://codesandbox.io/static/js/72.2c983ea22.chunk.js .https://csb.app/..&K../.....".C...=...X...h.?.1.8'.^..8..Q..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7238af54101ad45e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.530942393642843
Encrypted:	false
SSDEEP:	3:m+lUP+dA8RzYP2D1HGLMkBGKuK3NEXHH6eCvDQ/F41t/lHCJsWu5JZ32K+OvL9Wt:m+YeD1bnCk41tgJsWW32KxBhCtbK6t
MD5:	E52EBC719EB8B22DD5739B2C4440D1D8
SHA1:	8904F59B19C8D32D5DAFDCCDCD8CBD558E4D4BAE
SHA-256:	E426C80646FD9707BCAC76E98C12C818D2B15032F3C12355DA6B5B0F3257A6A2
SHA-512:	FC8FEF9E0353028C3DE4F906279D218698450373C619C1C2B8D0F7984B6A6170D81F1BFB7A6AAA3BD25307A004F5AB06D538AA9DBF102F3421E09E41BB96C508
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....V....._keyhttps://codesandbox.io/static/js/watermark-button.d47e1de20.js .https://csb.app/!..K../.....,.....^.<..7..e]E.z....S.J....+.E.R..A..Eo...../.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\787b4a320a9acceb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.505027280970312

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\787b4a320a9acceb_0	
Encrypted:	false
SSDEEP:	3:m+ljvllLA8RzYP2D1HGLMkBGKuKDYdLWwiINRQ/wvt/lHCOFtLb07jDbgoZqmNBI:mMYeD1cwHNntg4hGngSqmNQrTK6t
MD5:	969308CA93C877D42E9A580AE3E6069B
SHA1:	9447FF954DDB334B4FD00D7719A746A8DDC4165F
SHA-256:	7435C37F877ADB2A60CD0616DFBD1A19F2E593752D534F8FC2FC207E5BC1D1A9
SHA-512:	0E737AF00F96E79DE32D7B56DD98B537C7D9AD98900C8683ED999414ABAEDC67F926DDF994E391464B76B9A979B0A7C50D548FD3203BD39DEF0C93FFC1B1DA2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K....liB...._keyhttps://codesandbox.io/static/js/sandbox.81e0de32a.js .https://csb.app/...K../.....+.....P.(Q...&.kK....J;.S 7..6C.....A..Eo.....h.....A..Eo. .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b92c1431104de88_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.518795232685937
Encrypted:	false
SSDEEP:	3:m+lON/dA8RzYP2D1HGLMkBGKuKSTFUjURQ/KJApKt/lHCxrstrKGcVU682p5mBlR:mzYeD1jTFUYQKtgxQV968G4BlZK6t
MD5:	BADC79E0645BBBED7A6975BCC3DF842D
SHA1:	EF1053E0E7A49A92717BAF9D79EE92B7BE56DBD5
SHA-256:	417C973DB21398EDC0089B23E3E1426498933DA2DF332BB5E66917C8AEB20E06
SHA-512:	A3E4F9CEA4A55E8695A401FBE412CD8B0C43AF50989567B099E7C2222D9828EFC7F4A8033BFB8E7F1A5705ED067A10ED0F33DF62202A05C750ECEA0C1AA0927A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....._keyhttps://codesandbox.io/static/js/76.c312409fb.chunk.js .https://csb.app/o,%K../.....v...>.2.....q.k...r0....6.0...A..Eo.....]..E.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9a84336bbf206ea2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.423768992417833
Encrypted:	false
SSDEEP:	3:m+lXGoit08RzYP2D1HGLMkBGK3KcFVdML7WFvDQ/+EuUt/lHCNDDSfcoQ8kH5mn4:mbYeD1YKFL7HuUtgcfcik4nkRK6t
MD5:	344868C3AB969E70D33F1E4A9D42F96F
SHA1:	B51020296B990B8E1C82247C43A6C0EE4B3B5333
SHA-256:	01FEB053D0D78B157C1DD832D0891F32034B132D90F2D8AD81B0373D59B054E3
SHA-512:	9CBBF6166E6C3B0186175F6C1DB2276D4F9B4B0AA1630B56D013C37A381D28FC7FD76FC3AF9FAAEEB93CDCBE0E7F321404533224F19AD95807988B5A0280537
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....#M....._keyhttps://codesandbox.io/static/browserfs8/browserfs.min.js .https://csb.app/...K../.....K.....E;...0..Jw..(.<.Vb!.{.W^.!.3…A..Eo.....^.....A..Eo .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bad56957642addd2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.503465201332362
Encrypted:	false
SSDEEP:	3:m+lFecat08RzYP2D1HGLMkBGKuKKBX1dLDSoJGNeOSRQ/Cu7t/lHCZeFau6UOqgO:mOatVYeD1xyuGzSOtgZ9uJYcbK6t
MD5:	332E851B7AA39DD4F5CF926443B728CB
SHA1:	30D1631A0D72858AC454352ACE1CB3AFFBE95133
SHA-256:	CC1560D2125A09DFB0A2B695430670CCB58B7B1F5EF0987E173FB1804DC9878A
SHA-512:	24676D1764491A26B2DBA5AA0F06215C3C906D9E6DABFA8B6FE90CC96FD1AEBFC243209B3438F42C1E127AE9144E4B7573B04F4835015BE523E390C0A982891
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...-.y?...._keyhttps://codesandbox.io/static/js/vendors~app~sandbox.3a7b80a48.chunk.js .https://csb.app/8..K../.....m.....*...$=.Q,..6...#...l.../3r...A..Eo.....r i.M.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dbecaed5c01c2696_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.532276896802736
Encrypted:	false
SSDEEP:	6:mYvXYeD11N6YWcPPNg1tgnO/H8lG4K4WK6t:FDYCPlgSO/clG4U
MD5:	4ED36DD4F34BFA21185C733985A34C64
SHA1:	E3ED509B4EB3632FB70CD1B153F3EDBDCB703893
SHA-256:	22780F3FAACB5719F2C59B10C070F6EAC330136EA31450D2C22FB72CC81CDE58
SHA-512:	91AAA14BCE9828B908D6BD87A8971D7110935BA224022375E0B71CB9368C2ED69EAC90758901BA59C33BB2B5523E0299F03618DA98B9B80D3ED7C83A47021F7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...yVk....._keyhttps://codesandbox.io/static/js/default~app~embed~sandbox.39603aef6.chunk.js .https://csb.app/D..K../.....`.=.....g..h.....A. .Eo.....y.m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\edce4b4068efcfbc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.537717697582443
Encrypted:	false
SSDEEP:	3:m+l3TtLA8RzYP2D1HGLMkBGKuKdAHENGLZN0RQ/l0Kvt/lHClJPYB0lByRmEpK5M:mwDYeD1QCN0WtgIqWBGK6t
MD5:	CA8782100D8793AC611CBA65619015F2
SHA1:	429EA986E6230E35DD69DECE26FF606BE7894585
SHA-256:	3C06048D5F4984A2AA2E0622C5190A40544ADE2BBCFC75696E5266C0903648E8
SHA-512:	8376A5514D0726C6A25E304034353AA2E01A0CA869B4BCAFF78F9B0E897ABEEA4424445AA9BE094A22F053C812397C96F7A1C0DAE6DD687093D850B2D732247
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X....Or....._keyhttps://codesandbox.io/static/js/common-sandbox.71780db40.chunk.js .https://csb.app/...K../.....I.....KI..MO52..M.....{....I.zh...Y.A..Eo.... ..&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	576
Entropy (8bit):	5.04598567939753
Encrypted:	false
SSDEEP:	6:SBlL1lSo3nrmmQoUEsd1sgtscF/N4DsGW2Tf0m6tsH64zQ3zbn3pHkQ+IRwH6:SjB0o3YzdUWrmGgPzyz7V4h6
MD5:	016D1E7D77913FF2791B3A91D7DABF74
SHA1:	3CE83475F2CFD2658131E1AD9AE98466320E9D75
SHA-256:	1527D16A54064F7CF41F85D7D86B6DF50F8608EDBB578F473ECC014A5B639CAD
SHA-512:	BE7B6160215318151361736CF84D33E38152F17D6835A16F78BB77E9205D891E2815EB6522112CA3C4DF3B38D9ABCA6B30961686804AAF290E4FDFF04D5D648E
Malicious:	false
Reputation:	low
Preview:	8.....1.oy retne.....(.....bT.....PSK../..... ....X.q..%K../.....<8k..4+..%K../.....C..{..%K../.....^...T.8r...K../.....2J{x...K../.....&.....K../.....<.6...$...K../ .....*dWi....K../.....h@K....K../.....*.]|VR...K../.....n .k3.....K../.....O..U<v....K../.....QF..>.=V...K../.....^}.Np..@ikt../.....-..0..x@ikt../.....3.KPu../..... .....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q....._KPu../.....+<P|...X.KPu../.....TK../.

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:	modified
Size (bytes):	12288
Entropy (8bit):	1.1279619705008923
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06Uwrtr5Au8jGDgAZOZD/Fc:TekLLOpEO5J/Kn7U3GDNOZG
MD5:	8ADBC07F51E2B4221B1D2EE6173103CA
SHA1:	82B869EA56D522F9505941737DC8BAC036C3B5C2
SHA-256:	80ADE94386E05465356775B7239F5B35615FC35B2AEC72B3EC62182C5D744B32
SHA-512:	DBC1478915F8576C5F2B98867A7BF374269AC77769AE84EB73689373A2229F9D6BFA411F62948059142281638B7E8B5AB784F23DFCBB9F3D1C64CC695A4381C1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
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):	0.9673777983700576
Encrypted:	false
SSDEEP:	24:ocLgAZOZD/o98qLbJLbXaFpEO5bNmISHn06UwO8:o8NOZo8q5LLOpEO5J/Kn7Ud8
MD5:	2158037BDADECEF0952F331F691E6EC2
SHA1:	33A3DFA667269A6A824214E0B653E398C91CB31F
SHA-256:	FCFFF5989485C6AD3D6449DD6E54B29B5B89FB58B8C4F5E1E8C7A89CCA13EFB8
SHA-512:	C2252239D3FF7C83CD24B6935ACCDA24DCBA4FD8558171F2C336B5FC1A3395C797B9BEF9A138C869F4AA75A7F873C1AA90206366691ED83EE51F3723E70A3D2
Malicious:	false
Reputation:	low
Preview:	....

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):	7498
Entropy (8bit):	4.081784283773468
Encrypted:	false
SSDEEP:	192:3pnY3h0TNSLZ3hcTNS33h3NSv3hD3h3NSv3hu:5nY3mNSLZ3eNS33lNSv3d3lNSv3c
MD5:	6D471870802B7C8DDB1E91DFCE73C605
SHA1:	16E45DB2EBD0E8AF7EBC613C4BAE9C064950E701
SHA-256:	C56B0AED33D3768CE8DCF0D674F1185A88503B37BBDA01B2F44FD67E5E9AF099
SHA-512:	2A636C6B24A7D745072209EE16A79B4B9CA241E0B8297973691FAB9E52CCF3EED408C3F821B8D7E380367FE447BC423350A7D2088859E2C4E0212114B22C5D5D
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...58c18390_0b9d_4ca0_8ff1_eb76a9cc31e1..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....Q..L.....$...https://7388r.csb.app/?#asdf@asdf.de....S.i.g.n. .i.n.t.o. .y.o.u.r. .a.c.c.o.u.n.t.\...X.....P.....h.....`.....x.....y.....P...$...h.t.t.p.s.:./.7.3.8.8.r...c.s .b...a.p.p./.?.#.a.s.d.f.@.a.s.d.f...d.e.....8.....0.....8..... .....h.....`..... .....z.....{.....(.....@.....@.....a

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..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):	320
Entropy (8bit):	5.2283618897898485
Encrypted:	false
SSDEEP:	6:m1+UwUq2PWXp+N23iKKdK8aPrqIFUtpS+UwDGZmwPS+UwESVFzkwOWXp+N23iKKV:H3Uva5KkL3FUtp33i/P33ES75f5KkQJ
MD5:	A30FE0D91CD834277D61F111403954E5
SHA1:	8994C8C2EB94056F72F0213EB74F493BFCE0CBC9
SHA-256:	C24EA2407353B44563DE1ED03A518861FFDD3778A627F58D95DCEFCC55231FB2
SHA-512:	52EAA598311A68AD69A3D559937B4A8F651089D71245625629ACE8FC605BB108AC7145C3441E5FF89796E7C537284FC6217823AAF7C942DD603E768440326B66
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:30.806 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/01/27-16:31:30.807 15b0 Recovering log #3.2021/01/27-16:31:30.808 15b0 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):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.f.5.................................f.5................f.5................f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.235474454005355
Encrypted:	false
SSDEEP:	6:m1+UWcyIq2PWXp+N23iKKdK8NIFUtpS+UWcRShZmwPS+UWcOkwOWXp+N23iKKdK2:HeyIva5KkpFUtp3eRSh/P3eO5f5KkqJ
MD5:	AC5F6442B1B1112F57106BD55149F1CB
SHA1:	0F2D4B6EE31045069668291BF31E4EC4A0920208
SHA-256:	94DD456332196C6A8652B5EADC8D3E3938DA9EC96F22F364A96C6D9DD373C2F1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
SHA-512:	B2471BD8D44732035ACE28963B6F0DB8CEE6D2ABD41FC46A99F0301D4ECA30B9AE04CB21FDDE92A5AFCDBD4CC0B4536B19A9FB36F23C749B0AFB58A284FED8AD
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:32.923 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/01/27-16:31:32.925 15b0 Recovering log #3.2021/01/27-16:31:32.927 15b0 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\1.0.0.5_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):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49C
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2l/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

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:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","hqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+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):	26624
Entropy (8bit):	2.2697165873531224
Encrypted:	false
SSDEEP:	192:mF3hZX3hyMAmy8uoME4tq3hI3h+3hF3h0:s3/X3IMRRmtq3K3o3X3C
MD5:	8718596C87C1EB7075F7FA59AF28E328
SHA1:	66E1EB670D7A0084C3304FAA2E42892CBFCA4A88
SHA-256:	0FE523B52BE904EDEB20B28D54864F5437F23638A6FF2FB441A9AE2E280A7AC3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
SHA-512:	7EDE13BF618331E28B1EB81CC6144CA6D4F4A85166B6AE8DA116A1265372D361227C08614804E9F2B63145F25FD1753A2AA1108DCBD3C73D0AB089F29B31529(
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):	23664
Entropy (8bit):	0.9195664702825315
Encrypted:	false
SSDEEP:	48:QKdBmw6fUE3Kc/ZsP8Ww3tw00tT+8Ww3tw00PhKzKt8:QKdBC8En3hqn3hh
MD5:	D58B69D9D4D00FED7EF4ADF5DBD97E6A
SHA1:	ACC9C567DBFF3487FD3CDB423C28343723F84A70
SHA-256:	355B8F9F6CA68135925D8A44433767E325978C542E8E647F1A8CF6434FD786A0
SHA-512:	E10D9D1313B4A1F93E2254E19EE01ACC10BEC443E778FE96207436D633CE6EC8B01C033DF843C3F5F5E4497E404D3FD3C031F15CEBDD3D87418F5FC6961F33
Malicious:	false
Reputation:	low
Preview:	.....?.p..... ....

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):	5.275583181525342
Encrypted:	false
SSDEEP:	6:m1+Utpt+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpS+Utj9XZmwPS+UtOVkwOWXp+D:Hkpova5KkTXfchI3FUtp3kj9X/P3k+5M
MD5:	C3AFC991C3F8DAC3FD5C6D04F4D9E5FC
SHA1:	D904EFB02432934CA027DE0EE922F59E19E8EA1F
SHA-256:	E38A2EC234EA96D85C54FD4144533EE6B3077FE6A4934A0900621A5667326578
SHA-512:	C9C4A587C0CCF3A4CAF8770C099DF98C1B34591116BCEA9E69EA5E69CAAEFAAA4ED45CE7DC092B3335B10EEDDFC809BBA57A7B612665BE0750E33207BFED D2C7
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:37.074 1bb8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/01/27-16:31:37.076 1bb8 Recovering log #3.2021/01/27-16:31:37.077 1bb8 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.279430715729372
Encrypted:	false
SSDEEP:	6:m1+UtHN+q2PWXp+N23iKKdK25+XuoIFUtpS+UtCZmwPS+UtFMHNVkwOWXp+N23iM:Hkova5KkTXYFUtp3kC/P3kWT5f5KkTXp
MD5:	55E9645E9521A6239B760F78BB0342AB
SHA1:	C98C89B271D0DBAB2AA7E69826771DF58EB613AD
SHA-256:	5774414AF2461E622294C5B2CBBE7A85996B03FD5D60AB5481AEAE77820AC298
SHA-512:	9D693F5C934016AD57D779732A8ADACDDA83153FCE90DEB75C3057FC2CA2468FB8EBBB5094EDF1D51FB7DEA6DD0342ECFD1821049FE7776CCA6A8A8C2DCB B4E
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:37.054 1bb8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/01/27-16:31:37.059 1bb8 Recovering log #3.2021/01/27-16:31:37.060 1bb8 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
Entropy (8bit):	5.330702634681326
Encrypted:	false
SSDEEP:	6:m1+UqCd3+q2PWXp+N23iKKdKWT5g1IdqIFUtpS+UqQZmwPS+UqIINVkwOWXp+N2z:HIdOva5Kkg5gSRFUtp3C/P3zz5f5Kkgk
MD5:	42E8A69C49D64D400612B895B1F931FA
SHA1:	C8885856747D5CD97FC94967D43108392C0C7B71
SHA-256:	3E7AD8EF743AE89313DAEB7CCA9AB3BDA5D7E8A413C1D8E21044C94C34A50018
SHA-512:	C3DB550AF8703EDC8A1F88D27DF5E7F2FC4FA38A050C784CFA1882621F01833C1E11DB1C3712659BF48E68A71176573A9AF514BE766D14F3D9AF855F30097B4E
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:36.792 1bb8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/01/27-16:31:36.794 1bb8 Recovering log #3.2021/01/27-16:31:36.795 1bb8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\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):	81920
Entropy (8bit):	0.5111231565428105
Encrypted:	false
SSDEEP:	192:Y3hLA2R3hxc3hS3hB2QE3hF3hl3ho3hB20U:Y3VF3l3s3y3X3z3y3c
MD5:	214416EF768B0A91CC49C11C75E94056
SHA1:	D1F0893CF3A43B66EF6EF737D8AE3F88A71F6013
SHA-256:	4402240F1A9D6828427C6AE6EBC00ED0E1E04F18DDED784DF0C435B5363028EC
SHA-512:	1FDB990F5ED24AD2D82BA417A2E9A64A565E174DF21944C47C264E0B5A8AE751F6678BE8E8E0D174970603169FEF930B64FD4F57B08E41677188187E8580D585
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):	2112
Entropy (8bit):	5.9352778751676665
Encrypted:	false
SSDEEP:	48:A5w095fw05YMM/KLpM7ilGZLmiHsb9P5d+fsHzw8Ww3tw00bNmWB:A1vLiMNtAilGZ6iHsb9P5vvn3hi
MD5:	F27055AFA34BCC0AA17D40284499A38E
SHA1:	AAC6B23A11FC18B6D85147CD54FAEB8069C0E2B9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
SHA-256:	B7BB742E64D17A7E256ED6BBFF1972A93B72DF02B2C27FABA62703E9E71D1027
SHA-512:	7CDF77800D8D385C6627E12B48FB4DAF35E2E1137EA0A70BC49EAEEE2EC546F2CD1102B31D2917DF280F2515AFC31B917979E9849596D7D6FA656672BFDB31A1
Malicious:	false
Reputation:	low
Preview:	.....".."..2..30. 8c60cf39e11d1659051190bdc1f1a8a8..95newbeie..amazonaws..asdf..auth..com..de..east..elasticbeanstalk..html..https..in..index..log.Dohixyzo80anc4ymtixxziztngwnf8yntq1mzcumdu4ntkwmdawlcngi1mjmtcxndejrq..s3..uid..us..ver..7388r..account..app..csb..edu..goto..http..into..lib..sign..tnua..tw..your*..."....2.....30.....7388r...$. 8c60cf39e11d1659051190bdc1f1a8a8.....95newbeie.....account.....amazonaws.....app.....asdf.....auth.....com.....csb.....de.....east.....edu.....elasticbeanstalk.....goto.....html.....http.....https.....in.....index.....into.....lib.....log...H.Dohixyzo80anc4ymtixxziztngwnf8yntq1mzcumdu4ntkwmdawlcngi1mjmtcxndejrq.....s3.....sign.....tnua.....tw. ....uid.....us.....ver.....your.!2...$.....0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....

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):	83652
Entropy (8bit):	0.32354878706769297
Encrypted:	false
SSDEEP:	48:aqk3m8Ww3tw00tTfb48Ww3tw00XhoqQun2atfd9v8Ww3tw098Ww3tw00XhoV7RIl:aFn3hEn3hEEun2an9kn3hyn3hEq6n20
MD5:	8BE224B772ACA680BC33F9A11F528866
SHA1:	3828576582CF25884A542C30CE408D24F0851D7E
SHA-256:	B3CA61FB892765C0A0F438428A92DB48E6BBA6966E07C4BC1B76E3D875C29D06
SHA-512:	EFD96FD8383B70A9FFAA60ADD53EFAF094536E0F36E600997F3A4048B28120EA0D47ED35EB0272B65BB2CD1765921E9ECE9782ABF5CA6BC0B0F483E889B2E46
Malicious:	false
Reputation:	low
Preview:	.....9..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_7388r.csb.app_0.indexeddb.leveldb\000001.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//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_7388r.csb.app_0.indexeddb.leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13890
Entropy (8bit):	4.9560870638067644
Encrypted:	false
SSDEEP:	192:v2paSDB8mO3hmQhL2iGJuHjfmoqtIy4OjUKwKZZWsCU9U:Rf3v06mLIy4iUKwKZq
MD5:	0871AED94DC9586EE0340B0CE565D85E
SHA1:	E57F225A3E720F7B62A41320AE4A0A58C501598F
SHA-256:	0B0AC2619501E97496621B5DFBEBB846924A87A775C5F69928F8D6BB3B786E61
SHA-512:	736A724133A33C887B9FB9A0C5EEC1BB87875D979DAF809B56208E4F775D855CA05C5031CCCB7562050CCF33AEEA635A3FE1B10B8D434C9A236821D43F0DAB4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_7388r.csb.app_0.indexeddb.leveldb\000003.log	
Preview:	. .....2....(.o".....W..#|.....Q.....h.t.t.p.s._.7.3.8.8.r...c.s.b...a.p.p._.0.@.1..C.o.d.e.S.a.n.d.b.o.x.A.p.p.....`U..... .....0".OV.....2.....2.....1.....2....s.a.n.d.b.o.x.e.s.....2.....2.....2.....2.....2.....2.....2.....2..... ....s.a.n.d.b.o.x.e.s.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2.....2. .....2.....2.....2.....2.....s.a.n.d.b.o.x.e.sJ...n.. .....2..@.l.o.c.a.l.-.f.o.r.a.g.e.-.d.e.t.e.c.t.-.b.l.o.b.-.s.u.p.p.o.r.t.....2.....2..... .2.....2.....2.....2.....2.....F..... .l.o.c.a.l

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_7388r.csb.app_0.indexeddb.leveldb\000005.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6826
Entropy (8bit):	6.50544253268373
Encrypted:	false
SSDEEP:	96:t9m97tmD7LRdcrcNJE9SjySs5OKitGYg3FyZp/9taV2+BZq74SG2ZxrlO5/qIFbz:t9ooLR2ANABGy3FCp/9toLA74S2Fjbz
MD5:	37CD013776B86D03AC1BB9C49FD3548A
SHA1:	DC3C4EAC319042AD07EC41BE48628FF79601D615
SHA-256:	31B5C15947F6524437F08BE7BC9BE730FB59C6F059298647FC151AEF91FCA8A8
SHA-512:	1458495D9399F1DF93ECE819A76929F1703F27F3B0BBB6B18083C8636729EAEF1FBED4721383C82E481D40A3508C504B3D5F03C72DA308702A79B12B128E664B
Malicious:	false
Reputation:	low
Preview:	. ...K.....(.....2...l.....J.!....*.....9.p.....P..29....9.....$.9.....B...^9...(...$...&..-....>.....(....2.....j....2j...:j.-..j...j.....N..... .....2c...5.....$.9.....B...^9.:..-.....N.c.....B....c..c...-..c...Y...B....c..c.....5.X...J.4....H.F.... .l.o.c.a.l.-.f.o.r.a.g.e.-.d.e.t.e.c.t.-.b..*(b.-.s.u.p.p.,.t...R.2.p...6.... ....3..@.....2.....7...".2..".....8...".1..".....9...".0..".....:...".../...".....;...".....".....<...".-..".....=...",...".F.....>.&.....+.....l.....T...?.....#d...s.a.n.d.b.o.x.e.s.....@.(..... .....!u...A..."....."!u...B....."!u...C..."....."!u...D..."....."!u...E..."....".F1....F.&.1In.1!0...G."....S.....H.....-u.....l..!....1.....qP...q.!.,.o.....].d...O...r...#.n...#lZ.s...#.m.. .#.....t...#.l...#Y\.....u.'.....k.....,2.....v.....e.....%....s.te..eEV.w. !{.d..%Y..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_7388r.csb.app_0.indexeddb.leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.354208874405598
Encrypted:	false
SSDEEP:	12:HLRva5KkXQiFUtp3uZjIf0P3ucfC3uBN3usXoT:HLda5KkgWgtuT/uRuBZuX
MD5:	438FDF3ABE8535AEC062AE657FD614F7
SHA1:	7C921BE1145C83EE38F1F0E3DEC16490A10A3B23
SHA-256:	B8DAFA7EDAB7F14D2864B6470E3FDED2854BAE7F433139797663149E383B6677
SHA-512:	4AA494A11F1C8E8006D0B9F1596F9229AF2F2B0DF4294ADFA1F789F1C6F5F3F57C46D3159447CCAE7AAD3F2ABD64A013AF794DEDCCAA64EF97D4E48034B28D 4C
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:34.701 d14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_7388r.csb.app_0.indexeddb.lev eldb/MANIFEST-000001.2021/01/27-16:31:42.773 1c94 Level-0 table #5: started.2021/01/27-16:31:42.780 1c94 Level-0 table #5: 6826 bytes OK.2021/01/27-16:31:42.782 1c94 Delete type=0 #3.2021/01/27-16:31:42.783 1c94 Manual compaction at level-0 from (begin) .. (end); will stop at (end).

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_7388r.csb.app_0.indexeddb.leveldb\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	4.171019677784281
Encrypted:	false
SSDEEP:	3:Fdb+4L4whFActdDe+p3N8YE0LxlylLRlERMzWlt3L3PslA6XlKlNlw4plzlX:Z/HKYE0yZYRM6njsa6gl3jzlX
MD5:	0CD174437BFECC35D4C02C60D7FA9631
SHA1:	C8F358E9BD4B62D7941F78760EAF99C4360737CD
SHA-256:	2CFCAAD01B89DE8EDEE3F07EFBA489B2F2B210555543BF2603185B3AA669B12C
SHA-512:	165F9458B465E03E4A21FE8954CB00689829E821E4FA47880889F0835AA0F3CC47AFB3A443BADAA0CFB16E9A20FB1C5FC9F80EFF3EE411E4350FCF00FD250B5
Malicious:	false
Reputation:	low
Preview:	.....idb_cmp1.....w.3.....5.....-qftwB..6.h.t.t.p.s.:././.c.o.d.e.s.a.n.d.b.o.x...i.o./.s.t.a.t.i.c./.j.s./.7.2...2.c.9.8.3.e.a.2.2...c.h.u.n.k...j.s.....

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:	DOS executable (COM, 0x8C-variant)
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Size (bytes):	3085
Entropy (8bit):	5.52249302652893
Encrypted:	false
SSDEEP:	48:y0ZXGwua7QM78dbGzDZbQSefgGiNrS0U9RdiN97g:16a7QMIdbGzDZbQ5fgGurS0Vg
MD5:	93DB686F9DFD1EC262A99A091CF65AF8
SHA1:	778F014625C73F30B99C656DC4306E7B421A5103
SHA-256:	027949EDC8BA3B7B8B778CD6014EA8AC8C431D069F38DB920CC4D3FE1D8BDA95
SHA-512:	44D279FA95D7D3BBAC708A45D6705EE8F6FD5432BFBA31F3C83BFC322C2A8DD2034E1196226E519661669CDC07811C18996087211CF2409C80F281D8E665EC9
Malicious:	false
Reputation:	low
Preview:	.(..{..*.....META:https://7388r.csb.app..... _https://7388r.csb.app..__test__....._https://7388r.csb.app..running..H7...-.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..286122000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-01-27 16:31:40.66][INFO][mr.Init] MR instance ID: ed29d32c-ea21-40ea-8630-d29256e09dae\n","[2021-01-27 16:31:40.66][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-01-27 16:31:40.66][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-01-27 16:31:40.67][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-01-27 16:31:40.67][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other c

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):	332
Entropy (8bit):	5.234347730344916
Encrypted:	false
SSDEEP:	6:m1+UwbQL+q2PWXp+N23iKKdK8a2jMGIFUtpS+UwnnG1ZmwPS+UwFQLVkwOWXp+Nt:H3pva5Kk8EFUtp33G1/P33O5f5Kk8bJ
MD5:	44B3332806F0A534CBBC04A8688E6560
SHA1:	9BF91D628667CAD5B00825B4FA881AD921287E83
SHA-256:	2E11DD54E11A689C7740EE0EA1E5149B328205C1BC1E5A33B9F4E802D0D519D8
SHA-512:	AF46EEED1591D2AB878B10C7167C1D4E2F37760E9DBC23A53CAD82116762B828C8AD56AB41E925CCAA25840A6177BD54706E55C0CC6271AE54162E7F0DDB77D
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:30.560 1478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/01/27-16:31:30.564 1478 Recovering log #3.2021/01/27-16:31:30.584 1478 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):	24576
Entropy (8bit):	1.2528272663459952
Encrypted:	false
SSDEEP:	48:Trw/qALihje9kqL42WOT/QUTbw/qALihje9kqL42WOT/VnJB:vOqAuhjspnWOkgOqAuhjspnWOdJB
MD5:	0EC709F0EFF4D5CE8F17AD30B1BAF4A8
SHA1:	F4F2162F5C380A98BA0B9315F7E44469F507BD46
SHA-256:	855E0690B4504E5BEED7944520AD1BC28F652C431640AFFD9B2D294E34466245
SHA-512:	18BDA5A0FD9128065FCC099691E584ED543968D15D0C5C0FA407E7E70CA978C32EFD3FE4697727FA661F7FB08F61CAC75DBAB1FC1988DFE53F0748378D69EB5
Malicious:	false
Reputation:	low
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):	25672
Entropy (8bit):	1.021046363256649
Encrypted:	false
SSDEEP:	48:RQq7w/qALihje9kqL42WOT/3cqrw/qALihje9kqL42WOT/c8:RQUOqAuhjspnWOAkOqAuhjspnWOr
MD5:	291D126EB79078DABF84A5AAE8CCC6BE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
SHA1:	58153AE63A6412E9905C3B17175712C44A995A15
SHA-256:	8459962315AFA6E7695C724767F7F179711CBB0A7E3F4CC793E1C568E5C74383
SHA-512:	352DAFD6A993369917E0E180F94A2EF3EE57741A6CF9EEBDFF8289721761DD80ED5EB8435FFF320FC6FAB78C03033F37A98DE7F200359E57A3FA3A4458CC205
Malicious:	false
Reputation:	low
Preview:	....

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):	334
Entropy (8bit):	5.253563842549547
Encrypted:	false
SSDEEP:	6:m1+UwNIq2PWXp+N23iKKdKgXz4rRIFUtpS+UwSjZmwPS+UwSUfPzkwOWXp+N23iE:H3mva5KkgXiuFUtp33m/P33nXz5f5Kkt
MD5:	A2962EB1AC72CABB6AC4C8C979D64E96
SHA1:	6D4B9D29869AC41DE5D625A8D845DA42D0620A40
SHA-256:	C5E654E40FDF7AF18ED869830CD0858456ACDC8A7C3632B6D23BA5EAFE9C1FBB
SHA-512:	CCB33136045AB6328EB38F67FFD78353D36951ABDAC08E1FD86729E9079C7A70820190394E4A3FF7478A69AF70D0E9E143C4E2511D5D2D340528BC91AA67D78
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:30.848 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/01/27-16:31:30.850 15b0 Recovering log #3.2021/01/27-16:31:30.851 15b0 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\QuotaManager	
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):	77824
Entropy (8bit):	0.47947898922287074
Encrypted:	false
SSDEEP:	96:vCIG+6bDdsDaBJvtHIm50I4sX/CIG+6bDdsDaBJvtHIm50I4pWw:a96EJTv4sXK96EJTv48w
MD5:	F14B55DE007A7741A2961C79FC29B540
SHA1:	511228943B9C9D3A694405500E427BFA0E0A3996
SHA-256:	CA9BB635478844F1FD40EE1692D167F44EA95CE7146766F173025548123495E8
SHA-512:	3D5E40DCAAD1A926C1636257238475EA30C16EAEE5F750D131E3C78F9B27A12C1816AC5A7C6357118B4DE6D9DDE7F4FA6BED711636B5A7A352BE091E82B869 5
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g.....*.W.L.[....."..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	0.6543266608038137
Encrypted:	false
SSDEEP:	48:nMnUqzLbCIG+6bDdsDaKgJgKtHIm50I9a+UU5:nmUsCIG+6bDdsDaBJvtHIm50I40
MD5:	BCFACA6FE544AFC941201AA1EF75DE27
SHA1:	17A673B8C8989336CBECEFD22AB856CAE1A88AB3
SHA-256:	311032F2E467BA19ABE9CC4D33E82517B8B1A1CDA015CFC52DEE13FFA1F3E232
SHA-512:	ECD4F30A57FE8CE5995FDBB84E5F5EADD6940ECE3489E0A39AC6A54CD8F53D890538813F707BD7C7534AD21600E43489034960274FDC90257588F58D65FD297
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager-journal	
Preview:	.....c..... ..... .c.....z.j ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\65f01577-c1a0-4567-b7fb-a01c7243529c\index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	3:m+l:m
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CE 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\65f01577-c1a0-4567-b7fb-a01c7243529c\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	2.9972243200613975
Encrypted:	false
SSDEEP:	3:3+1jEhX4:O1who
MD5:	6F8CB7D51DB98D2EE09A35ED0592C3D3
SHA1:	B105E771EF13144D41F07728527FB32B8C2ACF6C
SHA-256:	28032EA04CD7D6D4A58E2E4CFE4C9A47ECF0ACD0CF682BB337BF5370A252436F
SHA-512:	58F8F13BD8DF2923C9CCB10018789299DFB2B9FE10F70CA8354069E2E77377105121032A8CDB3FDDDF815A3329F39021AD25B0ED6F8C31AC6BD3DEC79D68C5 D
Malicious:	false
Reputation:	low
Preview:	(...j...oy retne.....K../.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\76da32e7-664a-43eb-9d38-effd3e5276ac\184390d23e1bf4f4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7475
Entropy (8bit):	5.489489953728191
Encrypted:	false
SSDEEP:	192:edO3hmsOLAZ+3hX+WN4Lq5e6vGOzTjv8XkaJc:t3uD39+WG25e6vRzTz0Jc
MD5:	7009AA24384D32F06CBCC240CB823F73
SHA1:	B6797517DE4B1FB1B2EDEFE5940F07DC154C2F3D
SHA-256:	4598329456EF5F02398C97EBD4F888AAA2B1A329897204F5C51B5CFDB62DA27D
SHA-512:	2A8D822380A37EB31ABD11E75D3E7C8EB8BE10C65F3EF8014362FCDA87819551BDCC7EB82E361349FCC219F957815C677EEFCA60F775E2087C7ECBD9C13819 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....r?....https://7388r.csb.app/frame.html?_sw-precache=358bc62ccbd9155c9f01d203199f04da<!DOCTYPE html>.<html>. <head>. <script crossorigin type="text/javascript" src="https://codesandbox.io/static/js/vendors~app~embed~sandbox-startup.10f5f18b4.chunk.js"></script>. <script crossorigin type="text/javascript" src="https://codesandbox.io/static/js/sandbox-startup.81d8a90a0.js"></script>..<script src="//codesandbox.io/static/browserfs8/browserfs.min.js" type="text/javascript"></script>..<script>. window.process = BrowserFS.BFSRequire('process');. window.Buffer = BrowserFS.BFSRequire('buffer').Buffer;.</script>.. <meta charset="utf-8" />. <meta name="viewport" content="width=device-width, initial-scale=1" />. <title>Sign into your account</title>. <link rel="manifest" href="/manifest.json">. </head>. <body>. <script>. function redirect() {. var url = new URL(. "https://elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.co

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\76da32e7-664a-43eb-9d38-effd3e5276ac\index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	3:m+l:m
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CE 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\76da32e7-664a-43eb-9d38-effd3e5276ac\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3609758039057924
Encrypted:	false
SSDEEP:	3:JkkFjEfMoZXetAyXl/lBn+Tc3l/TRn4n:qMwfMiuNoEo
MD5:	78EE3EFFCD38D7528DA5747F739FC07B
SHA1:	4447B066F2E32E81408F5B2D07FFE179E0C54E09
SHA-256:	7C63C75BAFD9B9C863FEDC662350AC58378CB6FF8466BB520A5F9AA10B3F8E02
SHA-512:	F775DD092994D6B5DB62A644899C0FD3E70AB89DE6B67076C45B5353031B58C3A99465E68DBC27C210601FB740960FE4089BB90DE6FD9160174A9B346C7DD0D
Malicious:	false
Reputation:	low
Preview:	(...T...oy retne.....K../.@.....).oy retne.....>.C.....K../.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\8e4a827a-f74e-4188-9806-1faa63a29ef1\02ffbff9939db27c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	746115
Entropy (8bit):	5.424320028430574
Encrypted:	false
SSDEEP:	6144:ksZkjGmYXC6Ls5XXAUTp2d0clpfEyGsMKje8Rz8a7hHd3Oqzp5Ep6L+pasUCZZNQ:kQMTp2dfRqmpXLeaRrr7TlP
MD5:	9B4EB5A8F7360821EC6250E42BEE77F3
SHA1:	3CCBCC7C31BEB84298479B5801818C3C71FCC43E
SHA-256:	62B3228BCE12D4588AD415674AAC9DBC6F2EE028AAC76A384397015DDC57A31F
SHA-512:	9BBA156F95A6010102F1569FB711A4061E98B76AD33DD2BC345FE7C881124C54291513A0B51A83A2AAB3667EAEE370FA8B2FE6AABE89B8BED5FD908934709DD A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....6.....https://codesandbox.io/static/js/72.2c983ea22.chunk.js(this.csbJsonP=this.csbJsonP||[]).push([[72],{"../../node_modules/@babel/code-frame/lib/index.js":function(e,t,n){"use strict";(function(e){Object.defineProperty(t,"__esModule",{value:!0}),t.codeFrameColumns=a,t.default=function(t,n,r,o={}){if(!i){i=!0;const t="Passing lineNumber and colNumber is deprecated to @babel/code-frame. Please use `codeFrameColumns`.";if(e.emitWarning)e.emitWarning(t,"DeprecationWarning");else{new Error(t).name="DeprecationWarning",console.warn(new Error(t))}}return r=Math.max(r,0),a(t,{start:{column:r,line:n}},o)};var r=function(e){if(e&&e.__esModule)return e;if(null===e||"object"!==typeof e&&"function"!==typeof e)return{default:e};var t=o();if(t&&t.has(e))return t.get(e);var n={},r=Object.defineProperty&&Object.getOwnPropertyDescriptor;for(var i in e)if(Object.prototype.hasOwnProperty.call(e,i)){var s=r?Object.getOwnPropertyDescriptor(e,i):null;s&&(s.get||s.set)?Object.defineProper

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\8e4a827a-f74e-4188-9806-1faa63a29ef1\134c91c98518603b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	18994
Entropy (8bit):	5.360813652097222
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\8e4a827a-f74e-4188-9806-1faa63a29ef1\134c91c98518603b_0

SSDEEP:	192:dYrJfJJcCplBtugwEqsR1XugcKw6wAT/rdlbYeHTowPmn8hGqA/AEiTQpNLJwGVj:EMCdqEXu+2eHToUpU/AEioYxGmjsMAb1
MD5:	177EA7688626C6C40A1F19226CE774DD
SHA1:	8DFC7B28D140F40ADBB90B4EF24A9F42CFC9DF92
SHA-256:	F2104CE3C1C9A252E0B0928E59C768A74B099A55D4BCA45488E468414F250901
SHA-512:	053F62B2FA1BBE39E7A4FF9FBE0A290803B0D035164E16107ED85E142EF7B6A684C62D0C5EF931BA9491BF69B38E4B19937840AF8C2116E261370D96DFDA964E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....6.....https://codesandbox.io/static/js/76.c312409fb.chunk.js(this.csbJsonP=this.csbJsonP||[]).push([[76],{"../../standalone-packages/codesandbox-browserfs/dist/shims/buffer.js":function(e,t){e.exports=BrowserFS.BFSRequire("buffer")},"../common/lib/utils/jest-lite.js":function(e,t,r){"use strict";Object.defineProperty(t,"__esModule",{value:!0}),t.messages=void 0,function(e){e.INITIALIZE="initialize_tests",e.ADD_FILE="add_file",e.REMOVE_FILE="remove_file",e.FILE_ERROR="file_error",e.TOTAL_TEST_START="total_test_start",e.TOTAL_TEST_END="total_test_end",e.TEST_START="test_start",e.TEST_END="test_end",e.DESCRIBE_START="describe_start",e.DESCRIBE_END="describe_end",e.ADD_TEST="add_test"}(t.messages||(t.messages={}))},"./src/sandbox/eval/tests/jest-lite.ts":function(e,t,r){"use strict";r.r(t);var n=r("../../node_modules/@babel/runtime/regenerator/index.js"),s=r.n(n),a=r("../../node_modules/@babel/runtime/helpers/slicedToArray.js"),o=r.n(a),c=r("../../node_modules/@babel/runt

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\8e4a827a-f74e-4188-9806-1faa63a29ef1\cb22034d7c8bc530_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	50572
Entropy (8bit):	5.418583422258249
Encrypted:	false
SSDEEP:	768:lC1aarFqukkIOnUJhGZ33mSoXik8NuiFsWmpC:03qXkIk4GZ33mzi/F/mpC
MD5:	1A5F83B494C696173E832924D5BC5930
SHA1:	A1694535670D061200DF5CBEBACCB42D3FA58850
SHA-256:	D68D6DFF08CC590F09D11EA0C6FCDD44858A7EEEC926679BE19953AC4C54E269
SHA-512:	FA32C71C10F8CF269DF627D52FC5677CC28C8C551445ECCCE10C3C52D6A5F878774F10AE1F6E078A542413E0CC9AC9115535782D4BD977481D5B59F95A7F424
Malicious:	false
Reputation:	low
Preview:	0\r..m.....5...}k.....https://codesandbox.io/static/js/7.a39df6d6b.chunk.js(this.csbJsonP=this.csbJsonP||[]).push([[7],{"../../node_modules/constants-browserify/constants.json":function(e){e.exports=JSON.parse('{"O_RDONLY":0,"O_WRONLY":1,"O_RDWR":2,"S_IFMT":61440,"S_IFREG":32768,"S_IFDIR":16384,"S_IFCHR":8192,"S_IFBLK":24576,"S_IFIFO":4096,"S_IFLNK":40960,"S_IFSOCK":49152,"O_CREAT":512,"O_EXCL":2048,"O_NOCTTY":131072,"O_TRUNC":1024,"O_APPEND":8,"O_DIRECTORY":1048576,"O_NOFOLLOW":256,"O_SYNC":128,"O_SYMLINK":2097152,"O_NONBLOCK":4,"S_IRWXU":448,"S_IRUSR":256,"S_IWUSR":128,"S_IXUSR":64,"S_IRWXG":56,"S_IRGRP":32,"S_IWGRP":16,"S_IXGRP":8,"S_IRWXO":7,"S_IROTH":4,"S_IWOTH":2,"S_IXOTH":1,"E2BIG":7,"EACCES":13,"EADDRINUSE":48,"EADDRNOTAVAIL":49,"EAFNOSUPPORT":47,"EAGAIN":35,"EALREADY":37,"EBADF":9,"EBADMSG":94,"EBUSY":16,"ECANCELED":89,"ECHILD":10,"ECONNABORTED":53,"ECONNREFUSED":61,"ECONNRESET":54,"EDEADLK":11,"EDESTADDRREQ":39,"EDOM":33,"EDQUOT":69,"EEXIST":17,"EFAULT":14,"EFBIG":27,"EHOST

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\8e4a827a-f74e-4188-9806-1faa63a29ef1\index

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	3:m+l:m
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CB0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\8e4a827a-f74e-4188-9806-1faa63a29ef1\index-dir\temp-index

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	168
Entropy (8bit):	3.697706440953923
Encrypted:	false
SSDEEP:	3:gxVKuAyEjouJVtNj9FlTWL/lt4/p4eSvRgLzlltxzn:gxVS9jo0tNatpexlnzn

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\8e4a827a-f74e-4188-9806-1faa63a29ef1\index-dir\temp-index	
MD5:	895AE1D3C526A7EB8CC68EAADFCB305E
SHA1:	EEFB2425C142054A0D442EA12887FE1848A7E035
SHA-256:	8B9B6E3D1ABFEAB1FB7D3BAA8B185697472582E797F4E29B4AA593F332A1AB88
SHA-512:	C3C9AB8E6B578427B11E882E807F7D086148513BE55740356E535623A218E328089183FCF3F067DFC150A14F0DCB7EBF10F2B8D16A35B7DC3BE282E0D53A3B5E
Malicious:	false
Reputation:	low
Preview:	(.....'.oy retne.....!$K../.p.....1.oy retne.....v.....0.|M."....|.....d.....;`...L.....K.....'K../.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\91ddbac4-f65e-4942-ab83-8c3d87875c40\index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	3:m+l:m
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CE0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\91ddbac4-f65e-4942-ab83-8c3d87875c40\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	2.955557653394731
Encrypted:	false
SSDEEP:	3:JkkFjEfMoJ:qMwfMC
MD5:	30D309C790EF7D74CA173AE5E1DE71CC
SHA1:	956CEC2A9D8F3278A15D4A42E2D20E1FDC2AE6FD
SHA-256:	9ADAD508807409B2DFE060CE5BC88CCA391776BD61E15A42C3532088C1A0BD0E
SHA-512:	780E549B8E89BDCBDEC40BD6B0EAB1C308C6CA83E261374A7729A85001D4B28E759FE206B54D4DCF33EA50FB9A7F18E96AF223120A2E5869CA1538B1ACD78E28
Malicious:	false
Reputation:	low
Preview:	(...T...oy retne.....K../.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\eb1235d8-795c-4853-9125-823d3fcb9821\ab425f50d67661ba_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14233
Entropy (8bit):	4.9902201375414785
Encrypted:	false
SSDEEP:	96:nbHnl287Yj/OOJ6pw011lrwD9WDoHrmGyk7gO61tzGMTpDUXkd3DjQaLXdE/k3bs:j40K01rrwD9sk7gjXV3DjQaLdE8RG
MD5:	0C4AD2848A99E14A21E22C805D20F8C4
SHA1:	B5535A70E652E67703971E0611E7E8F64101B077
SHA-256:	B7379B9C9AECD54EDC57382AB8E8A88BA12F64698460BE05D15CD89F677C8623
SHA-512:	191A19CAA057CF54B01DB68D6384895AC77FDCB51012F72BADBA8D7137C3FAA9EEB9DD5F6098828CBD2D061A548FE43D5E1927897103B89D41D368BFB7F406D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\eb1235d8-795c-4853-9125-823d3fcb9821\ab425f50d67661ba_0	
Preview:	0\r..m.....T.....q....https://prod-packager-packages.codesandbox.io/v2/packages/@babel/runtime/7.12.5.json{"contents":{"/node_modules/@babel/runtime/package.json":{"content":"{\"name\":\"@babel/runtime\",\"version\":\"7.12.5\",\"description\":\"babel's modular runtime helpers\",\"license\":\"MIT\",\"publishConfig\":{\"access\":\"public\"},\"repository\":{\"type\":\"git\",\"url\":\"https://github.com/babel/babel.git\",\"directory\":\"packages/babel-runtime\"},\"homepage\":\"https://babeljs.io/\",\"author\":\"Sebastian McKenzie <sebmck@gmail.com>\",\"dependencies\":{\"regenerator-runtime\":\"^0.13.4\"},\"exports\":{\".\/helpers\/\":\"./helpers/\",\"./helpers/typeof\":\"./helpers/typeof.js\",\"./helpers/jsx\":\"./helpers/jsx.js\",\"./helpers/asyncIterator\":\"./helpers/asyncIterator.js\",\"./helpers/AwaitValue\":\"./helpers/AwaitValue.js\",\"./helpers/AsyncGenerator\":\"./helpers/AsyncGenerator.js\",\"./helpers/wrapAsyncGenerator\":\"./helpers/wrapAsyncGenerator.js\",\"./helpers/awaitAsyn

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\eb1235d8-795c-4853-9125-823d3fcb9821\index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	3:m+l:m
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CE 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\eb1235d8-795c-4853-9125-823d3fcb9821\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.4005998664238213
Encrypted:	false
SSDEEP:	3:8mWglX00EKkkltPRmTXl/lCXO8pKl:82lwFk/t0jCjs
MD5:	70ACB515B8E82EFFEA56C60FCFC05B5B
SHA1:	76A5851265013265DC98D5C411F942B5683B362E
SHA-256:	6D51F6B04D135397C12F12462D6604819CF279104A5C74A39BFA07CD1EEA86BE
SHA-512:	BB37E663264DEA80ADFE36E48EE9335402CB4FD7B57B096A665EC595A2AED85B969F77BEDBB2956261E3E668AAEAEB617159F11F7A31D263EA01C69719DAA4 54
Malicious:	false
Reputation:	low
Preview:	(....CsEoy retne.....q.K../.@.....oy retne.....9.....av.P_B.....9.....F..K../.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\CacheStorage\7ccb655c42ac4a48d40d852bfc245bb9eb5df148\index.txt.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2321
Entropy (8bit):	5.6031238428600485
Encrypted:	false
SSDEEP:	48:dpbpQs5FjwHs5z8T/qownTJLwnTJsJwnTJutPcwnTJuDPGc:T1QTHK8TijnTJcnTJsSnTJutnnTJuDb
MD5:	5F3C106AE5D5CF6E05A320FB8586935A
SHA1:	A87EAF4BDD741FB310EDBA4E0A4D64DE65546DFB
SHA-256:	4CF2AEFA23894BC11F6C8FE053DF9C5A6C78BBB1630E4999D478D6541A636BE5
SHA-512:	7317289239AF0B7BF31D7CF62D47957BDA163C9DDD27FA2F13E99949FC330D5035308FD811AABCF3ECF050EAFE04F012B8C19574429CC47D037836BD95BA0CA
Malicious:	false
Reputation:	low
Preview:	....:sw-precache-v3-code-sandbox-sandbox-https://7388r.csb.app/.$76da32e7-664a-43eb-9d38-effd3e5276ac"...=..6...J?x.I..(.....0...https://7388r.csb.app/....:sw-precache-v3-code-sandbox-sandbox-https://7388r.csb.app/.$76da32e7-664a-43eb-9d38-effd3e5276ac"...=..6...J?x.I..(.....0.....:$$$toolbox-cache$$$https://7388r.csb.app/$$$$$$inactive$$$.$91ddbac4-f65e-4942-ab83-8c3d87875c40"...=..6...J?x.I..(.....0...https://7388r.csb.app/.{.:sw-precache-v3-code-sandbox-sandbox-https://7388r.csb.app/.$76da32e7-664a-43eb-9d38-effd3e5276ac..<"...=..6...J?x.I..(.0..z.:$$$toolbox-cache$$$https://7388r.csb.app/$$$$$$inactive$$$.$91ddbac4-f65e-4942-ab83-8c3d87875c40.."...=..6...J?x.I..(.0..s.,$$$toolbox-cache$$$https://7388r.csb.app/$$$.$65f01577-c1a0-4567-b7fb-a01c7243529c"...=..6...J?x.I..(.....0...https://7388r.csb.app/.{.:sw-precache-v3-code-sandbox-sandbox-https://7388r.csb.app/.$76da32e7-664a-43eb-9d38-effd3e5276ac..<"...=..6...J?x.I..(.0..l.,$$$toolbox-cache$$$https://7388r.csb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\000001.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//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	714
Entropy (8bit):	5.820862746952289
Encrypted:	false
SSDEEP:	12:cyQI2xcBzNmKolicncmp4aaWH3HaMvAkd3jXdUqLPw5+AM2vGHaMvAsRAjXdUql:F2xc5NmK4icncmKv6dTzLOvyozl
MD5:	D31E943395D7E890E5B29B9ED6E308C1
SHA1:	352368588EB62CEA8891F1ACA4725DEF67AEB880
SHA-256:	86241096815ED075D6F3724FDE2D7C9CD64F961D9CA00C24982C82125B653E6A
SHA-512:	2A27EAF1668E2091C2C6DBA6214A880C5DE667CE49A48769746792AB977D7A97352A3351A5B551997612BEAC8B6E654C7B7D66D8356FBF1A6BDCDF916994FAD
Malicious:	false
Reputation:	low
Preview:	....I.....URES:0...INITDATA_NEXT_RESOURCE_ID.1..INITDATA_DB_VERSION.20..v.....INITDATA_NEXT_REGISTRATION_ID.1..INITDATA_NEXT_VERSION_ID.1.-INITDATA_UNIQUE_ORIGIN:https://7388r.csb.app/...REG:https://7388r.csb.app/.0.....https://7388r.csb.app/./https://7388r.csb.app/sandbox-service-worker.js .(.0.8.....@..Z.b.....trueh..h..h..h..h..h..h..p.x.....REGID_TO_ORIGIN:0.https://7388r.csb.app/..RES:0.07.../https://7388r.csb.app/sandbox-service-worker.js .....URES:0..PRES:0...>.....REG:https://7388r.csb.app/.0.....https://7388r.csb.app/./https://7388r.csb.app/sandbox-service-worker.js .(.0.8.....@..Z.b.....trueh..h..h..h..h..h..h..p.x.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	147
Entropy (8bit):	5.267172458635467
Encrypted:	false
SSDEEP:	3:tUKU+UuLkWvvwQWKKqFkPWXp5cViE2J5iKKKc64E/rAXKeqh5oEWIV//Uv:m1+UEkivIq2PWXp+N23iKKdKE/a2ZIF2
MD5:	CCF035CE66E3D33936E196F33525A420
SHA1:	82D349E7D8900C837254877D3B5F3EC299AB06A2
SHA-256:	DED281188A7BD0565D99A8C63E97CBB8E8F7DFCE37FE417C9D81313E3B57EA2F
SHA-512:	E20C0CB73EAC8E294185A01CD3EE64E1F009A89F071D67F1FE7407C8A5A3EEF3F237265F124221203B446C969420D753DD0329A55ECAD68CE8B4300E0EA1D3FC
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:34.723 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database/MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAIxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\MANIFEST-000001	
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C235B
Malicious:	false
Reputation:	low
Preview:	.|..".....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\2cc80dabc69f58b6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22877
Entropy (8bit):	5.845694686675001
Encrypted:	false
SSDEEP:	384:HfWj7CCxlvJm/MiQf6DdFLnj+x1uiWar2JL8TXMaB3DAQsffaVzYBhxzPV+9XL6B:Hej7CsvJJiZD7q1uyhy3HmTcSnkIg
MD5:	3E83F0630ED7B5B660BBAA27D4A17C99
SHA1:	304BC7F9766EF28FEABD5755DA948F8EC88AFA74
SHA-256:	4E49646490F38BA878C94E0B64FEB5353CE9AB13E70AAD8ABDB07EBE2D6B4CE7
SHA-512:	2B225A2B6398F9121972923E331FF07665042344B8FC12C0CA23433BDA0317F309AABD8999C00E4D1B9B286025C2A5B1DECB5B72D8BDA9699E68CD63DF7DCBFB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....rSG.....0"use strict";var precacheConfig=[["frame.html","358bc62ccbd9155c9f01d203199f04da"]],cacheName="sw-precache-v3-code-sandbox-sandbox-"+(self.registration?self.registration.scope:""),ignoreUrlParametersMatching=[/^utm_/],addDirectoryIndex=function(e,t){var n=new URL(e);return"/"===n.pathname.slice(-1)&&(n.pathname+=t),n.toString()},cleanResponse=function(e){return e.redirected?("body"in e?Promise.resolve(e.body):e.blob()).then(function(t){return new Response(t,{headers:e.headers,status:e.status,statusText:e.statusText})}):Promise.resolve(e)},createCacheKey=function(e,t,n,r){var o=new URL(e);return r&&o.pathname.match(r)||(o.search+=(o.search?"&":"")+encodeURIComponent(t)+"="+encodeURIComponent(n)),o.toString()},isPathWhitelisted=function(e,t){if(0===e.length)return!0;var n=new URL(t).pathname;return e.some(function(e){return n.match(e)})},stripIgnoredUrlParameters=function(e,t){var n=new URL(e);return n.hash="",n.search=n.search.slice(1).split("&").map(function(e)

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\2cc80dabc69f58b6_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	51249
Entropy (8bit):	5.703295926336359
Encrypted:	false
SSDEEP:	768:JNfw+X6K36dfb5Sv8MnZDJX7lUGENYdpTdeOdCs:bfw833lb5fMnZDJXhuedpTdebs
MD5:	515F193452F849E5D199105A95A1C66F
SHA1:	C88947C68DE63ED5323C1E59394BA43405C13376
SHA-256:	DBCEF333D72A9C331A870EDAC68F8D21358EF12B1869E93ADAACF3EB640AF2DD
SHA-512:	B9806F4A67C4D5374511B7280E1DAA0E6292FA523702549E39178B575CFD2DB71632B52B7341590B72C530BFD0E0379512D8B9CAE7005D2B7996DFFACAC1965E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....rSG.....0.....'.lJ....O.....h.....(S....`2.....L`z....8L`.....Qe.....precacheConfig....Qd.....cacheName....(Qh...[....ignoreUrlParametersMatching.. Qf~.RY....addDirectoryIndex.....Qe.j,"....cleanResponse.....Qe..B.....createCacheKey... Qfn.d`....isPathWhitelisted....(Qhr43@....stripIgnoredUrlParameters.....Qe._.J....hashParamName.....Qe..N....urlsToCacheKeys..(S.T.`b.....L`.....E.....(S.4.`$.....L`.....Qb.z.....map..(S.(.`.....L`.....Qb.t.D....url...K`.. ..Dd.....(.....(Rc.....I`....Da.....b.....@.-....<P...../...https://7388r.csb.app/sandbox-service-worker.js.a.....D`....D`....D`.....`Z...&...&.(S.l.`.....L`.....Qbr46.....URL...Qb...../.....Qcn..m....pathname..Qc..G.....slice.....K`....Du(.....&.%.e....&...&.(...&.(...&...&.Y....h....(...&.%.4..&.-...%.(...&.X.....(Rc.....`....Da.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	3:m+l:m
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CB0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\index	
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.5254324490140494
Encrypted:	false
SSDEEP:	3:91u7dE0v8AtdXl/ledlxE2V:+7KW8SHa
MD5:	35569D698465CDD06BB067D4FA740292
SHA1:	3793038BF1AC123060295B3C77C067641C3B224C
SHA-256:	9DB9B981F268246FB3B504AA579D9A5052DF27AC86B82D47773073F523A32E44
SHA-512:	08E05052227A2404D58C0850606F64E7215F4B2B1E18F57FC38C53DF6CCFF6B008D4BBB44C1CE011B2D4A05770E7461334F831BEE6A067F6F68CDAB52B3269F
Malicious:	false
Reputation:	low
Preview:	(...`...oy retne.....J.K../.@.....Hoy retne.....".....X....,.....".....K../.

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):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

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):	320
Entropy (8bit):	5.187544242741664
Encrypted:	false
SSDEEP:	6:m1+Uwg4q2PWXp+N23iKKdKrQMxIFUtpS+UwNZZmwPS+UwNzkwOWXp+N23iKKdKrb:H3hva5KkCFUtp33NZ/P33Nz5f5KktJ
MD5:	A73A95532EAB78798F228C8D4FF2C68E
SHA1:	EEF2439E5802727D97405BE45247C594DC415C58
SHA-256:	1AC580EEF60BBC93C343209DB49CD5D6D1C4405E8569F961BE5CB4EF66CD9AC3
SHA-512:	E81811A8D6D98080730933D1373A25C4F353912B9AF5E4DD043A318C5EFBFF5061F8B842024F12A18A951845BB21B363683CE3E58A6AFE5AB94C9C8263421460
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:30.759 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/01/27-16:31:30.761 15b0 Recovering log #3.2021/01/27-16:31:30.761 15b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/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):	345
Entropy (8bit):	5.183851623121668
Encrypted:	false
SSDEEP:	6:m1+Uw0yq2PWXp+N23iKKdK7Uh2ghZIFUtpS+Uwxj1ZmwPS+Uwx1RkwOWXp+N23in:H30yva5KkIhHh2FUtp33xJ/P33x1R5fl
MD5:	271D62F905D6AE427B56AD06D7557605
SHA1:	0176534DE3F9859059A2549F9FE6D10C9AFB05B7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SHA-256:	9CCB985118BD271D1638147B8EE35B9081EB49AB45B5C444C1C4C7CC93A4DC5D
SHA-512:	E5468AAEFC5A31E03307002871BFE74E75524EBD17AB126D20FD3104342F4FDC61CC1932AD34FFF08EE2B3A032B850F5A98217AE7A5AB426D5824BFB206AA2F5
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:30.521 d54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/01/27-16:31:30.522 d54 Recovering log #3.2021/01/27-16:31:30.522 d54 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\29c850d9-9905-47ac-90ad-fa7859b5efa4.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):	430
Entropy (8bit):	5.2519195083776635
Encrypted:	false
SSDEEP:	6:m1+UwWWfPIq2PWXp+N23iKKdKusNpV/2jMGIFUtpS+UwWQJZmwPS+UwWQDkwOWX2:H3NPIva5KkFFUtp33XJ/P33XD5f5KkOJ
MD5:	C5D9731C1A1A0FCF52D5AB5874E93F77
SHA1:	8AA3AAEBED8B696C73E22094E5D59606087FC549
SHA-256:	0176CEA2A2F88294ACBE044412C92932B16947A12E19EAB41E9CA8DEE73610BA
SHA-512:	4D5E003FA6635933DBAD042A1F0EAE4757A802986DFD653BCF7523AE51E60D4911C8BBD619783D29F2860E0C19573E83FD144311A01F63AC6CA306DE71C8BDD
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:30.813 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/01/27-16:31:30.815 15b0 Recovering log #3.2021/01/27-16:31:30.815 15b0 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
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.309635355598212
Encrypted:	false
SSDEEP:	12:H3cOva5KkmiuFUtp33UJ/P3355f5Kkm2J:HsMa5KkSgtERbf5Kkr
MD5:	DC03DF2744D6C8FFD8C538CD7873272A
SHA1:	61F168DE609A2A110D4051948218E04083A92928
SHA-256:	340AF5FA18574C4BA26938B12CBB43D8FD2B4A0FED9E2C9A81E1F33A7302C8B9
SHA-512:	E3F0B4B3E86CF68927E8016F03ECADD8A4500EA389EAA5542201A9793C7CAF23548A2C379DF761C86FF6C39AC477F72871BA2EF7F7CDEB78460CD08576F6619
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:30.846 d14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/01/27-16:31:30.848 d14 Recovering log #3.2021/01/27-16:31:30.849 d14 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):	5.322285600898678
Encrypted:	false
SSDEEP:	6:m1+UZgSuH+q2PWXp+N23iKKdKusNpZQMxIFUtpS+UZg0S6ZmwPS+UZgc0FNVkwOy:HiXFva5KkMFUtp3iJn/P3iqFz5f5KkTJ
MD5:	2BB9D767EF504E00CE9FE188BD23C744
SHA1:	5E9DF30B6794697F073B22FB481390E54FAA411C
SHA-256:	98309FC6FA15A438ACBA2B23B9090516ECAA6ED88991BF5035BE28E3693C617A
SHA-512:	9044CD8E08C82D41D38F3202457CDE08138F2FDC070F02434208057B0FD859D3422FDFE7EB3AEA7DF6CF294E88410439F309FB213BE597202D96705D6909F85A
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:46.947 17c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/01/27-16:31:46.948 17c8 Recovering log #3.2021/01/27-16:31:46.949 17c8 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\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
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):	5.224220291654886
Encrypted:	false
SSDEEP:	12:Hk3va5KkkGHArBFUtp3kOJ/P3k25f5KkkGHAryJ:Hia5KkkGgPgt5RNf5KkkGga
MD5:	3C88D4711FE7AAAFB4815655FA6D02BB
SHA1:	85352EFBEBA963B3390E2FD0C0C51984A45F6B3E
SHA-256:	B270D100A25E9AA8BF1FB4B8364CC5C9A414538EC2CD9EECAE9D78E1BFAA30FA
SHA-512:	767EA71A63494EC648BAB1D394EAB6BDC4CD626F7833AF004746A222C27C388136E14062B90A53D593FE6331C2DEAD39790BB893830B30D6769795E4725E8AF2
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:37.682 d14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/01/27-16:31:37.688 d14 Recovering log #3.2021/01/27-16:31:37.691 d14 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):	429
Entropy (8bit):	5.272016826136218
Encrypted:	false
SSDEEP:	12:Hk81yva5KkkGHArqiuFUtp3kM/P3kKlR5f5KkkGHArq2J:HDKa5KkkGgCgt/Zf5KkkGg7
MD5:	6712D87EF387D701031DC9CB753B33E8
SHA1:	4922F3FCEC0312D60412A1D1D932CFE75FC4A388
SHA-256:	79F6F89B410AF61284AE1A5B1A3770CF9CC61CDA7BF272EF84FB77D86A131327
SHA-512:	197A9025235E87FAA958AFD6472A0C01FEB6BE52DE123077D4F21698B6A565D4F845BC7FAC3DF4DE6B1BEB20C15E90E8DAB05B48FE048FB23B085E5575BE90E0
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:37.682 d54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/01/27-16:31:37.688 d54 Recovering log #3.2021/01/27-16:31:37.691 d54 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):	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\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Entropy (8bit):	5.208012579457135
Encrypted:	false
SSDEEP:	12:HAFva5KkkGHArAFUtp3//P3t5f5KkkGHArfJ:HAJa5KkkGgkgtv/f5KkkGgV
MD5:	E286D3BBA1CBD1C4B9E29880B2F7A077
SHA1:	D1BDCFAF05384E32CF60E3FDE3ABC60A87F8FC7B
SHA-256:	6D43331F7202D9C27A51FAAAD0EBD925427F08192E629F24C09D297C12BC64A3
SHA-512:	97EEA5811BB4515F0C11E0E25869CC0FAFF3D918B2119ED4003929F3AA026F5E46728FC0C9FF2C0A9A812686F2CE5AC00801A0AC4BAC8251BBE46CDF90242FE5
Malicious:	false
Reputation:	low
Preview:	2021/01/27-16:31:53.206 17c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/01/27-16:31:53.208 17c8 Recovering log #3.2021/01/27-16:31:53.208 17c8 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\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\cce6abd3-2504-455b-9fef-4752af18a5fa.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
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"}}}

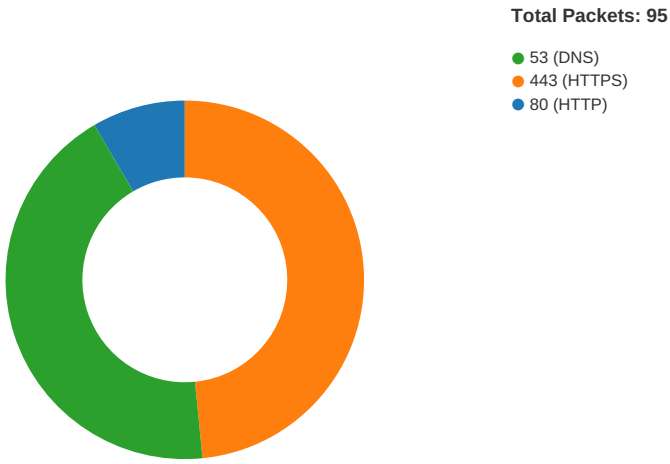
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:31:33.152621984 CET	49725	80	192.168.2.3	203.71.172.211
Jan 27, 2021 16:31:33.154014111 CET	49727	80	192.168.2.3	203.71.172.211
Jan 27, 2021 16:31:33.338146925 CET	49730	80	192.168.2.3	203.71.172.211
Jan 27, 2021 16:31:33.390933037 CET	80	49727	203.71.172.211	192.168.2.3
Jan 27, 2021 16:31:33.391098976 CET	49727	80	192.168.2.3	203.71.172.211
Jan 27, 2021 16:31:33.391587973 CET	49727	80	192.168.2.3	203.71.172.211
Jan 27, 2021 16:31:33.572597980 CET	80	49730	203.71.172.211	192.168.2.3
Jan 27, 2021 16:31:33.572715044 CET	49730	80	192.168.2.3	203.71.172.211
Jan 27, 2021 16:31:33.626518965 CET	80	49727	203.71.172.211	192.168.2.3
Jan 27, 2021 16:31:33.725132942 CET	80	49725	203.71.172.211	192.168.2.3
Jan 27, 2021 16:31:33.725217104 CET	49725	80	192.168.2.3	203.71.172.211
Jan 27, 2021 16:31:33.771971941 CET	80	49727	203.71.172.211	192.168.2.3
Jan 27, 2021 16:31:33.826101065 CET	49727	80	192.168.2.3	203.71.172.211
Jan 27, 2021 16:31:33.846606016 CET	49735	443	192.168.2.3	104.18.27.114
Jan 27, 2021 16:31:33.886488914 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:33.886569977 CET	49735	443	192.168.2.3	104.18.27.114
Jan 27, 2021 16:31:33.887089014 CET	49735	443	192.168.2.3	104.18.27.114
Jan 27, 2021 16:31:33.927756071 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:33.934618950 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:33.934685946 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:33.934748888 CET	49735	443	192.168.2.3	104.18.27.114
Jan 27, 2021 16:31:33.984201908 CET	49735	443	192.168.2.3	104.18.27.114
Jan 27, 2021 16:31:33.984380007 CET	49735	443	192.168.2.3	104.18.27.114
Jan 27, 2021 16:31:33.984596968 CET	49735	443	192.168.2.3	104.18.27.114
Jan 27, 2021 16:31:34.024044991 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:34.024200916 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:34.024416924 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:34.025017977 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:34.025222063 CET	49735	443	192.168.2.3	104.18.27.114
Jan 27, 2021 16:31:34.065018892 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:34.104348898 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:34.104365110 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:34.104381084 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:34.104392052 CET	443	49735	104.18.27.114	192.168.2.3
Jan 27, 2021 16:31:34.104438066 CET	49735	443	192.168.2.3	104.18.27.114
Jan 27, 2021 16:31:34.104480028 CET	49735	443	192.168.2.3	104.18.27.114
Jan 27, 2021 16:31:34.253540039 CET	49737	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.253978968 CET	49738	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.254311085 CET	49739	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.254698038 CET	49740	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.255069017 CET	49741	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.255439043 CET	49742	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.255635977 CET	49743	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.293807983 CET	443	49737	104.18.22.207	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:31:34.293845892 CET	443	49738	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.293936014 CET	49738	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.293951988 CET	49737	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.294256926 CET	49738	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.294258118 CET	443	49739	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.294341087 CET	49739	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.294485092 CET	49737	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.294603109 CET	49739	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.294617891 CET	443	49740	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.294698954 CET	49740	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.294954062 CET	49740	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.295180082 CET	443	49741	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.295239925 CET	49741	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.295314074 CET	443	49742	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.295428991 CET	49742	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.295722008 CET	49741	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.295974970 CET	49742	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.296607971 CET	443	49743	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.296689987 CET	49743	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.296889067 CET	49743	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.334278107 CET	443	49738	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.334362030 CET	443	49737	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.334387064 CET	443	49739	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.334743023 CET	443	49740	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.336770058 CET	443	49737	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.336860895 CET	443	49737	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.336889029 CET	443	49741	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.336998940 CET	49737	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.337312937 CET	443	49742	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.337939024 CET	443	49743	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.338099003 CET	443	49740	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.338138103 CET	443	49740	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.338175058 CET	443	49739	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.338207006 CET	443	49739	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.338207960 CET	49740	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.338258028 CET	49739	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.340172052 CET	443	49742	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.340220928 CET	443	49742	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.340321064 CET	49742	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.340497017 CET	443	49738	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.340532064 CET	443	49738	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.340576887 CET	49738	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.340853930 CET	443	49741	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.340910912 CET	443	49741	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.340967894 CET	49741	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.343079090 CET	443	49743	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.343117952 CET	443	49743	104.18.22.207	192.168.2.3
Jan 27, 2021 16:31:34.343187094 CET	49743	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.348861933 CET	49737	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.349690914 CET	49740	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.350534916 CET	49739	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.351341963 CET	49742	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.352339983 CET	49738	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.353188992 CET	49741	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.353988886 CET	49743	443	192.168.2.3	104.18.22.207
Jan 27, 2021 16:31:34.354134083 CET	49740	443	192.168.2.3	104.18.22.207

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:31:24.967380047 CET	53	63492	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:26.132700920 CET	60831	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:26.183881044 CET	53	60831	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:27.051938057 CET	60100	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:31:27.102886915 CET	53	60100	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:28.102001905 CET	53195	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:28.150309086 CET	53	53195	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:28.888190031 CET	50141	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:28.938961029 CET	53	50141	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:29.762043953 CET	53023	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:29.810055971 CET	53	53023	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:31.438714981 CET	49563	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:31.486809015 CET	53	49563	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:32.796492100 CET	57084	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:32.844587088 CET	53	57084	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:33.089780092 CET	58823	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:33.093626022 CET	57568	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:33.095674038 CET	50540	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:33.097224951 CET	54366	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:33.146933079 CET	53	54366	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:33.148756981 CET	53	58823	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:33.152477980 CET	53	57568	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:33.156552076 CET	53	50540	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:33.568502903 CET	53034	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:33.633111000 CET	53	53034	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:33.714622021 CET	57762	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:33.725986004 CET	55435	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:33.771068096 CET	53	57762	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:33.782890081 CET	50713	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:33.792433023 CET	53	55435	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:33.845633030 CET	53	50713	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:34.195832968 CET	58987	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:34.252551079 CET	53	58987	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:34.687757015 CET	56579	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:34.735871077 CET	53	56579	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:34.947664976 CET	60633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:34.982772112 CET	61292	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:34.984369040 CET	63619	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:35.011540890 CET	53	60633	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:35.040133953 CET	53	61292	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:35.082379103 CET	53	63619	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:35.392508984 CET	64938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:35.454269886 CET	53	64938	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:35.630508900 CET	61946	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:35.694385052 CET	53	61946	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:36.710278034 CET	64910	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:36.758246899 CET	53	64910	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:36.875055075 CET	52123	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:36.941639900 CET	53	52123	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:38.030106068 CET	58784	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:38.078033924 CET	53	58784	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:38.483105898 CET	63978	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:38.545069933 CET	53	63978	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:39.225523949 CET	62938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:39.293922901 CET	53	62938	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:39.305054903 CET	55708	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:39.370594025 CET	53	55708	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:40.508852005 CET	56803	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:40.574748039 CET	53	56803	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:40.869195938 CET	57145	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:40.950105906 CET	53	57145	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:41.045747995 CET	55359	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:41.099613905 CET	53	55359	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:42.262028933 CET	49361	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:42.313604116 CET	53	49361	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:57.487086058 CET	53279	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:31:57.550410986 CET	53	53279	8.8.8.8	192.168.2.3
Jan 27, 2021 16:31:57.814567089 CET	56881	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 16:31:57.862965107 CET	53	56881	8.8.8.8	192.168.2.3
Jan 27, 2021 16:32:13.560734987 CET	53642	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:32:13.617777109 CET	53	53642	8.8.8.8	192.168.2.3
Jan 27, 2021 16:32:14.381937027 CET	55667	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:32:14.432697058 CET	53	55667	8.8.8.8	192.168.2.3
Jan 27, 2021 16:32:15.528141975 CET	54833	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:32:15.585901976 CET	53	54833	8.8.8.8	192.168.2.3
Jan 27, 2021 16:32:21.169194937 CET	62476	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:32:21.232316971 CET	53	62476	8.8.8.8	192.168.2.3
Jan 27, 2021 16:32:26.110045910 CET	49705	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:32:26.209161043 CET	53	49705	8.8.8.8	192.168.2.3
Jan 27, 2021 16:32:26.647489071 CET	61477	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:32:26.709199905 CET	53	61477	8.8.8.8	192.168.2.3
Jan 27, 2021 16:32:27.620927095 CET	61633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 16:32:27.679402113 CET	53	61633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 16:31:33.097224951 CET	192.168.2.3	8.8.8.8	0xc335	Standard query (0)	lib.tnua.edu.tw	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:33.782890081 CET	192.168.2.3	8.8.8.8	0x93df	Standard query (0)	7388r.csb.app	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:34.195832968 CET	192.168.2.3	8.8.8.8	0x4ce3	Standard query (0)	codesandbox.io	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:34.982772112 CET	192.168.2.3	8.8.8.8	0x5d	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:34.984369040 CET	192.168.2.3	8.8.8.8	0xe409	Standard query (0)	prod-packager-packages.codesandbox.io	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:35.392508984 CET	192.168.2.3	8.8.8.8	0x9cc3	Standard query (0)	col.csbops.io	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:35.630508900 CET	192.168.2.3	8.8.8.8	0x229	Standard query (0)	elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:36.875055075 CET	192.168.2.3	8.8.8.8	0xeda9	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:38.030106068 CET	192.168.2.3	8.8.8.8	0x824c	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:39.225523949 CET	192.168.2.3	8.8.8.8	0x9d38	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:40.869195938 CET	192.168.2.3	8.8.8.8	0x23e3	Standard query (0)	elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 16:31:33.146933079 CET	8.8.8.8	192.168.2.3	0xc335	No error (0)	lib.tnua.edu.tw		203.71.172.211	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:33.845633030 CET	8.8.8.8	192.168.2.3	0x93df	No error (0)	7388r.csb.app		104.18.27.114	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:33.845633030 CET	8.8.8.8	192.168.2.3	0x93df	No error (0)	7388r.csb.app		104.18.26.114	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:34.252551079 CET	8.8.8.8	192.168.2.3	0x4ce3	No error (0)	codesandbox.io		104.18.22.207	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:34.252551079 CET	8.8.8.8	192.168.2.3	0x4ce3	No error (0)	codesandbox.io		104.18.23.207	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:35.040133953 CET	8.8.8.8	192.168.2.3	0x5d	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 16:31:35.082379103 CET	8.8.8.8	192.168.2.3	0xe409	No error (0)	prod-packager-packages.codesandbox.io		104.18.23.207	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:35.082379103 CET	8.8.8.8	192.168.2.3	0xe409	No error (0)	prod-packager-packages.codesandbox.io		104.18.22.207	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:35.454269886 CET	8.8.8.8	192.168.2.3	0x9cc3	No error (0)	col.csbops.io		148.251.96.176	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:35.694385052 CET	8.8.8.8	192.168.2.3	0x229	No error (0)	elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com	s3-r-w.us-east-2.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 16:31:35.694385052 CET	8.8.8.8	192.168.2.3	0x229	No error (0)	s3-r-w.us-east-2.amazonaws.com		52.219.100.16	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:36.941639900 CET	8.8.8.8	192.168.2.3	0xeda9	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 16:31:36.941639900 CET	8.8.8.8	192.168.2.3	0xeda9	No error (0)	googlehosted.l.googleusercontent.com		172.217.22.225	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:38.078033924 CET	8.8.8.8	192.168.2.3	0x824c	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 16:31:39.293922901 CET	8.8.8.8	192.168.2.3	0x9d38	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 16:31:39.293922901 CET	8.8.8.8	192.168.2.3	0x9d38	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.11.11	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:39.293922901 CET	8.8.8.8	192.168.2.3	0x9d38	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.11.4	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:39.293922901 CET	8.8.8.8	192.168.2.3	0x9d38	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.11.45	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:39.293922901 CET	8.8.8.8	192.168.2.3	0x9d38	No error (0)	d26p066pn2w0s0.cloudfront.net		143.204.11.13	A (IP address)	IN (0x0001)
Jan 27, 2021 16:31:40.950105906 CET	8.8.8.8	192.168.2.3	0x23e3	No error (0)	elasticbeanstalk-us-east-2-95newbeie.s3.us-east-2.amazonaws.com	s3-r-w.us-east-2.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 16:31:40.950105906 CET	8.8.8.8	192.168.2.3	0x23e3	No error (0)	s3-r-w.us-east-2.amazonaws.com		52.219.100.8	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- lib.tnua.edu.tw

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49727	203.71.172.211	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 16:31:33.391587973 CET	690	OUT	GET /goto/https://7388r.csb.app HTTP/1.1 Host: lib.tnua.edu.tw Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 16:31:33.771971941 CET	710	IN	HTTP/1.1 302 Found Date: Wed, 27 Jan 2021 15:32:43 GMT Server: Apache Location: https://7388r.csb.app? Content-Length: 206 Keep-Alive: timeout=15, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 37 33 38 38 72 2e 63 73 62 2e 61 70 70 3f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 16:31:36.001672029 CET	52.219.100.16	443	192.168.2.3	49755	CN=*.s3.us-east-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jul 24 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Thu May 27 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	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 Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jan 27, 2021 16:31:36.003031969 CET	52.219.100.16	443	192.168.2.3	49756	CN=*.s3.us-east-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jul 24 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Thu May 27 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	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 Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior

● chrome.exe
● chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5944 Parent PID: 2128

General

Start time:	16:31:29
Start date:	27/01/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://lib.tnua.edu.tw/goto/https://7388r.csb.app#asdf@asdf.de'
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 4968 Parent PID: 5944

General

Start time:	16:31:31
Start date:	27/01/2021
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=1584,11749481043944155124,6311535833497222460,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1668 /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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly