



ID: 383571
Cookbook: browseurl.jbs
Time: 23:12:07
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report https://1dil9.codesandbox.io/?bbre=aHR0cHM6Ly91dGFpenhveHV4enVzYWN4Y3gtZGFyaW5nLWNyb2NvZGlsZS13Yi5teWJsdWVtaXgubmV0Lz9iYnJlPX 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Startup 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Signature Overview 3
AV Detection: 4
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
Contacted IPs 9
Public 9
Private 9
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 41
No static file info 41
Network Behavior 41
Network Port Distribution 41
TCP Packets 42
UDP Packets 43
DNS Queries 45
DNS Answers 45
HTTPS Packets 47
Code Manipulations 48
Statistics 48
Behavior 48
System Behavior 48
Analysis Process: chrome.exe PID: 4840 Parent PID: 4900 48
General 48
File Activities 49
Registry Activities 49
Analysis Process: chrome.exe PID: 5320 Parent PID: 4840 49
General 49
File Activities 49
Disassembly 49

Copyright Joe Security LLC 2021

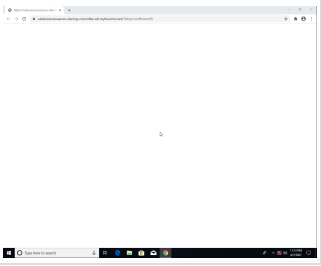
Analysis Report https://1dil9.codesandbox.io/?bbre=aH…

Overview

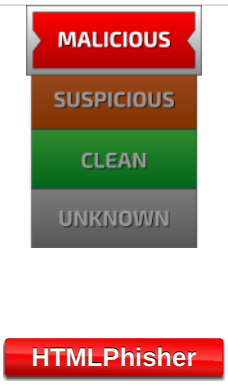
General Information

Sample URL:	https://1dil9.codesandbox.io/?bbre=aHR0cHM6Ly91dGFpenhveHV4enVzYWN4Y3gtZGFy...GFyaW5nLWNyb2NvZGlsZS13Yi5teWJsdWVtaXgubmV0Lz9iYnJlPXpveDlzb3h6bw&en=sdocxo
Analysis ID:	383571
Infos:	

Most interesting Screenshot:



Detection

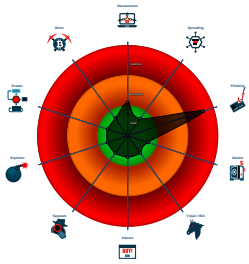


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 4840 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://1dil9.codesandbox.io/?bbre=aHR0cHM6Ly91dGFpenhveHV4enVzYWN4Y3gtZGFyaW5nLWNyb2NvZGlsZS13Yi5teWJsdWVtaXgubmV0Lz9iYnJlPXpveDlzb3h6bw&en=sdocxo' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5320 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1508,110634690922127284,6560826107686931846,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1788 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

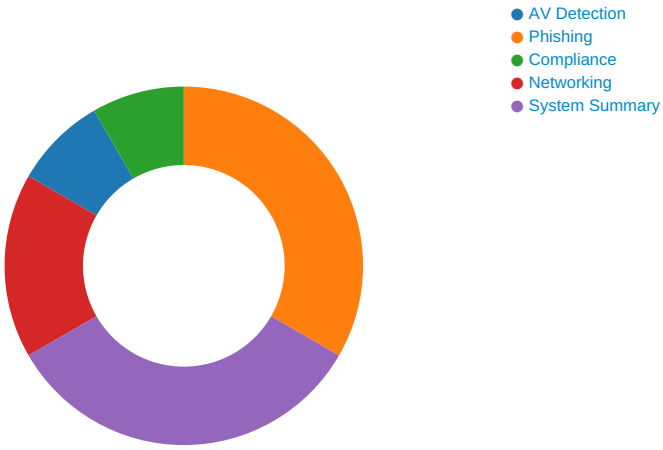
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Phishing:



Phishing site detected (based on favicon image match)

Yara detected HtmlPhish29

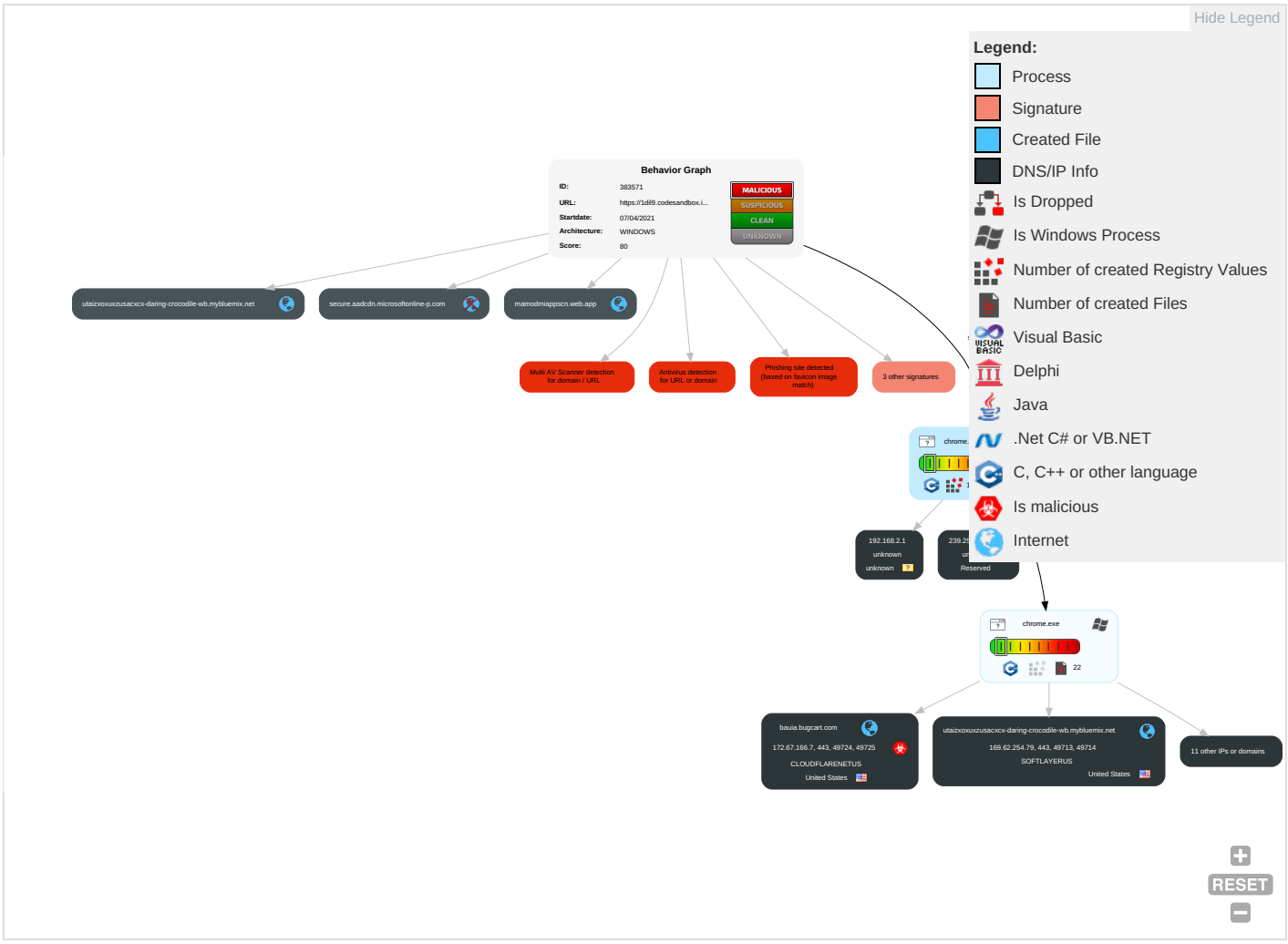
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

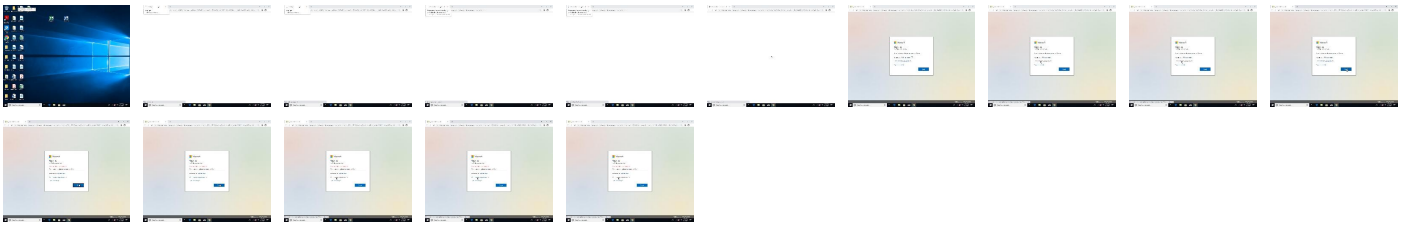
Behavior Graph

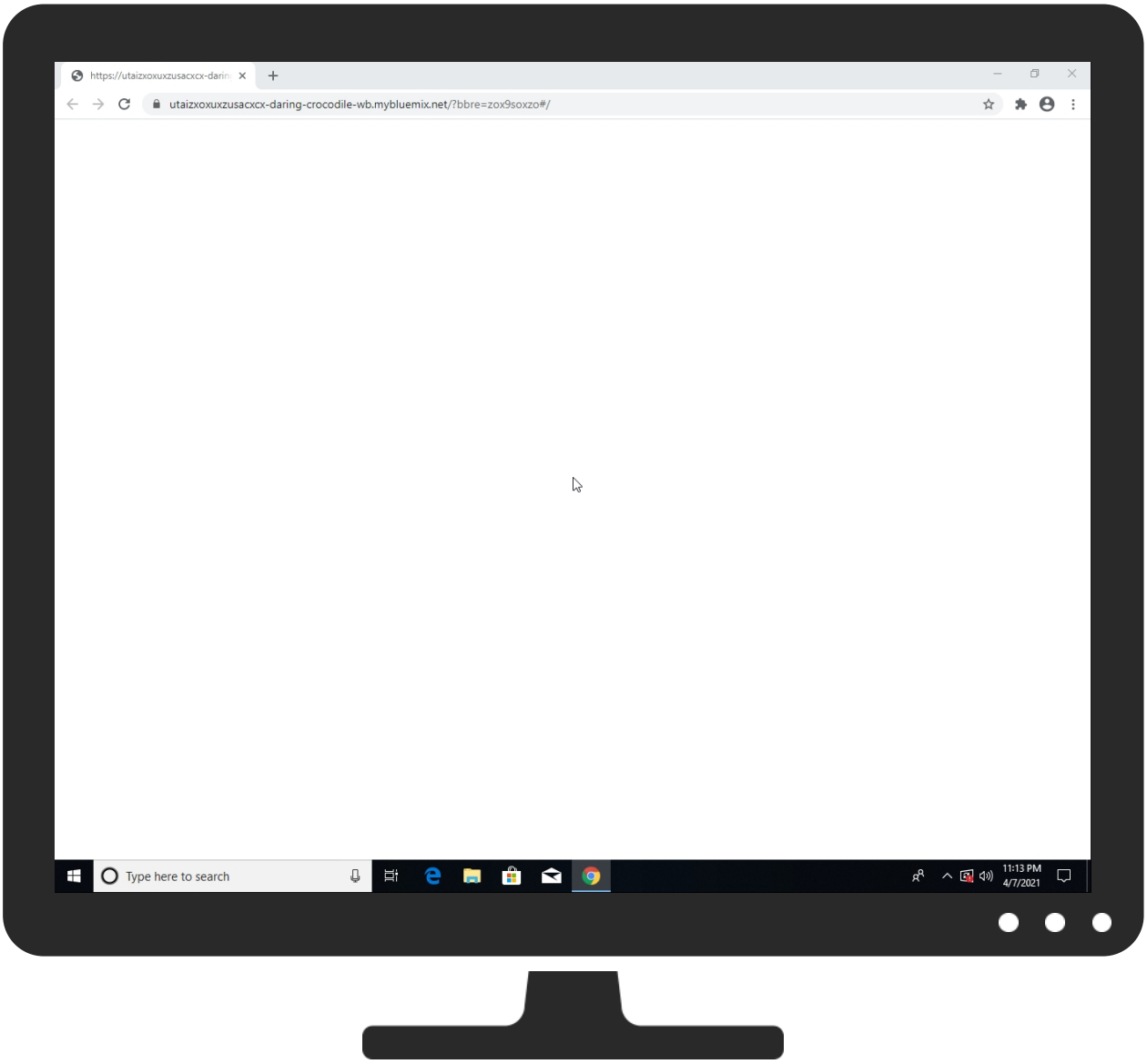


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://1dil9.codesandbox.io/?bbre=aHR0cHM6Ly91dGFpenhveHV4enVzYWN4Y3gtZGFyaW5nLWNyb2NvZGlsZS13Yi5teWJsdWVtaXgubmV0Lz9iYnJlPXpveDlzb3h6bw&en=sdocxo	0%	Virustotal		Browse
http://https://1dil9.codesandbox.io/?bbre=aHR0cHM6Ly91dGFpenhveHV4enVzYWN4Y3gtZGFyaW5nLWNyb2NvZGlsZS13Yi5teWJsdWVtaXgubmV0Lz9iYnJlPXpveDlzb3h6bw&en=sdocxo	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bauia.bugcart.com	8%	Virustotal		Browse
sslcnd.aioecoin.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/WkXFqC1KsV5DdqvxM6qYrUhjnxlodCzuIEBa33Q-!@&PK3BC4ut7DkqRS&!@B8OmulSAEnQFya3!@&-W4r2X3r4HRfcy8KlpXMdFl7BRc74LU45bBjpjkezJ6kQ2Ck8OgB7gYivtWmuK3VcxIY7w8FuKUnuarDlUU3mksHDxGJcblA-ZTB8uM7vUVNdU8uDQL7tGM8ZeeonEPmnzUCcaGvCUzwdAErAtMSwfD7eijgwDsRhVeBtXpJauz/2b5qVKkhzQWcPa0Ym6cW4OlewDOVqDy1X64Aj7o9FZqYBCKMs340DS3e2R2c1dXwmS	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://mamodmiappscn.web.app/dfgtyhgcvxcxzxcx/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301617631055.	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	Avira URL Cloud	safe	
http://https://mamodmiappscn.web.app/dfgtyhgcvxcxzxcx/themes/84663c95639ba690acf716f39df131acnbr1617631064.	0%	Avira URL Cloud	safe	
http://https://mamodmiappscn.web.app/dfgtyhgcvxcxzxcx/themes/1419a0bd7c8e13fc51f9714c675afc17.js	0%	Avira URL Cloud	safe	
http://https://sslcnd.aioecoin.org/bDFJcXd6cDMyaS9ORE5vSXdNVGdLaW9oOW14Z2p5M2NGSE5vd2xWWnAwYnlKbkhreVc3aG1x	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://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.netMhttps://utaizxoxuxzusacxcx-daring-croco	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mamodmiappscn.web.app	151.101.65.195	true	false		unknown
bauia.bugcart.com	172.67.166.7	true	true	• 8%, Virustotal, Browse	unknown
codesandbox.io	104.18.22.207	true	false		high
utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net	169.62.254.79	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
1dil9.codesandbox.io	104.18.22.207	true	false		high
unpkg.com	104.16.123.175	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
sslcnd.aioecoin.org	172.67.176.224	true	false	• 0%, Virustotal, Browse	unknown
clients2.googleusercontent.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
aadcdn.msauth.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net	000003.log4.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js	f747e026eefdaac9_0.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=ltIfOCcHOlhuIFnTMdKEkw90r33WTX%2F2FXYbfgvI6UE2IAPH9g0wrHgXoFdz	Reporting and NEL.1.dr	false		high
http://https://mybluemix.net/t	b6ef8681c83f6864_0.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo2:	History Provider Cache.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#Sign	History-journal.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://1dil9.codesandbox.io	Current Session.0.dr	false		high
http://https://mamodmiappscn.web.app/dfgtyhgcvxcxzxcx/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301617631055.	b6ef8681c83f6864_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://mybluemix.net/l	c6e1780a88646c8d_0.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/R	Favicons-journal.0.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://mybluemix.net/=	f778065137f2cb2f_0.0.dr	false		high
http://https://mamodmiappscn.web.app/dfgtyhgcvxcxzxcx/themes/84663c95639ba690acf716f39df131acnbr1617631064.	05a903e08cfdbf22_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://1dil9.codesandbox.io/?bbre=aHR0cHM6Ly91dGFpenhveHV4enVzYWN4Y3gtZGFyaW5nLWNyb2NvZGlsZS13Yi5te	History-journal.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js	ddacd2c15f59d922_0.0.dr	false		high
http://https://mamodmiappscn.web.app/dfgtyhgcvxcxzxcx/themes/1419a0bd7c8e13fc51f9714c675afc17.js	1e5ef1f4d4da98c0_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://unpkg.com/axios	c1a6fa7c31c3ccdf_0.0.dr	false		high
http://https://codesandbox.io/static/js/banner.8d93e521a.js	7c0b8dbb7aa8807b_0.0.dr	false		high
http://https://codesandbox.io/	7c0b8dbb7aa8807b_0.0.dr	false		high
http://https://unpkg.com/vue-router	f778065137f2cb2f_0.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/	Current Session.0.dr	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://https://sslcnd.aioecoin.org/bDFJcXd6cDMyaS9ORE5vSXdNVGdLaW9oOW14Z2p5M2NGSE5vd2xWWnAwYnlKbkhreVc3aG1x	17474f55ef485b09_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo	Current Session.0.dr	false		high
http://https://dns.google	b71ab9a6-d831-41a6-9472-10ffcbc4c6ee.tmp.1.dr, 284b376a-6223-4bd1-bcd1-245836f08d66.tmp.1.dr, 31864252-a5eb-4833-839c-98c63fcf2de4.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/https://utaizxoxuxzusa	History-journal.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#=	Current Session.0.dr	false		high
http://https://mybluemix.net/(	4d3807be645f8dea_0.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js	4d3807be645f8dea_0.0.dr	false		high
http://https://mybluemix.net/	1e5ef1f4d4da98c0_0.0.dr, 17474f55ef485b09_0.0.dr, ef21b07c6ae2decd_0.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/kCavjLSFBW3dR6feDB0nga	History.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo2	History Provider Cache.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo/	History-journal.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/Sign	History-journal.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/f)	Current Session.0.dr	false		high
http://https://codesandbox.io/public/sse-hooks/sse-hooks.cb2ef05bda555d18c964cf27a52aebac.js	6c179afef040ee7b_0.0.dr	false		high
http://https://mybluemix.net/.	c1a6fa7c31c3ccdf_0.0.dr	false		high
http://https://mybluemix.net/ml	8f02ce8f1f8eee69_0.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/	000003.log0.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/WkXFqC1KsV5DdqvxM6qYrU	History-journal.0.dr, Favicons-journal.0.dr	false		high
http://https://unpkg.com/lodash	c6e1780a88646c8d_0.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=h8oB%2FmaKKHH3zdX0HnuS0RDIYCNPjUdLjyOOlkl678dlWbtT6pTnxvVH4Bb5	Reporting and NEL.1.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/2Nhttps://utaizxoxuxzu	History Provider Cache.0.dr	false		high
http://https://clients2.googleusercontent.com	b71ab9a6-d831-41a6-9472-10ffcbc4c6ee.tmp.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://unpkg.com/vue	81cc3335c6a78fef_0.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.netMhttps://utaizxoxuxzusacxcx-daring-croco	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report?s=UtHqPkNk37YvnBvsxUovpzLltQDeIm8THmGQAbPEBMwCosjaRNQ7SgvdhFjRzP	Reporting and NEL.1.dr	false		high
http://https://mybluemix.net/IB	81cc3335c6a78fef_0.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#	Current Session.0.dr, Favicons-journal.0.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.js	ef21b07c6ae2decd_0.0.dr	false		high
http://https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo#/6	Current Session.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.166.7	bauia.bugcart.com	United States		13335	CLOUDFLARENETUS	true
172.67.176.224	sslcnd.aioecoin.org	United States		13335	CLOUDFLARENETUS	false
104.16.123.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.22.207	codesandbox.io	United States		13335	CLOUDFLARENETUS	false
151.101.65.195	mamodmiappscn.web.app	United States		54113	FASTLYUS	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
169.62.254.79	utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net	United States		36351	SOFTLAYERUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

Copyright Joe Security LLC 2021

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383571
Start date:	07.04.2021
Start time:	23:12:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://1dil9.codesandbox.io/?bbre=aHR0cHM6Ly91dGFpenhveHV4enVzYWN4Y3gtZGFyaW5nLWNyb2NvZGlsZS13Yi5teWJsdWVtaXgubmV0Lz9iYnJlPXpveDlzb3h6bw&en=sdocxo
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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.phis.win@29/181@15/11
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.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): 40.88.32.150, 13.88.21.125, 104.43.193.48, 172.217.168.13, 216.58.215.238, 172.217.168.35, 173.194.160.74, 142.250.34.2, 172.217.168.10, 13.107.246.19, 13.107.213.19, 104.111.246.178, 172.217.168.42, 172.217.168.74, 216.58.215.234, 52.255.188.83, 13.64.90.137, 23.54.113.104, 23.0.174.200, 23.0.174.185 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, standard.t-0009.t-msedge.net, r5.sn-1gi7znes.gvt1.com, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcoleus15.cloudapp.net, clients2.google.com, redirector.gvt1.com, dual.t-0009.t-msedge.net, Edge-Prod-ZRH.ctrl.t-0009.t-msedge.net, audownload.windowsupdate.nsatc.net, e13761.dscg.akamaiedge.net, edgedl.gvt1.com, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, ajax.googleapis.com, aadcdnoriginwus2.azureedge.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, r5---sn-1gi7znes.gvt1.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, www.googleapis.com, star-azureedge-prod.trafficmanager.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, t-0009.t-msedge.net, blobcollector.events.data.trafficmanager.net, aadcdnoriginwus2.afd.azureedge.net, clients.l.google.com, skypedataprdcolwus15.cloudapp.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

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\6ba8bed1-dbca-4960-9140-49fd3b432bf0.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):	164170
Entropy (8bit):	6.082081113439333
Encrypted:	false
SSDEEP:	3072:svZZM4iTMFp3l+7LSx8sogeKFcbXafIB0u1GOJmA3iuRc:s/gMTo7JsogHaqfIlUOoSiuRc
MD5:	0E912DD05B7627D67A884BC4B836313F
SHA1:	F26DF8CBA911F0AD72EB9083B0ED4CF3FAB127C0
SHA-256:	9F61C7F8A40730F89469ECBB6D96C8A26E8CF6F79251D3022EF8E3875E6F1D14
SHA-512:	F9D226BAD829A508B23615BF260C2B9ADF190692C07EEC9AE2469DFD0639AC5ED0DA83E63678C6AE8CF520B95AD05507F763E65761D951095B1CF87B6AB72D7
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":1.617862375218367e+12,"network":1.617829976e+12,"ticks":94217697.0,"uncertainty":4732116.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510166079 96"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\6f2e0247-3390-4528-97e6-0f53b484cb3e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7464297749694278
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\6f2e0247-3390-4528-97e6-0f53b484cb3e.tmp	
SSDEEP:	384:TjUTvVWlJtS/uNPr8v7R38LZ0HdUGw/rK1DXxM5BRwrajmCFWB/L3MOpJrN213mZ:gyFd29QghOeHPt1kvrS1Kj1Pl/
MD5:	0E30EF32443C8BDF7201D3FA51F8362A
SHA1:	E9A39AA0093B36F3E9306287EB418DE5AC9126A4
SHA-256:	2DE1B8F032283B29118A67F2453DD9090BCF4345954DCD1AD10731270DD69648
SHA-512:	87E8D7100890890E8B7A43267130718D17E07796D15241355CC8572FBD46AEEDD579CA1AA7049FCC1C4C9B02D0FE7914BC4F32F0E0359A69D8D0635F13F96D3
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....68.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4799c300-6fb4-4621-a855-106fb8e02daf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.5360590592907375
Encrypted:	false
SSDEEP:	384:BV8tWLl5YXj1kXqKf/pUZNCgVLH2HfDZrUjHGwnThAybbY4N:zLllj1kXqKf/pUZNCgVLH2HftrUDGwnn
MD5:	D97625B3F330CF7F19622A55D32C2581
SHA1:	A72F9F2A2AA1A4F2F68A3A535E06CBE4878BE9DF
SHA-256:	B9158054B7887C989A5E34E5C42A0A8ADD5ED3E196C1157DF426BB1DA994CC76
SHA-512:	6F157431DF656C7453904BED88CD09EC0802D52B9BDA9A679CBEA104E8637BD004398C3C9A867781DA90EE9947740A9384229BC987A94ED408061A134E610F1
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13262335972124877","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\524a7981-b2b2-48d3-b260-ddf68c0bbe53.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.535977848954797
Encrypted:	false
SSDEEP:	384:BV8tWLl5YXj1kXqKf/pUZNCgVLH2HfDZrUjHGnnThAybDY4g:zLllj1kXqKf/pUZNCgVLH2HftrUDGnnO
MD5:	40E5E51DFBB367F7CE74DD0F45F551C2
SHA1:	F2AD7670A7C07892944669702622524241251AE6
SHA-256:	D9B3C548CDEDF96F12DC147A77ADE946F1FBBDF3E1D00B6909DDE0B8A55E5384
SHA-512:	D715607E0582C937FD0BED18E8504D8781D9779F4ADA0BA3E77BB05874AB2015A711479529B9B4BEEF486B6F2293B6F2E01B63D7F372F9043DC7BAAF366B6022
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\524a7981-b2b2-48d3-b260-ddf68c0bbe53.tmp	
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13262335972124877","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6ddf4ddb-e0bb-4242-8486-394fb71e8002.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1708
Entropy (8bit):	5.588702788731102
Encrypted:	false
SSDEEP:	48:Y9VwUK6UUh7U89seKUewqPeUer2UefhX+U4ZwUewUWUenw:dUfUUVU893KUGPeU9UEhX+ULUbUWUD
MD5:	B4FEA418603EE63275ED5322E68EEAE7
SHA1:	698F66C0692ADAA2AB8EDCAB7182307F3A709246
SHA-256:	74C21AE89C46F683B3E4353CB974A52417FF5E29F59B898FB4CCDF91ADFE2191
SHA-512:	DE96BBB65408C5B1FA7C164A225B8A874AAD02B363068D22B16B41F0599D3F51C31BDAEC7C3341302CDE47554B6FA4E468985480D77D15E1369E6FC93ABC3AB
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633642380.341713,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617862380.341716},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1649398380.26827,"host":"e3SziuwfuO2UvuBno+qkR1ObHAzZmSUoJhrc7dbP1Uo=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617862380.268275},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\99ea4232-ccaa-4a1a-8c5e-c845d475046e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.234922262198626
Encrypted:	false
SSDEEP:	6:mrjkH39+q2PWXp+N23iKKdK9RXXTZIFUtpmzJZmwPm6T99VkwOWXp+N23iKKdK9l:2jcIva5Kk7XT2FUtpm1/Pm6Z5f5Kk7XH
MD5:	E33940B2755B5C89F8C6721CB12D904D
SHA1:	24284921E3B3BBDD767E7E83AD0E0A51C411E201
SHA-256:	E1C0E1C539EA06413573D370F0C4EFA93D3A216D29E9E3B7AFAF17FEE07A711A
SHA-512:	45E65FA1B1105F5EED130B3DECEA1AB81F61D0D3B37738CA6C96B12E34615C95F062C01D476F728956B24C955B295158DE65EC729FBD21F608B9079456E46507
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:13:04.169 1908 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/04/07-23:13:04.171 1908 Recovering log #3.2021/04/07-23:13:04.172 1908 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):	5.227215655918383
Encrypted:	false
SSDEEP:	6:mr5kX9+q2PWXp+N23iKKdKyDZIFUtpmWc3JZmwPmWc39VkwOWXp+N23iKKdKyJLJ:25lva5Kk02FUtpmL/PmB5f5KkWJ
MD5:	37DE87D49B02B2D019FFC6BB0E0BF433
SHA1:	07AA98D196DF755552DD3003B8DD22B711D4DC06
SHA-256:	94A2ECDA8EA14DE75F0A0925253A485344126A9ED135A73BA2BFF2EC9C63A6B7
SHA-512:	6FAF29DD103B62652D7E6A4EBF4C583BC280D0EC9D37948DF0770B34A8B82FF20465F7E334F35494E5BF6EE75902C2A0BE48DF8B86336EE1E00ED6C1B94A628 3
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:13:04.163 1908 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/04/07-23 :13:04.164 1908 Recovering log #3.2021/04/07-23:13:04.164 1908 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatab ase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\05a903e08cfdbf22_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	262
Entropy (8bit):	5.710243834917262
Encrypted:	false
SSDEEP:	6:mgRMMXXYlIEG9Ob6a8EuPEHhLp+AIEEY9n2fTGYXhbK6t:6M0l+46jPWhYHEPwPhN
MD5:	66B71CF87B2DF217359843377776BBED
SHA1:	E15376ECADA9305FBD702E824524FADC5F521AE6
SHA-256:	EAC02991DCAAFDC0F6303074330E6DE61276BFF4C6225183159F772B05C45FF2
SHA-512:	79FD6EF5482D2CD5B47DC17075056C7BFAE98534B35B43F88CD124A266C35C8E2472DDF5C7F6CAE60F424880B17B4AA664E57131D9DC0AF05521E512114C99C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....ii...._keyhttps://mamodmiappscn.web.app/dfgtyhgcvxcxzxcx/themes/84663c95639ba690acf716f39df131acnbr1617631064.js .https://mybluemix.net/...8../ .....6C.A....*F..\?.$..O.....yK...A..Eo.....a .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17474f55ef485b09_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	533
Entropy (8bit):	6.14156224825281
Encrypted:	false
SSDEEP:	12:C9Gs+0fql92u3avX57Tka4kXThCtD4kwh8+x7:000yBqBTdJjhC94kS8O
MD5:	9E35D67DFBC82D8061027BE0E79201C1
SHA1:	F03C7D37E03D13ED4DC68026F3E94B4EE0372EC4
SHA-256:	E9D29BEE0AACADE846F1735AF5B63B10EAACDEC4EC479C60A571824DFA28F28A
SHA-512:	C9BECFBD1AADD3D3B8565F2A2E6A9CA35A0A823F88C4B22DC9156B43E7782714B3AA9DEA15818570B73DE36F84DF197FDFCA72787150BDCD0AD891644EA67 CC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....%....._keyhttps://sslcnd.aioecoin.org/bDFJcXd6cDMyaS9ORE5vSXdNVGdLaW9oOW14Z2p5M2NGSE5vd2xWWnAwYnlKbkhreVc3aG1xeVB4NzhCbkNz RG83QkZkNVFidWdocGxpaEZGbWhoMHpMZ3l1T3dDTkhsU3h0NkpZelBoaklUdWlxaW1rQlB1MzFLbkQ0WWxjWmFPU0o1YzZxbTAwc3hzU09saFhNNXdwMng0 NE1DVTAwU1Jtd3FGQWVIR3o1Nkt2U3UxNjFWdXZSdVZnNWFtSHB2enFmZ2oyRkExWFFwWERZUVZ5dFNvM1ZseWN2UEVkNmhCd0kyOVd6RUZHR2djMXlBMUJH UjFwSzNiSUJYQk1xZg.js .https://mybluemix.net/\<.8../.....7.....bJ.PA.w.*)...{.nD2...>{....I.A..Eo.....-y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1e5ef1f4d4da98c0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	249
Entropy (8bit):	5.641432241943564
Encrypted:	false
SSDEEP:	6:m5YlIEG9Obp+VFW0e1JZ+ltP7hoTSPbmbIAfK6t:ll+4sM1WtP7hoTSabX
MD5:	FCFB9753CCA38EF8E7B5DD4997583152

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1e5ef1f4d4da98c0_0	
SHA1:	2553A2C7F5D3E3501A5C8EC299CCE89AFFF38ABA
SHA-256:	EBB4C674E22B09C37189F80EB106A974261EDC91E07E87C05F62833DD7B3B7DF
SHA-512:	F6CF6992AB386C6032CA75FB2F9C1C9D753F0281E052219005A249FE27A2EBA320897C507D28A9D649A0CEA62E79F7C86A69CE1C30BEC55A6D4D684ACB562D0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u....J....._keyhttps://mamodmiappscn.web.app/dfgtyhgcvxcxzxcx/themes/1419a0bd7c8e13fc51f9714c675afc17.js .https://mybluemix.net/...9../.....u..=..%0.....G5.G.S....g(...A..Eo.....j.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d3807be645f8dea_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.50789387864581
Encrypted:	false
SSDEEP:	6:maL9YET08NmAjEIPMmKANAQSsWW40rK6t:lg8NmAoyMRowGd
MD5:	4EAB9766EBD706CEEEB23CE5C09DC1D2
SHA1:	5DDC5634609CE251E0CA3B0F049F0BE9071B8B16
SHA-256:	F463D3B2BB9481F4D9E61F3CAC125A705E0F418EEA1FF90CDFF323A27C684A33
SHA-512:	5C308F896CB5FDD8072DE67A0151F44379626F051DE35AB323B3C260FE68B94832CEC4CE5927684612471B56CC6776F1B752CD50FE8C02E482B9CDE63FC1DA8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y...b..v...._keyhttps://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js .https://mybluemix.net/(..8../.....(.....:J.U.J..8...&...~nK{./O.@.@....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6c179afef040ee7b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.539570920376703
Encrypted:	false
SSDEEP:	6:mMPYeD1cJfIWnQ7NXD1pmZ9+yZ3FEvU+4+bK6t:NZDCJfIWQdDrmZ9hQU+F
MD5:	743A93A13326CD70E9498E102FA26E0A
SHA1:	157C269C35093978F4E39A810682AD53249692C7
SHA-256:	C714CF5B32FBC45C52E44DB4E02452508743B9DE53131BB0352105BF55A1B61E
SHA-512:	4089D1FD6C9D9256F217FC4D469FBA7E2BD001FFB52054133155C7FE10FA93B939EDBC3E5D0EE331CD04F44D2FEA41D7D1C8C545DDDDC084F99DBE9A8F17C6C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r...+.@....._keyhttps://codesandbox.io/public/sse-hooks/sse-hooks.cb2ef05bda555d18c964cf27a52aebac.js .https://codesandbox.io/...8../.....sx.....>j1..,#T,.*..R.K.2.tSA....a..J1.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7c0b8dbb7aa8807b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.403006247559422
Encrypted:	false
SSDEEP:	6:mll9YeD17mEXXD1K1UQnLe59kH4c/ZK6t:wvDUUDwUQLU9kfr
MD5:	167B0992A6F626D46865564613B97BB6
SHA1:	0519A79159B32881FBC00847DB544FA19AD5BFCF
SHA-256:	549404ECA9E891D4FF05F47B4F3BD27E01805BC45F73CEBB1B83FDC99A7C31C6
SHA-512:	ED4B3BC19C9DE17512F7443520C0301659F45891B016A761EBC479D33096471206D956330A17B08E837D069EA855A2D1E62D42987C5BDFA8DC00D0E98F295A1A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q.....B....._keyhttps://codesandbox.io/static/js/banner.8d93e521a.js .https://codesandbox.io/.k.8../.....tx.....-2.Ro.3C...6.P..)|.=.k.....A..Eo.....1bC.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\81cc3335c6a78fef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\81cc3335c6a78fef_0	
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.519225695100466
Encrypted:	false
SSDEEP:	6:my7nY0OCZl+HHHMk4yrX9Z+5OfltDK6t:X7dnIqMkH9Z+5OfR
MD5:	3EBF5448B6B5748134299EDE4F864339
SHA1:	734DE1F580788813C132482254F197ACD8318162
SHA-256:	C235B51DA4A80375139B2EBBFF18B2ECD597D91126081EDFBC3662044C79DAE4
SHA-512:	860B87F87F473C90BD40E575ED5312548F7ADF8F892D2D43B04CD599DDD4941DAA024CB684D5771B28E52CB3C419F5236E9E637060C1223F55397986B3E358AE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...{....._keyhttps://unpkg.com/vue@2.6.11/dist/vue.min.js .https://mybluemix.net/IB.8../.....P.....t..?....!.....B.LQ.....jT..A..Eo.....FDI.....A..Eo..... ...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f02ce8f1f8eee69_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.485767726879466
Encrypted:	false
SSDEEP:	3:m+lUR/gv8RzYRhmHT8NWQABKidFvDWicLL0ge4v1lHCLnslllxXVEUT5mtvhllX:mgEYSHT8NWQA8kzLswzT4tPK6t
MD5:	9AF5725AFC49D92ECCF7702DCEC50E91
SHA1:	72797847451DFEF37B623C0EA4DB5E682B91263E
SHA-256:	EB2A2B5F232FAF86B3765D6CCBF599EB4EF486CE5E5A989B6AE8B1BFFA87F9EC
SHA-512:	6020D7C510BEC623DA5372304E8B65C9926E854768F9FF27E2E9B2FDBC9B2088ACCE9FB050B1A3FB3B9354C3C21223013376DB4B4AACA7912FC90E413A59BC0 E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\...\X"j...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js .https://mybluemix.net/mI.8../.....)...$...:dM.<.r.E..b...)L..\..A..Eo.....T.. .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b6ef8681c83f6864_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	262
Entropy (8bit):	5.668448004394957
Encrypted:	false
SSDEEP:	6:mM3YlIEG9ObJScpFAnngBRf6CpF6B1J6Pee/ygrORK6t:4l+4JScDjBPCBz6Pee/Or
MD5:	4BB82958897CC20715450190070212DB
SHA1:	8404D969706D62AAE189D3AAFB7127A359326381
SHA-256:	6DC798B8B7C07EBB133AD7C8EEBC8CE7BE20A2002A0364F58D76DC123E6BA3AB
SHA-512:	752F74AC71CA001CEA6B744578CEFE5CAAF209F166BC3A9ED7517656C1B0A8DC58C13C972984E355F18D120AC6B5C51742585AD3B2F071255F7ED385C4FE5A D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i.0....._keyhttps://mamodmiappscn.web.app/dfgtyhgcvxcxzxcx/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301617631055.js .https://mybluemix.net/t..9.. /.....UWB\.9"....ud_.[4..vSP..|@.p....A..Eo.....XU.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c1a6fa7c31c3ccdf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.476704427387075
Encrypted:	false
SSDEEP:	3:m+le/FK8RzY0OCLGKIKEkVLKPBMW7K7WFvDWicLL0Qv7elHCSXeWvMjyhyP5m09J:mbY0OCZIfkVJMsZSkWhyP4uK6t
MD5:	5B2146AA3272BD5512EE5BB426EDBD48
SHA1:	9CC71A80747B5351226658D58471F249949CA9C0
SHA-256:	07316279721C8989B24E5873C8B11E7979A97BF10C5C73182C7F2BA8C2D2F971
SHA-512:	1F155FD67997C11B17764B009CFE1A2095D7159A6EB90E2E9F78A9D31C24EC3F721C1ADBCF4081DA41A1D01D8B4105D69A2C20D4D7EAFF7CC08AE10F2A14C1 3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c1a6fa7c31c3ccdf_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....`....._keyhttps://unpkg.com/axios@0.16.1/dist/axios.min.js .https://mybluemix.net/...8../.....$7.a6o..Q.1nH.K.G...O.....IG..A..Eo.....lUL.....A..Eo.. .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c6e1780a88646c8d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.465012921535261
Encrypted:	false
SSDEEP:	6:m06EY0OCZI5B5LZzEhLEq2TZp5q243RK6t:kEnI5B40zqr
MD5:	93E7C9B012159B93C35DC979693549C3
SHA1:	6E968E693079F20A121E225D753916E07C06A1DA
SHA-256:	F90A780525A9F9A9059900674C593134060CBADE962B39E2738F0E3216AEB273
SHA-512:	1A90939879809DBD1E29ADC7A0A19F58307EE32E0EDEC90B8BAF39F35EC548E7F5682DC6D39AB7D64D29C7B0420B2FA54FBD1438EB82BD638821AE759A0813 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...t....._keyhttps://unpkg.com/lodash@4.17.4/lodash.min.js .https://mybluemix.net/l..8../.....7..v.-u.E.b-.6.._z..H.G....j.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ddacd2c15f59d922_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.491237775242284
Encrypted:	false
SSDEEP:	6:msUYET08NmAjmNaHMl7KyBtlSQzAC9RK6t:Cg8NmAjmNaHMhntlSsV
MD5:	55BFD8FA3FC3926F8A980533DD2C1692
SHA1:	38EB9C03268BB64515D6FF17D581E6107A274BDF
SHA-256:	8AD7D172089172B904835B818259B9F384958802C2F1D250A7C6A6FA2F095C59
SHA-512:	E725F2B0F298E3B51DC50E983CB02C6D470354CED261E5A87AE5F8B26DDF0FDD70D845A4D68408CF46604BF7D3F7431374A02D6C3D36573B9F3C23D05B90284
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a....^....._keyhttps://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js .https://mybluemix.net/...8../.....t.....!lh..PC.9..'..9..ozr...d..Zt.Z...A..Eo... ....+8^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ef21b07c6ae2decd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.524929510992898
Encrypted:	false
SSDEEP:	6:mUcEYET08NKB8Nq8dsr+161I6OQ8YWHc6uEnJ4K6t:pc0g8NK8srK0I6gYWYEJa
MD5:	78EF375CF41AC7A026722C904BD02BEF
SHA1:	96FF8874DF5EE18865FAB1CFA5330B96B81C4BA3
SHA-256:	88516BFDB2795862201A984F58DA5270C0CEBD4812CC91097782E4AC1C056F5D
SHA-512:	384370EB89E6A6F557288F6392A68C48185BCD292067BEF145CEB12B207574ABA4B826A6098E265191B6719267A1AA0E0926F51FB18DA595CC4FF912836E0C9B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....._keyhttps://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.js .https://mybluemix.net/]..9../.....F..f..Y.P...k..<.4.*'z.\..Z. A..Eo.....!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f747e026eefdaac9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	5.478351247678476
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f747e026eefdaac9_0	
SSDEEP:	6:moVYET08N2AITPNMXqGjILNLxMtBnN96GH4llhK6t:pg8N2AuCX9jHthv6+8
MD5:	857C70DECDAEDA30EECD0F9EA4B77787
SHA1:	3D61018F0DD7D6CB8C4CB3587139D834C917A3A1
SHA-256:	6AE81C1CC1C0C9F7D7241433A93C461EB25766D0B88F93E98AE746BE6D28B09C
SHA-512:	041F9490A2EC172E47CACF554E96E203F41A607AD86D4D72977463E28E3A18F3D82C5A28C14A40649DCC8A7924C1AF40A7AA723636E72A7F697C942A0478E6B1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n.....48...._keyhttps://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js .https://mybluemix.net/...8../.....9.....pl.....0....d\.4.d....7.....A..Eo.....<..A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f778065137f2cb2f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.502158189120299
Encrypted:	false
SSDEEP:	6:mtDyEY0OCZIm1sRsQEHhvAOVDEgRBfrem8K6t:6DyEnImkVEB7v30
MD5:	10AC95156EE9F24BC5E1EE5C4B5621EC
SHA1:	19515AD8485BA274066FD9BB49C072AA218885F5
SHA-256:	1289F293C02E3DC7F0C057A945EC720993E179B36ECFF8142779A3817ACBE17C
SHA-512:	A3814CBF221DE71C7B9914E1ABBB36A3D7BF695DF6FB53C9C6A3E624F366374F7EEA3564B2D4F1E302000451BAE1CF885E09DA7C898DB0520FA55CA962B43B8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U.....,...._keyhttps://unpkg.com/vue-router@2.7.0/dist/vue-router.min.js .https://mybluemix.net/=..8../.....{...+b..=.=...>...vK.:....{.A..Eo.....".V.....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):	600
Entropy (8bit):	5.094944228301736
Encrypted:	false
SSDEEP:	6:XSoGTjFCsEYAYIteYdD66ksNNHMedHMTdMKARKev1OtozQ3zbn3pHkQ+IRwHsn:DGv8HYSTAad6O1gGzyz7V4hs
MD5:	0626FDF243BADC451A98981048D05528
SHA1:	BC45EB1E9340216ECAFD282DD04A529E36497DB3
SHA-256:	AECE2664B54BB1853B2BCCF60294375C66B7D7759EEC50753D0EFDF87C56F505
SHA-512:	08E2099240D87E8A24DCAF2335E7515A5CCBFC9C033947A4F1F23C345878DF3AEF5CB9C12AC4145DB5A328DD73F4B584F0ED0B1664F11AE8E49772F7EE372D02
Malicious:	false
Reputation:	low
Preview:	P...?I..oy retne.....0.....dh?...W.9../.....^....8../.....j|.!....8../.....ld..x.....8../.....".Y_.....8../.....&.G....8../.....i.....8../....._d..8M...8../...../..7Q.x....8../.....53....8../....."....8../.....1|.....8../.....[H.UOG....8../.....{..z...|@..8../.....{.@....l@..8../.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q...._.KPu../.....+<P|...X.KPu../.....5N.9../.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.8511397610281182
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwaI5r/1AcYBV:TLyqJLbXaFpEO5bNmISHn06UwHr/JYBV
MD5:	2AFAE595DFE1146261A95113FFBF42BB
SHA1:	8A56EF6620E494E0CD4E0EC9A3273B5B7D37E7EC
SHA-256:	7FAB15BCE219DB04C93DEDE3CB1F398B2C550727C67CF19351DA50AC7A31D79D
SHA-512:	74A4692EC418823F3EC84142B1CDD6332D2D85C0A53A720EF001E7CE20C306CFB62B37D1BB8711020B421BC0C6D14A74F85F5AF1D0D3C7B02B955EB7D8A0084
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
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):	0.9681372593961077
Encrypted:	false
SSDEEP:	24:kcLgAZOZD/uqLbJLbXaFpEO5bNmISHn06Uwh8:k8NOZuq5LLOpEO5J/Kn7Uu8
MD5:	75FD76732CD2F6841E62B489562C7152
SHA1:	2FF6CD73E0EDA45EA47A0F64438A21956D1447E1
SHA-256:	9F7141F64EC86686CFECAA67FCADB239F29DA77EB94516ECEFADB479992BB758
SHA-512:	53D8F9BFCC92FB07EAEB88C9A6628A99419FC0EC48940BC055BB308FDA832090570727D74238E9C91BF0832941C21020AE7CCBC88369B9EC276C0B1F1292139
Malicious:	false
Reputation:	low
Preview:	.....m..... ....

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):	14806
Entropy (8bit):	4.217658090363566
Encrypted:	false
SSDEEP:	96:34qMYSfrjkSWVbgSkSxnatDqpHeSFUSOSxAdatDqpEeSFUSpSzO9DSklSDSfMV+u:3vME2DqTtDqKMoILHSNm3O0/
MD5:	970187E9FD08FBE6C702A68C0410723E
SHA1:	E8B6BC6C525473F145EAE5C1DA20063810E89E75
SHA-256:	8DCD2137AB3C6E070E6DAB99302D6FE7EB7BB12CF847D7B9D8811B8AF123DB95
SHA-512:	3F13BF36B4DC4269C7DCBD93BA18E0A716D8E1A58D14E2B9E72FD893D18B829CC37E48A5327B62E529EEDB8C90E99CDADD3DBA3D072645C6275166A1E34CD B50
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...84bd787a_4f0b_4e6c_9a10_9edaa99921b0.....ir..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....L...https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net/?bbre=zox9soxzo.....h.....`..... X.o.... X.o...@.....X.....X.....L...h.t.t.p.s.:. /./.u.t.a.i.z.x.o.x.u.x.z.u.s.a.c.x.c.x.-.d.a.r.i.n.g.-.c.r.o.c.o.d.i.l.e.-.w.b...m.y.b.l.u.e.m.i.x...n.e.t./.?.b.b.r.e.=.z.o.x.9.s.o.x.z.o.....8.....0.....8..... ....$.....https://1dil9.codesandbox.io.....@.....

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
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):	5.26922811102547
Encrypted:	false
SSDEEP:	6:mrJarjM+q2PWXp+N23iKKdK8aPrqIFUtpmJauXZmwPmJauqMVkwOWXp+N23iKKdr:2w/M+va5KkL3FUtpmw+/PmwBMV5f5Kkc
MD5:	8C1BCB06998A004B828AA422BB99D3B7
SHA1:	82BB22F03F7ADE8E27BA3E6FFA8C09D02136D412
SHA-256:	DD812599217341C9CD39A0F048B1158572D2B1948E3D9BF68E800D1B65342C7E
SHA-512:	1F8902FC994CA6965A1354E8BA03EEC5AD3B46EED1BA6F78ADBA8A7D45B0C91E524FFD465FEB57989A334519BECA9249B497867B1E2586001367CB4C81EB479
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:12:52.491 158c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/04/07-23:12:52.493 158c Recovering log #3.2021/04/07-23:12:52.493 158c 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Reputation:	low
Preview:	2021/04/07-23:12:54.548 14d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/04/07-23:12:54.549 14d4 Recovering log #3.2021/04/07-23:12:54.549 14d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/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):	28672
Entropy (8bit):	2.441850405014634
Encrypted:	false
SSDEEP:	96:yBCVSuslg090ySrslXYXSfMVYoScStSWKSfMVtS8SMSRS4f3eSfMVYoScStSOAKm:IG4hY+MyXXMMrMykg3M7
MD5:	204F58C845E4776DDD7EE57DD533808F
SHA1:	0506C16D189ED170312D0013D7254E30806C4A39
SHA-256:	1D0A143A5DE8020D557BC19E48DD78339F5E5E6D93A418E0ECE7BAFCBD7455C4
SHA-512:	EF413DDF74B51010531B1AEC3778A58FAE5F0DF62266E06ADC339CA6899152AF3CA23C5D3863103F307EFADF8DA9B795FD8A1B06802389CF10E46962AFB3489
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
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):	30356
Entropy (8bit):	1.4230411856596874
Encrypted:	false
SSDEEP:	96:IydBCvGS/SCMKSfMVtS8SMSgXSfMVYoScStSs:FLlXMB+My3
MD5:	A6FA0A8B2BEF883195B7E2747CE720FC
SHA1:	C009CB7DB8488C1D8D1BADAD998F600264099AAC
SHA-256:	4F2A5648FC551E02256BB4BC1E4A1D93102907C69754E658260070A263CBC8FF
SHA-512:	B2FAAB305959468E07A77002EBC3ED4DB3F02FD410CF7709E83B2A3AA970D2B9EFD80F4BD760A59274AFB5D410FF2DE934C2ADFD6A0BB63D703B8BA91EDE2A3C
Malicious:	false
Reputation:	low
Preview:	.....k..... ....

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):	5.279371816774264
Encrypted:	false
SSDEEP:	6:mrL9+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpmiF/3JZmwPmd9VkwOWXp+N23iKKN:2Mva5KkTXfchI3FUtpmiD/Pm15f5KkTM
MD5:	A8FE7D5F92EA02B1B9FF3421BC54099C
SHA1:	BE4901B15D6E8808CCC2BF4E1FCC34545F13B77A
SHA-256:	F1BB66CF30F8E70EFBCF4A78B83C6D5103EA9EF9CB091E45AD77BA4340D84CAC
SHA-512:	BD47834F1F5EC77419B2F67144651D1B73E5728F533EAB89AF8F53C707CD87D16B1CFD30C8325EA6E80CFED123D76AE3778C2B23E20A1BB6FA57D0F9816B4C54
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:13:04.135 1908 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/04/07-23:13:04.136 1908 Recovering log #3.2021/04/07-23:13:04.137 1908 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Size (bytes):	358
Entropy (8bit):	5.208437556055205
Encrypted:	false
SSDEEP:	6:mrU39+q2PWXp+N23iKKdK25+XuoIFUtpm3JZmwPm39VkwOWXp+N23iKKdK25+Xu6:2UIva5KkTXYFUtpmZ/Pmz5f5KkTXHJ
MD5:	07AD08195FAD1BEFB1B251E68858B3AF
SHA1:	04AE10423EB70AA641E1461363657ED6B239EBCB
SHA-256:	F544D55C6D9514E67EDDB2D2C80C079C4A5BF8403E046FC4F7F3E15486B14D70
SHA-512:	057F8A6CE88D737446CCAED2807540E5FCF6B4A9E044188C39BDD102A52E20A2DFD63F89735E0A4EB7DFE629E0F05AB7438511BCC1B34CE5BCFF0749965145I 4
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:13:04.129 1908 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/04/07-23:13:04.131 1908 Recovering log #3.2021/04/07-23:13:04.131 1908 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):	5.2292105946674665
Encrypted:	false
SSDEEP:	6:mrC9+q2PWXp+N23iKKdKWT5g1IdqIFUtpm9VXJZmwPmFkH39VkwOWXp+N23iKKd6:2hva5Kkg5gSRFUtpm9V5/PmiHz5f5Kkn
MD5:	850B96AAA10C36142059037E38F44079
SHA1:	0A86F0F6E63C9487AEDDEB931C0055DD51DD3578
SHA-256:	09F72F05C3D9FB1D1D8695B00C866A9DEFFE71AF68A31A1F4F13F21F3589DDD4
SHA-512:	72792A06A662618CB8B25411ACD60D12259BA8BE3DC9BFF60ECA2682DE1B9A723D5FA544675500E8C43F175DD8F127E610B773A9E03F01EB95EA5FD8BC870E5 7
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:13:04.107 1908 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/04/07-23:13:04.108 1908 Recovering log #3.2021/04/07-23:13:04.109 1908 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	90112
Entropy (8bit):	1.101162452183737
Encrypted:	false
SSDEEP:	96:eSYSmS6S+qCdFWKSqStS91SfMVabSqSISwS+bjGEx9iKSfMVMhSuSqStS9lS4f3/:PKFW1MYLd9iXMsUMYp69+g9Mm
MD5:	C5E599CECADCA3DF4E9506ED442C855C
SHA1:	0257C69BE17BD757400EBB05F14DB98EA932188D
SHA-256:	5CFBA17245FDF80A5FC9E5277C46AB5DDFCE67BAB37AA27FA00FED2BEA078086
SHA-512:	4FD265757E583ADC3E0E1CB202CD97E3A69848BBA9336B29813713768504115AB22810409918E30AFBEB9535868F8063C55B448CC4E160AADD5FD498403377A1
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):	3122
Entropy (8bit):	6.303750335531746
Encrypted:	false
SSDEEP:	96:ANSP4Bhi/Pa4h7DVycSAVuynjPSFESBoSFVSqZvGnN:SMJAcXVuynQfZON
MD5:	70CE12FE1C3AC3E056AC3AB17820D653
SHA1:	56F8B617232EACDBD30E20F071DB048FE173E10C
SHA-256:	A0793AAF8101E65AD5CA344D1FEDCF50D1C409731EC5A2242B360E9C632CB03B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
SHA-512:	EBBD89AAF21FBB598B6A56E941C7448723D1BAFECE1DE28D1EDC32BA92EA3957CA0B87405C413929A8C71245A398DD0BEBFEC2302D0C37825D45B7AFA3F01B63
Malicious:	false
Reputation:	low
Preview:	....."".....B2b5qvkkhzqwcpa0ym6cw4olewdovqdy1x64aj7o9fzqybckms340ds3e2r2c1dxwms..365..b8omulsaenqfya3..bbre..crocodile..daring..https..in..mybluemix..net..office..pk3bc4ut7dkqrs..sign..utaizxoxuxzusacxcx._w4r2x3r4hrfcy8klpxmdfl7brc74lu45bbjpjkezj6kq2ck8ogb7gyivtwmuk3vcxiy7w8fukunuardluu3mkshdxgjcbla..wb..with.'wkxfqc1ksv5ddqvxm6qyruhjnxlodczuieba33q..zox9soxzo.Jztb8um7vuvndu8udql7tgm8zeeonepmnzuccagvcuzwdaeratmswfd7eijgwdsrhvebtxpjauz..1dil9.fahr0chm6ly91dgfpenhvehv4envzywn4y3gtzgfyaw5nlwnyb2nvzglszs13yi5tewjsdwvtaxgubmv0lz9iynjlpxpvedlzb3h6bw..codesandbox..en..io..sdocxo*.....1dil9...F.B2b5qvkkhzqwcpa0ym6cw4olewdovqdy1x64aj7o9fzqybckms340ds3e2r2c1dxwms.....365...j.fahr0chm6ly91dgfpenhvehv4envzywn4y3gtzgfyaw5nlwnyb2nvzglszs13yi5tewjsdwvtaxgubmv0lz9iynjlpxpvedlzb3h6bw.....b8omulsaenqfya3.....bbre.....codesandbox.....crocodile.....daring.....en.....https.....in.....io.....mybluemix.....net.....office.....pk3bc4ut7dkqrs.....sdocxo.....sign.....utaizxoxuxzusacxcx

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):	91860
Entropy (8bit):	0.6658598978757689
Encrypted:	false
SSDEEP:	96:6cKSqStS9nSYSmS6S+mNNCuMSfMVabSqSISwS+e9qEsjUKSfMVMhSuSqStS90:6cBNNnNMYu9o4XM1
MD5:	FCB9DB71BC859F8DF8F64CC167BDC177
SHA1:	EC805668AEF91648510E7AE7B27F52BC872CACFD
SHA-256:	CFD1F261653C23B4FF5D58CD8C10C96AB3AB6CCE848A137F78743DC3B01A3F83
SHA-512:	280FF8EE1CF77B5908D46CE458187C8E3A6DFD97842F8C45E0DF023826DFE21914B6FD41B3C280E8BF9F4ED0EDD46564DCF75CF7EA91268E5B4AAFF8728429A
Malicious:	false
Reputation:	low
Preview:	.....8Yh*..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3580
Entropy (8bit):	5.525309723134802
Encrypted:	false
SSDEEP:	48:hHIpTpoklVr/swGGWLha73MG8dbVXn/bQSefgGSNrS0U9RdiN93A:hopG2Vrs9a73MddbVXn/bQ5fgG+rS0BA
MD5:	A8DE5DA373DE17014B8721344E18FC21
SHA1:	5A22D46A3EE986312378C2BE0C3CF81EB65FED0F
SHA-256:	3814B6B11F473BC5FD813AA3DDEA67ABDA0CC11A9767DEA4DC0EAA4EC23B3E49
SHA-512:	CB0BE145A1E22A4961135BF3797DFFC96FAD62A8F9B86FD73DD0B18815235632166E314F76DDD5F182DBBB57B624C04B5F4F9AFACD2F9832EB8ADF2429EC39A
Malicious:	false
Reputation:	low
Preview:	M..j..*.....AMETA:https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net.....I_https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net..browserkeyP.{"browser":{"detect_browser":"","detect_browser_detail":"","detect_btan":"ok"}}.F_https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net..userkey...{"user":{"keepLoginLongtime":0,"AuthNBR":false,"AuthKeyNBR":false,"tk_nbr_uc_frv":"","br_nbrcheck":"","br_utcheck":"","testlist":[]}}.V_https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net.._canWriteToLocalStorage.H_https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net..nbrteststst...../.....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..591771000.H_chrome-extension://pk

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):	5.187992522962451
Encrypted:	false
SSDEEP:	6:mrJa/AOq2PWXp+N23iKKdK8a2jMGIFUtpmJaRXZmwPmJazFkwOWXp+N23iKKdK8N:2w/AOva5Kk8EFUtpmw9/PmwzF5f5Kk8N
MD5:	EEE8B3EB8DAAF4199E3E311C99236B6B
SHA1:	C70695286CF33C7CC118D31627C0504988EC496A
SHA-256:	6B0640957511FAE33FD4F6FD32942DB4066611CBDDC4741316FA70E09E75192E
SHA-512:	6460820F1D6996A4A3828578A06AC75FB80900EB4AF102E807E634FA3086FD968436311D56CA05F5B8EBE3B5B759B90A09758D00D53372DA0ED684AD660387AC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:12:52.170 14d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/04/07-23:12:52.173 14d4 Recovering log #3.2021/04/07-23:12:52.179 14d4 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.199583613138667
Encrypted:	false
SSDEEP:	6:mrJaxdDM+q2PWXp+N23iKKdKgXz4rRIFUtpmJaegZmwPmJaeDMVkwOWXp+N23iKj:2wxW+va5KkgXiuFUtpmwT/PmwDV5f5K2
MD5:	36B2C9C0963FCB0078B732D26CCA6694
SHA1:	3EA0B75062D918F88A070B74931DECCBD58242A4
SHA-256:	D80AE1ABD445E1ACA6D0AF77BAF36BD818B1B879E5FF82D11761F5ECFB95A6BC
SHA-512:	F16FCF0B8019A06422B3A68746C23E25AE144A4DFA0DEFE2DBCB14F4A2B501736028A8EAA3FF545C3237A9E3DFFB1676303EBAD845ED22E8C7ECF06B825009A6
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:12:52.504 131c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/04/07-23:12:52.505 131c Recovering log #3.2021/04/07-23:12:52.505 131c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	28672
Entropy (8bit):	1.2670991112796626
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU1iwl8ulGlckcA:wIElwQF8mpcSrN3kweq6
MD5:	F01547053AD160A9E13F8ABF10B11479
SHA1:	3DA8A3BBD1FBF124C5D4176AE6659987E45BF862
SHA-256:	66898E62C4677ACF25A5B5F93F95D3C158D5419B18075018B7ECB7226BA43A94
SHA-512:	7A1DE50AA6C7DD919D2B4F3E14729E8786F8F9F51EF67E2F5AE902EAA80F3CCADF3A8D0C17AD9CDD63D659F2570BC3ABCF5970476165326B3B2A55D66EE633EE
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6273529105201393
Encrypted:	false
SSDEEP:	48:2sqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUV4:2shIElwQF8mpcSm
MD5:	9BA00D4F85807D0DE8602F0F5BAB05AA
SHA1:	529EBAE741F68A038C2C28F95C25CE5FFC290EB9
SHA-256:	FBBBBEBC9FB587AD9103509287270CD7C06D9DB0F90CFAC34FB1D1FEA0FF22B9
SHA-512:	AD224715A4ADD05F9EE52278A57096AFF9BEC97CE64BA84DE0F21347BF37FFE9A0FA89C3000C4913D2D5E23F5A8A2C2666B06DCDE4AD176DD8ED0BBC45B4C504
Malicious:	false
Reputation:	low
Preview:	.....'..m..... ....

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):	318
Entropy (8bit):	4.716509976443682
Encrypted:	false
SSDEEP:	6:5leulawWuuu36dTxMtXyMLVqRKJef3ul1kAl1kAl1kAl1kAl1:5l7YuuG6dVMlyMURKJKmkAvkAvkAvkAv
MD5:	1D3A076ACA6A59FFDE998EAF0471F5D5
SHA1:	0694F75B98084ADCD46C573A761081CBEBBA7012
SHA-256:	E0420EF6674C97F1A261EC56E918905B00D360A3C9FD8C1103C78C7617470663
SHA-512:	6996AC10F6C98D783F3B8B65B873836CF847ED33FD8ED3DC18E4CD28D35987A7B808469EDC50CB79F172C616FB65CB581CC6EF64AC16BFB45EA6E2F3FF6DE 3D
Malicious:	false
Reputation:	low
Preview:	..&f.....VGD.....next-map-id.1.lnamespace-84bd787a_4f0b_4e6c_9a10_9edaa99921b0-https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.n et/.0&U.93.....map-0-ReadyFIle.{.}...map-0-nbrteststst. ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.184214210972149
Encrypted:	false
SSDEEP:	6:mrJaCM+q2PWXp+N23iKKdKrQMxIFUtpmJaB6ZmwPmJaEMVkwOWXp+N23iKKdKrQq:2wCM+va5KkCFUtpmwM/PmwEMV5f5KktJ
MD5:	B323384B2D1306E90763293194CCA2EC
SHA1:	A9EB7D3DC8D0B1430CC29D6B9037703C561671D0
SHA-256:	35A8670E1B406D08EE82171A3AD0437659EE2CAC7A1388E1B22A3CB4246CE986
SHA-512:	0EEEF51F850D7DE9E6EA37420EA9887E39212B95994BB53F1645121638F602B1E9A797B67A6D2D35570E509EB138EDB8412216212B9365913D7D8C2D52E43B1C
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:12:52.410 158c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/04/07-2 3:12:52.411 158c Recovering log #3.2021/04/07-23:12:52.412 158c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/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):	5.204682620628332
Encrypted:	false
SSDEEP:	6:mrJaaM+q2PWXp+N23iKKdK7Uh2ghZIFUtpmJaJwZmwPmJaH5lMVkwOWXp+N23iKm:2waM+va5KkIhHh2FUtpmwJw/PmwZlMVK
MD5:	B50AA4AAE08305260D971E11038D82CD
SHA1:	D3CD3B06D6D3E3E6557C6970260A931DD3EB87FF
SHA-256:	BA2662FA400727BC5C7081CEE1AB6E70B9555DD5DD03C44E5076A8CFB1F743DB
SHA-512:	115B653ED8FCB8F8CBED9552F6ED8C2E7A71D084E44EB8F2DD936165AF918B29D3118ECCF0DB64865C5DF9982FA0E1F8DFC31ACFC0B243245056EB61396393 A
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:12:52.096 f6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/04/07-23:12:52.097 f6c Recovering log #3.2021/04/07-23:12:52.099 f6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Char acteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\284b376a-6223-4bd1-bcd1-245836f08d66.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\284b376a-6223-4bd1-bcd1-245836f08d66.tmp	
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):	5.2785022440840645
Encrypted:	false
SSDEEP:	12:2wQqM+va5KkFFUtpmw6A/Pmw9MV5f5KkOJ:2Mda5Kkfg0/Lm2f5KkK
MD5:	9DECE987CC1D23A30A567EE8412572EB
SHA1:	06B53DF34E452727B08366AA1340DCF9D7FB75A1
SHA-256:	56B906B73F8FE5A76606649F6653DD7B6F4452B8E93A37CD7084148E8A239162
SHA-512:	A81F305C821479D7845146D95CD90971FD31D01F33CA707AD1BCC7402493BDE45972F5BAFAAB7828DF516EED83B1E88C0A039A41978666DACD618B0493DB390
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:12:52.499 158c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/04/07-23:12:52.500 158c Recovering log #3.2021/04/07-23:12:52.501 158c 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):	432
Entropy (8bit):	5.323883282066868
Encrypted:	false
SSDEEP:	6:mrJaQjIq2PWXp+N23iKKdKusNpqz4rRIFUtpmJaaXZmwPmJa9kwOWXp+N23iKKdA:2wQMva5KkmiuFUtpmwq/Pmw95f5Kkm2J
MD5:	11F1552DAA50EEC599610B4FE0ABC7D5
SHA1:	CDD73E3417E74647403CC794790393969EEA2731
SHA-256:	F4F58EF6E108D59C6A683E0D4A78150641F8AAF2FCCE2F624CAFB0497715DA30
SHA-512:	1F8CA30DBD0E7D22F964361A0E873309031A84C8299D131DBC24DB20109378ADF92111A3397ED45E82BB4065C22565BBEB13F4BA726CB8BAA2A99F975C5A47D
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:12:52.493 1574 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/04/07-23:12:52.495 1574 Recovering log #3.2021/04/07-23:12:52.496 1574 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):	5.306408039599632
Encrypted:	false
SSDEEP:	6:mr4nq2PWXp+N23iKKdKusNpZQMxIFUtpm2uZZmwPm2uzkwOWXp+N23iKKdKusNpB:2Kva5KkMFUtpm2uZ/Pm2uz5f5KkTJ
MD5:	E492DE35B8AD3CE558D9BDD4DEAB033F
SHA1:	83D5B4FCFD135895C6655B55DF1A7A2C5C458725
SHA-256:	3A2D60429CDD61CB56FC27659433956E681033F9331784D0F37293B8B59A5525
SHA-512:	6F26FBD9DC2EF95F8CCEA48C40E152D8587770CD28914E2119F8BD99FEE8290308C0F0C5B60DF84178417B4359DA881A49665B1DFA3859BEB549132C9E92FB4
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:13:08.556 1574 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/04/07-23:13:08.558 1574 Recovering log #3.2021/04/07-23:13:08.558 1574 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\31864252-a5eb-4833-839c-98c63fcf2de4.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"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	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):	430
Entropy (8bit):	5.226209489198035
Encrypted:	false
SSDEEP:	12:2iM+va5KkkGHArBFUtpmo/Pm2MV5f5KkkGHAryJ:2ida5KkkGgPg0D22f5KkkGga
MD5:	07B283F38F4DA71F687464866A27B19A
SHA1:	9B62D8C6236672E05B48181B2160D7CCB06CC1F9
SHA-256:	B264DB0A2895C0A2D7DD9D908B6A0656D91FE86654C771B23233DCAA467A65ED
SHA-512:	64F22EAEF87938C559A2261EE41D05CCB88BBD5567140F1D049717096C4008FC43F16224A924BEA005F3A4F868EB653B77B2C674DDC375A8132C8EDD701581FA
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:13:03.755 158c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/04/07-23:13:03.758 158c Recovering log #3.2021/04/07-23:13:03.759 158c Reusing old log C:\Users\user\A ppData\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):	5.185969102157827
Encrypted:	false
SSDEEP:	12:232y+va5KkkGHArqiuFUtpm33/Pm59V5f5KkkGHArq2J:232Da5KkkGgCg03mbf5KkkGg7
MD5:	FA204CCD78882D41A6F88F3D8F163A49
SHA1:	6363551BC62AB3C96E64496CB3153E2EF83A384D
SHA-256:	9DA72FFA9EAA3CA2C0FD8E71DF6B273D32E130C189362E1916F49BAEAF6A9BE8
SHA-512:	26BD2B099172C3FDBEDAB3681E26DAE5BD50D5C04EF5A8D4C466005DCD4ACDEB42D610AC605A92EDE69032B7F623A0D2E3A4E1D8ED0539DB22E028C425F4 EE3
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:13:03.777 e7c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Platform Notifications/MANIFEST-000001.2021/04/07-23:13:03.779 e7c Recovering log #3.2021/04/07-23:13:03.780 e7c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Size (bytes):	418
Entropy (8bit):	5.206462732045285
Encrypted:	false
SSDEEP:	12:23c9+va5KkkGHArAFUtpm3cU/Pm3cLV5f5KkkGHArfJ:2ta5KkkGgkg04of5KkkGgV
MD5:	4B149DEC1D8F22773C0530C2CCB6C19E
SHA1:	E8DF73182F9D9F314C84FE451FC4868CF0DD6A7E
SHA-256:	E3371B5C9C41FBB0AEC29E1E49C9C4591C77806156910660B2F6C5873E2CA016
SHA-512:	667CBEDACC0EFC66B822CB67BC70CB36CE5B5301095C546E001999BF4C365E5A21C9CD1C232CCB4FF97A530EA74F7988608FA40D11D3F8B44D0516887B997D F
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:13:19.025 149c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/04/07-23:13:19.026 149c Recovering log #3.2021/04/07-23:13:19.027 149c Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.274949299008838
Encrypted:	false
SSDEEP:	6:mrJa2M+q2PWXp+N23iKKdKpIFUtpmJaFZmwPmJaNMVkwOWXp+N23iKKdKa/WLJ:2w2M+va5KkmFUtpmwF/PmwNMV5f5KkaQ
MD5:	197037B95A7BB3944BAACFE4972E0BE3
SHA1:	40D7F57395A603D052E89755885C3A97A748E3E4
SHA-256:	5734B35164E3EEC5F43C9FCE497096B238100A438684A19F95BECF78589B22D5
SHA-512:	A1ED9E98D65A33C2150DF9140A47E9CD531E567581704C31B183BDC7A7F0E366618B60C06FBA7E2644CEF49AE2E2271AC0839E4E1507FB46CA68607D1A874EF
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:12:52.135 f6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/04/07- 23:12:52.137 f6c Recovering log #3.2021/04/07-23:12:52.138 f6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000 003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.330291453662819
Encrypted:	false
SSDEEP:	12:2V+va5KkkOrsFUtpmMZ/PmMNV5f5KkkOrzJ:2Sa5Kk+g0MQMlf5Kkn
MD5:	C6498E6C45E06BEA536E9C624287B6C2
SHA1:	400A6D59F32C8DDA5EFB77829DBD0A643BD9DAB4
SHA-256:	EDD148291FCF05D9DC1C2CE57D0E585BFC048A39D7FB270B138E8B5DC538319C
SHA-512:	7775CA9150BADD6587253F103B8FC633F65375654370E2C1D67166CC1B3C2F8DC4B6E69EA23735C93593562DAEA4B69257B9F6401188452F0AF2A33088279D47
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Preview:	2021/04/07-23:13:08.796 e7c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/04/07-23:13:08.797 e7c Recovering log #3.2021/04/07-23:13:08.797 e7c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	84
Entropy (8bit):	5.085788364651607
Encrypted:	false
SSDEEP:	3:5VgrtmKT/BRSfeQHS+fWl8E6:5Vg42sBSgiO
MD5:	959EF0F96D080B9161516F2DCD9BBA09
SHA1:	DC010ED3FB697D53B6D30CB401E6D16296F57E17
SHA-256:	5D673881D2E90C94040E0A5399C4B8BD2126BCC5E9EED593A8760980D3282A95
SHA-512:	E8D7AF287D4DFE52AC388D3F81C671D6A1425967947A0BD3A0CAEE79F9046BD1EBF637F576BACA168C9E82FFA1D5F965B32A6074827558F81C730A0034115B6
Malicious:	false
Reputation:	low
Preview:	......p.7.G....@.^..j.....k..5..iF.....GG..+.:.....S.....i.2.....e....._

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ac306d00-d2bc-438b-b39e-feb222ba6366.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):	6095
Entropy (8bit):	5.2013255745511975
Encrypted:	false
SSDEEP:	96:n6f9X//4oo2rcV6SA7ok0JCmLRWL8uDk71/SkIh/bOTQVuwn:n6f14n2rccPW4uYFk7AkIx
MD5:	21D8CB5099064BAE319F8E224E4E8301
SHA1:	42A7361BE7F08A0F1BB38FEC878DEEC5F856F1D5
SHA-256:	68653D1C598315FC194E79BDDBB221DAD550616FD4E13C947BF4936C27ED4437
SHA-512:	AF57ADF5098B28873B315F9826B44D1F0891943B2614A265206A4149D9EA5179EDDEFF5B0BFA05E4923D3668DCB1F24824FE2FED5E7CF305CC74806AD95A69F(
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262335972440328","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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.418644349044613
Encrypted:	false
SSDEEP:	3:tUKO4qYUW9Kdj1Zmwv3s4qYUW9aqbASV8ss4qYUW9bMUBhASWGv:mrpdJZmwPmreVVvmsBhVtv
MD5:	8FB3DCC4A026381CF5EC8E8BAC53A032
SHA1:	B02B90F18B5C253944AA8FEFF45BDE46340015F1
SHA-256:	325199856F2A17995F27DF6D95D947BC8DADFDBF55D6B818A161272AED8964E1
SHA-512:	72909378F1259E7019DC3DA20B9F9386A216351DD80007345B66FD23689D7AD17058C26CBFA2336C8AE50B14B4396CB5E44BB745BE4D6388C5FA6F0D9E6B45E1
Malicious:	false
Reputation:	low
Preview:	2021/04/07-23:13:02.883 1148 Recovering log #3.2021/04/07-23:13:02.929 1148 Delete type=0 #3.2021/04/07-23:13:02.930 1148 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e160ccd6-35c7-4294-a0c5-8b22a49f276a.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):	6096
Entropy (8bit):	5.199421700475045
Encrypted:	false
SSDEEP:	96:n6f9X//4oo2rcV6SA7ok0JCmLRWL8uDk71/K4kJX1bOTQVuwn:n6f14n2rccPW4uYFk7dkJt
MD5:	AFC49E7C0EED1AFA38A5A05B5C6B52F4
SHA1:	F82CFBA4964B00761D44E93517036BC948ED3E9C
SHA-256:	2E82BC984FA597EFCF099B3E8A6D587ABE9CFFA1A2C892ED304113D6073AF92A
SHA-512:	671D676055FE5E3D7271C9900E5176D2029D1E59BC113D639D32E1DE054B5C02A38C2B2A49773A2F5916AB57F98816C6BD79BC233DD40901E6517DE422A426D3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e160ccd6-35c7-4294-a0c5-8b22a49f276a.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262335972440328","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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\c4b85f78-e95a-40b1-861b-1f33c9024179.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):	164170
Entropy (8bit):	6.082081983426806
Encrypted:	false
SSDEEP:	3072:sCMZM4iTMFp3l+7LSx8sogeKFcbXafIB0u1GOJmA3iuRc:1sgMTo7JsogHaqfIlUOoSiuRc
MD5:	494A9BE957382CA7F4F3E6599DA76542
SHA1:	2771CE7A92BAE524855E73006272BD0E3E7BE3B4
SHA-256:	E44680E6F085EB5055BFBBB2CD2D4600D2A77C58DF5963B62A9E0998DAD316FC
SHA-512:	9FBF22B9B584DBD8D961F7833E00762368A90438138B514931A3621A2195E7BD1191A0ED3E6E409194629DC6EFE946D8BDAB882E23C20E2E1004D2A1D6E9EBC
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":1.617862375218367e+12,"network":1.617829976e+12,"ticks":94217697.0,"uncertainty":4732116.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510166079 96"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\fbb6de92-d92c-4999-a4a3-159ae03a05c2.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):	164170
Entropy (8bit):	6.082080982076343
Encrypted:	false
SSDEEP:	3072:/1JZM4iTMFp3l+7LSx8sogeKFcbXafIB0u1GOJmA3iuRc:tPgMTo7JsogHaqfIlUOoSiuRc
MD5:	246B1A459DE9110B09358639E287731E
SHA1:	CB4F4B28B51F951DACA6D22296939B785CD1CD8A

C:\Users\user\AppData\Local\Google\Chrome\User Data\fbb6de92-d92c-4999-a4a3-159ae03a05c2.tmp	
SHA-256:	C7534F363C7FB6B159B1F99AF0C5DDAEBFC27E7F6D1B71340A7F4F437433807B
SHA-512:	8E9F6C44B6B4461DBB398C130220AA55075F1EF2B3FF1EFDA8B05AB5C178A9122D93056F8A9ECD0EF3E2FAB74D23D906B8FFFAFC19B62776DF0C49713C7C315
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":1.617862375218367e+12,"network":1.617829976e+12,"ticks":94217697.0,"uncertainty":4732116.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016205238"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Temp\1cb4799e-d979-4458-94a2-d3fc705ef827.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\2f875f9c-5953-4638-931b-dd9f308d9991.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\3ffe17ca-ce2d-4468-ad4c-93e8015207eb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\3ffe17ca-ce2d-4468-ad4c-93e8015207eb.tmp	
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\ee29984a-6627-4a62-9746-8c9cdbde806e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\3ffe17ca-ce2d-4468-ad4c-93e8015207eb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\ca\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CE B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885 B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\de\messages.json	
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65 FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65 FFD9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\en_GB\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\fi\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEA D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4840_951029629\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 82

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 23:12:56.735749006 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.736983061 CEST	49705	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.751610994 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.751705885 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.752136946 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.753170013 CEST	443	49705	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.753283978 CEST	49705	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.753612995 CEST	49705	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.767971992 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.769561052 CEST	443	49705	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.771102905 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.771158934 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.771224022 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.773756027 CEST	443	49705	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.773802996 CEST	443	49705	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.773861885 CEST	49705	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.962747097 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.963727951 CEST	49705	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.963852882 CEST	49705	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.967335939 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.968635082 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.978678942 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.979193926 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.979480982 CEST	443	49705	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.979675055 CEST	443	49705	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.979720116 CEST	49705	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.981493950 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:56.983058929 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.983118057 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.984678984 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:56.997353077 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.023376942 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.053539038 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.053579092 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.053622007 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.053636074 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.053669930 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.053710938 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.172225952 CEST	49711	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.172467947 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.172522068 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.188025951 CEST	443	49711	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.188060045 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.188143969 CEST	49711	443	192.168.2.3	104.18.22.207

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 23:12:57.188148022 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.192908049 CEST	49711	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.205549002 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.205569029 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.205598116 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.205610037 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.205637932 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.205646992 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.208717108 CEST	443	49711	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.210890055 CEST	443	49711	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.210936069 CEST	443	49711	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.211322069 CEST	49711	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.212869883 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.212888002 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.212913990 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.212923050 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.212945938 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.212970972 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.212980986 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.213020086 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.213059902 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.213136911 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.213320971 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.213372946 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.213393927 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.213449955 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.213495016 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.213540077 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.213557959 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.213596106 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.214458942 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.214483976 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.214519024 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.214545965 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.214555025 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.214595079 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.214612007 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.215065956 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.215097904 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.215142965 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.215178013 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.215209007 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.215221882 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.215254068 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.215301991 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.215909958 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.215939999 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.215984106 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.216088057 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.216130972 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.216233015 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.216365099 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.216903925 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.216948032 CEST	443	49704	104.18.22.207	192.168.2.3
Apr 7, 2021 23:12:57.216959000 CEST	49704	443	192.168.2.3	104.18.22.207
Apr 7, 2021 23:12:57.216991901 CEST	443	49704	104.18.22.207	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 23:12:44.250169039 CEST	49873	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:44.263560057 CEST	53	49873	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:44.985379934 CEST	53196	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:45.001353979 CEST	53	53196	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 23:12:45.938410997 CEST	56777	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:45.951411009 CEST	53	56777	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:46.872049093 CEST	58643	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:46.886630058 CEST	53	58643	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:47.642941952 CEST	60985	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:47.655843019 CEST	53	60985	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:48.588443995 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:48.602304935 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:56.712213039 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:56.713712931 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:56.714039087 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:56.714091063 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:56.718156099 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:56.726389885 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:56.726653099 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:56.727174997 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:56.734591007 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:56.743840933 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:57.044411898 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:57.057897091 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:57.109498978 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:57.122343063 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:57.135351896 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:57.158523083 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:57.434472084 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:57.477505922 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:58.182014942 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:58.201893091 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:59.107860088 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:59.134298086 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:59.335300922 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:59.354091883 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:59.754724979 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:59.774702072 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 7, 2021 23:12:59.892338991 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:12:59.932336092 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:00.555902958 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:00.602610111 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:01.462498903 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:02.370129108 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:02.383333921 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:02.456433058 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:02.471668959 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:02.882669926 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:02.882788897 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:02.905015945 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:02.912986040 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:03.092220068 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:03.105268955 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:08.340965986 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:08.360923052 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:08.487587929 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:08.500894070 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:08.607002974 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:08.633276939 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:19.197715044 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:19.212070942 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:19.920190096 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:19.932164907 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:20.676868916 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:20.690220118 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:23.226058960 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:23.240086079 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:24.693845987 CEST	63978	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 23:13:24.707988024 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:25.681288958 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:25.720452070 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:25.777319908 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:25.792252064 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:26.883389950 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:26.897598028 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:27.631650925 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:27.646940947 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:28.616455078 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:28.628503084 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:39.731031895 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:39.745006084 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 7, 2021 23:13:39.787791967 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:13:39.807300091 CEST	53	64124	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 23:12:56.713712931 CEST	192.168.2.3	8.8.8.8	0x2f23	Standard query (0)	1dil9.codesandbox.io	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:57.135351896 CEST	192.168.2.3	8.8.8.8	0x5624	Standard query (0)	codesandbox.io	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:57.434472084 CEST	192.168.2.3	8.8.8.8	0x212b	Standard query (0)	utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:58.182014942 CEST	192.168.2.3	8.8.8.8	0x8d38	Standard query (0)	sslcnd.aioecoin.org	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.107860088 CEST	192.168.2.3	8.8.8.8	0xf1d6	Standard query (0)	mamodmiappscn.web.app	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.335300922 CEST	192.168.2.3	8.8.8.8	0x289b	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.754724979 CEST	192.168.2.3	8.8.8.8	0xbf32	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:00.555902958 CEST	192.168.2.3	8.8.8.8	0x8455	Standard query (0)	bauia.bugcart.com	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:01.462498903 CEST	192.168.2.3	8.8.8.8	0xac5f	Standard query (0)	utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:02.370129108 CEST	192.168.2.3	8.8.8.8	0xb104	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:02.456433058 CEST	192.168.2.3	8.8.8.8	0xac5f	Standard query (0)	utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix.net	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:02.882669926 CEST	192.168.2.3	8.8.8.8	0xcd47	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:03.092220068 CEST	192.168.2.3	8.8.8.8	0x8301	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:08.340965986 CEST	192.168.2.3	8.8.8.8	0x42ec	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:08.487587929 CEST	192.168.2.3	8.8.8.8	0x6335	Standard query (0)	mamodmiappscn.web.app	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 23:12:56.734591007 CEST	8.8.8.8	192.168.2.3	0x2f23	No error (0)	1dil9.codesandbox.io		104.18.22.207	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:56.734591007 CEST	8.8.8.8	192.168.2.3	0x2f23	No error (0)	1dil9.codesandbox.io		104.18.23.207	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:57.158523083 CEST	8.8.8.8	192.168.2.3	0x5624	No error (0)	codesandbox.io		104.18.22.207	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 23:12:57.158523083 CEST	8.8.8.8	192.168.2.3	0x5624	No error (0)	codesandbox.io		104.18.23.207	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:57.477505922 CEST	8.8.8.8	192.168.2.3	0x212b	No error (0)	utaizxoxux zusacxcx-daring-crocodile-wb.mybluemix.net		169.62.254.79	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:57.477505922 CEST	8.8.8.8	192.168.2.3	0x212b	No error (0)	utaizxoxux zusacxcx-daring-crocodile-wb.mybluemix.net		169.46.89.149	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:57.477505922 CEST	8.8.8.8	192.168.2.3	0x212b	No error (0)	utaizxoxux zusacxcx-daring-crocodile-wb.mybluemix.net		169.47.124.22	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:58.201893091 CEST	8.8.8.8	192.168.2.3	0x8d38	No error (0)	sslcnd.aioecoin.org		172.67.176.224	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:58.201893091 CEST	8.8.8.8	192.168.2.3	0x8d38	No error (0)	sslcnd.aioecoin.org		104.21.91.175	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.134298086 CEST	8.8.8.8	192.168.2.3	0xf1d6	No error (0)	mamodmiappscn.web.app		151.101.65.195	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.134298086 CEST	8.8.8.8	192.168.2.3	0xf1d6	No error (0)	mamodmiappscn.web.app		151.101.1.195	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.354091883 CEST	8.8.8.8	192.168.2.3	0x289b	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.354091883 CEST	8.8.8.8	192.168.2.3	0x289b	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.354091883 CEST	8.8.8.8	192.168.2.3	0x289b	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.354091883 CEST	8.8.8.8	192.168.2.3	0x289b	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.354091883 CEST	8.8.8.8	192.168.2.3	0x289b	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.774702072 CEST	8.8.8.8	192.168.2.3	0xbf32	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Apr 7, 2021 23:12:59.774702072 CEST	8.8.8.8	192.168.2.3	0xbf32	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:00.602610111 CEST	8.8.8.8	192.168.2.3	0x8455	No error (0)	bauia.bugcart.com		172.67.166.7	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:00.602610111 CEST	8.8.8.8	192.168.2.3	0x8455	No error (0)	bauia.bugcart.com		104.21.11.124	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:02.383333921 CEST	8.8.8.8	192.168.2.3	0xb104	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 7, 2021 23:13:02.471668959 CEST	8.8.8.8	192.168.2.3	0xac5f	No error (0)	utaizxoxux zusacxcx-daring-crocodile-wb.mybluemix.net		169.62.254.79	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:02.471668959 CEST	8.8.8.8	192.168.2.3	0xac5f	No error (0)	utaizxoxux zusacxcx-daring-crocodile-wb.mybluemix.net		169.46.89.149	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:02.471668959 CEST	8.8.8.8	192.168.2.3	0xac5f	No error (0)	utaizxoxux zusacxcx-daring-crocodile-wb.mybluemix.net		169.47.124.22	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:02.905015945 CEST	8.8.8.8	192.168.2.3	0xcd47	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 7, 2021 23:13:03.105268955 CEST	8.8.8.8	192.168.2.3	0x8301	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 7, 2021 23:13:03.105268955 CEST	8.8.8.8	192.168.2.3	0x8301	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 23:13:08.360923052 CEST	8.8.8.8	192.168.2.3	0x42ec	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 7, 2021 23:13:08.500894070 CEST	8.8.8.8	192.168.2.3	0x6335	No error (0)	mamodmiappscn.web.app		151.101.65.195	A (IP address)	IN (0x0001)
Apr 7, 2021 23:13:08.500894070 CEST	8.8.8.8	192.168.2.3	0x6335	No error (0)	mamodmiappscn.web.app		151.101.1.195	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 23:12:57.766895056 CEST	169.62.254.79	443	192.168.2.3	49713	CN=*.mybluemix.net, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Apr 11 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Thu Jul 14 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 7, 2021 23:12:57.780838013 CEST	169.62.254.79	443	192.168.2.3	49714	CN=*.mybluemix.net, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Apr 11 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Thu Jul 14 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 7, 2021 23:13:02.780728102 CEST	169.62.254.79	443	192.168.2.3	49731	CN=*.mybluemix.net, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Apr 11 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Thu Jul 14 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Apr 7, 2021 23:13:08.537244081 CEST	151.101.65.195	443	192.168.2.3	49741	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Mar 17 19:54:48 CET 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jun 15 20:54:47 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 23:13:08.537295103 CEST	151.101.65.195	443	192.168.2.3	49742	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Mar 17 19:54:48 CET 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jun 15 20:54:47 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4840 Parent PID: 4900

General

Start time:	23:12:50
Start date:	07/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://1dil9.codesandbox.io/?bbre=aHR0cHM6Ly91dGFpenhveHV4enVzYWN4Y3gtZGFyaW5nLWNyb2NvZGlsZS13Yi5teWJsdWVtaXgubmV0Lz9iYnJlPXpveDlzb3h6bw&en=sdocxo'
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: 5320 Parent PID: 4840

General

Start time:	23:12:52
Start date:	07/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1508,11063469092212728 4,6560826107686931846,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1788 /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

Disassembly