ID: 404208
Sample Name: PaymentAdvice - Copy.htm
Cookbook: default.jbs
Time: 19:57:09
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

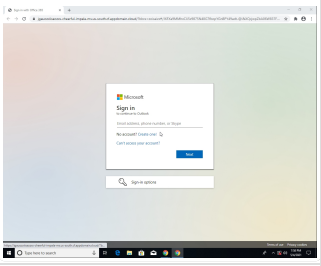
Analysis Report PaymentAdvice - Copy.htm

Overview

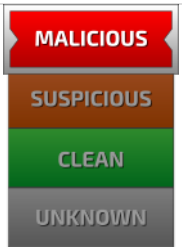
General Information

Sample Name:	PaymentAdvice - Copy.htm
Analysis ID:	404208
MD5:	d4db2888082b56..
SHA1:	617f8f0b10e6ecf…
SHA256:	efa07c2136f6a05..
Infos:	

Most interesting Screenshot:



Detection



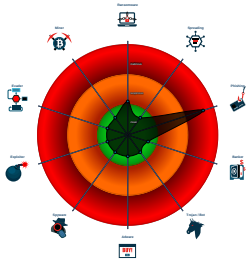
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish29
- Yara detected HtmlPhish44
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 2200 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\PaymentAdvice - Copy.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6196 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,7685515081326957322,2858013151591642698,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1688 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

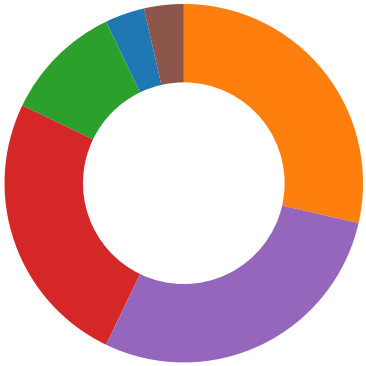
Initial Sample

Source	Rule	Description	Author	Strings
PaymentAdvice - Copy.htm	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Phishing
- Compliance
- Networking
- System Summary
- Persistence and Installation Behavior

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Yara detected HtmlPhish29

Yara detected HtmlPhish44

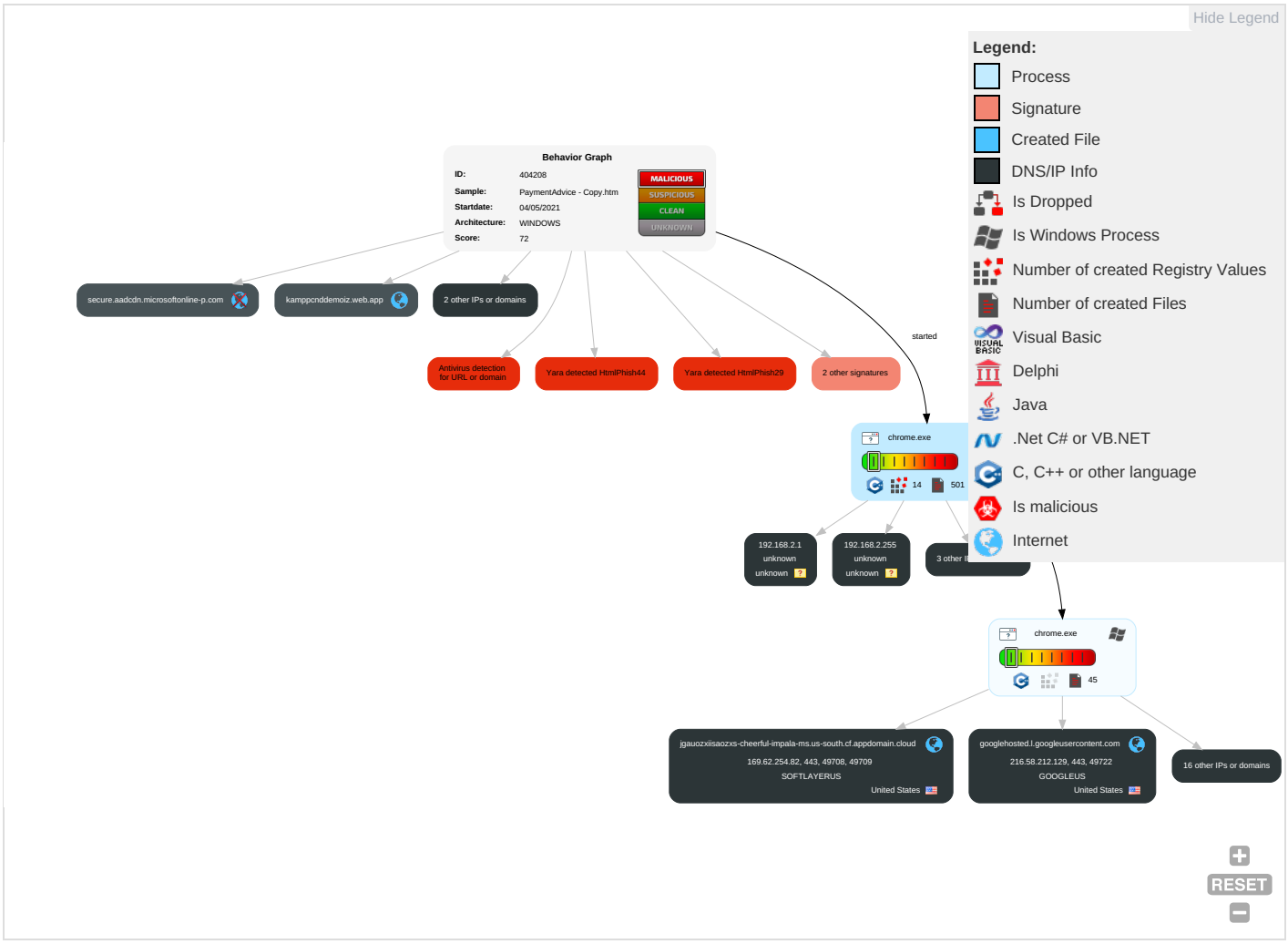
Phishing site detected (based on image similarity)

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

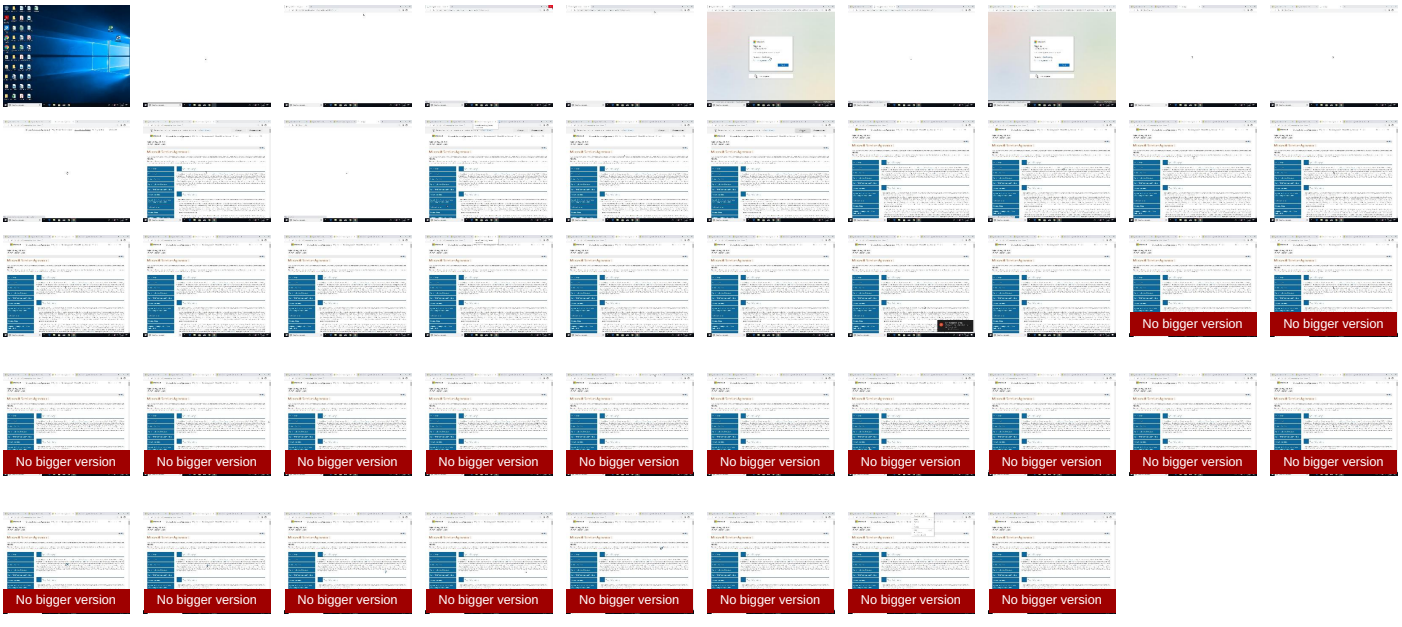
Behavior Graph

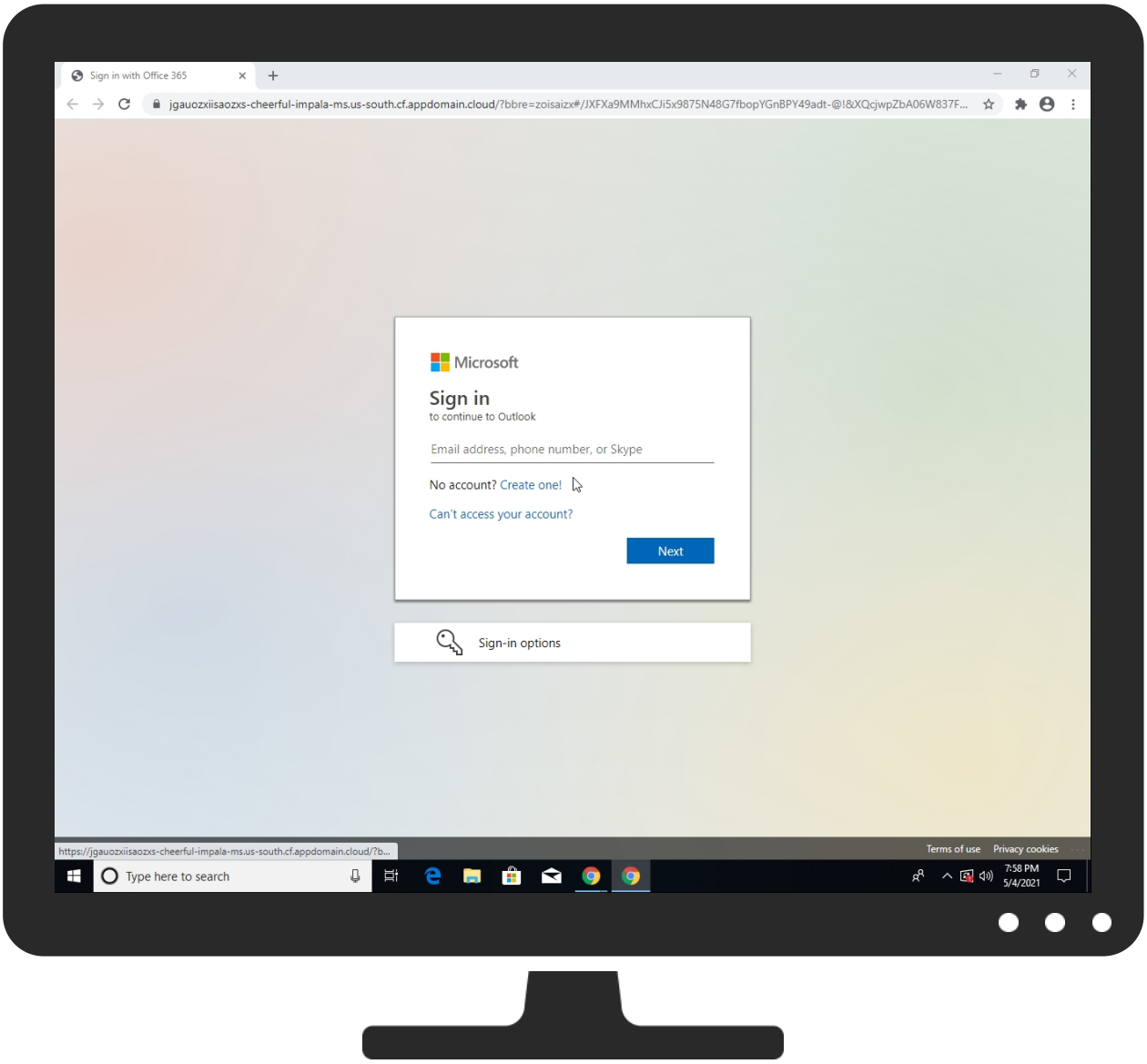


Screenshots

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
PaymentAdvice - Copy.htm	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/gSdqithwZ6JOvrFYf5A-@!&XQcjwpZbA06W837FG25l&@KyH3Uh9gYJOoZlbRWS2&@!-lJd75lpogt7PL6EQxmffD3oavFMeRyM5ygUOBBjQV0oCUpO0aoVVlZn-IrW8TEhMjWY3eA5HrJryGTPy6HVA89YakW/gOqviRSKLPRxSBN2KEsrK6yIql	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Source	Detection	Scanner	Label	Link
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/JXFXa9MMhxCJi5x9875N48G7fbopYGnBPY49adt-@!&XQcjwpZbA06W837FG25l&@KyH3Uh9gYJOoZlbRWS2&@!-pv6ca6NDzH6PLygxPRWghvQISLZCBCgIg7e8Mov8SVRRiq8zsP58oqh0VvrMiSkM1G7rkR7Xzc92BjVaRBWynOYNrb9pNWX-Ja9YA2uKGhAzzzUmac0jz0Qrl2ZgHVqtNmvwuKDha76DDlhqxGeJ4TJxll75nXCKn2YkavHV1e/gyL5GqCR0IqqGH8KpHKzhtEJa10e0JLrjzcj35M2lcLaNZY8ZlIRHCe1d9BWj7bRsf	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://vzas.aioecoin.org	2%	Virustotal		Browse
http://https://vzas.aioecoin.org	0%	Avira URL Cloud	safe	
http://https://kamppcnddemoiz.web.app	0%	Virustotal		Browse
http://https://kamppcnddemoiz.web.app	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/Sign	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/gSdqithwZ6JOv	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.icoD	0%	Avira URL Cloud	safe	
http://https://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301619796417.js	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx2	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	URL Reputation	safe	
http://https://appdomain.cloud/u	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizxA	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/857kExKl1FaBc	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizxSign	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://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloudrhttps://jgauozxiisaozxs-cheer	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/Z	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx2:	0%	Avira URL Cloud	safe	
http://https://vzas.aioecoin.org/608c21cac5bb6a21736d16e5.js	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/JXFXa9MMhxCJi	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth	0%	Avira URL Cloud	safe	
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#857kExKl1FaBcR	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/js/c0f5e0dd4f642062f92481ef2bb4381916197964418.js	0%	Avira URL Cloud	safe	
http://https://appdomain.cloud/M	0%	Avira URL Cloud	safe	
http://https://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/3b1c23908d0aeec856d06e17c3bd1cd1nbr1619796424.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/e430a383a6b882de50a75454faee6e33.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vzas.aioecoin.org	104.21.91.175	true	false		unknown
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
bit.ly	67.199.248.11	true	false		high
jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud	169.62.254.82	true	false		unknown
unpkg.com	104.16.126.175	true	false		high
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
kamppcnddemoiz.web.app	151.101.1.195	true	false		unknown
consentreceiverfd-prod.azurefd.net	unknown	unknown	false		unknown
aadcdn.msftauth.net	unknown	unknown	false		unknown
aadcdn.msauth.net	unknown	unknown	false		unknown
assets.onestore.ms	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/gSdqithwZ6JOvrFYf5A-@!&XQcjwpZbA06W837FG25l&@KyH3Uh9gYJOoZlbRWS2&@!-lJd75lpogt7PL6EQxmffD3oavFMeRyM5ygUOBBjQV0oCUpO0aoVVlZn-IrW8TEhMjWY3eA5HrJryGTPy6HVA89YakW/gOqviRSKLPRxSBN2KEsrK6yIql	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

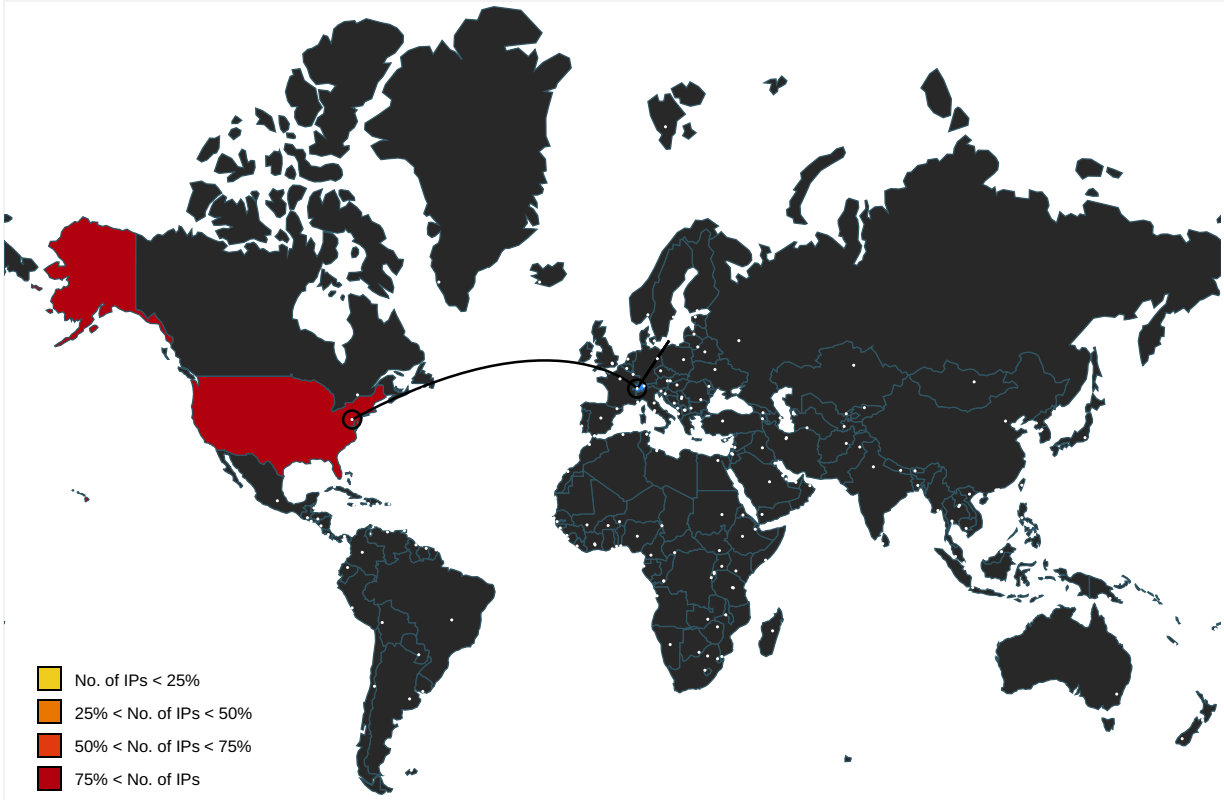
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://assets.onestore.ms/	Network Action Predictor-journal.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://vzas.aioecoin.org	33c8fea9-8146-4945-be17-a63302c1694e.tmp.1.dr	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://kamppcnddemoiz.web.app	33c8fea9-8146-4945-be17-a63302c1694e.tmp.1.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js	48f565ca8f495c25_0.0.dr	false		high
http://https://unpkg.com	33c8fea9-8146-4945-be17-a63302c1694e.tmp.1.dr	false		high
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/Sign	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/gSdqithwZ6JOv	History-journal.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.jsaD	bcba23f2a537c6bf_0.0.dr	false		high
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud	000003.log4.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.icoD	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301619796417.js	4a691c34bd0e3a16_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js	f46ad1d2652b0b43_0.0.dr	false		high
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	Favicons-journal.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://appdomain.cloud/u	bcba23f2a537c6bf_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js	1090860740f0bc96_0.0.dr	false		high
http://https://appdomain.cloud/	f9e631a007138c67_0.0.dr, f428b9f7917ec10e_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://bit.ly/2Jmn3lAMicrosoft	History.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdnjs.cloudflare.com	33c8fea9-8146-4945-be17-a63302c1694e.tmp.1.dr	false		high
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizxA	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://unpkg.com/axios	7df541af6f0604ae_0.0.dr	false		high
http://https://unpkg.com/vue-router	c7ac401a91b7fb3b_0.0.dr	false		high
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/857kExKl1FaBc	History-journal.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizxSign	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	0e7836c0-b7f5-444c-a4ca-4d07e7980df0.tmp.1.dr, ebcf7c00-8d14-46ae-b44b-5b5422f7c826.tmp.1.dr, 8000fba0-cdc2-4f78-842c-2eabd2170155.tmp.1.dr, 33c8fea9-8146-4945-be17-a63302c1694e.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.jsaD	48f565ca8f495c25_0.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js	6ea6b0fd83aa1e1f_0.0.dr	false		high
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloudrhttps://jgauozxiisaozxs-cheer	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://bit.ly/39oebGZ	Current Session.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=s4S%2FS5fK%2F8PK60fJ4xjIDg%2FDITVLtCNzW85FXwZ%2BnHaJN4SWDRAWAi	Reporting and NEL.1.dr	false		high
http://https://bit.ly/2Jmn3lA	Current Session.0.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js	094e2d6bf2abec98_0.0.dr	false		high
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/	000003.log0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://bit.ly/39oebGZMicrosoft	History-journal.0.dr	false		high
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/Z	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx2:	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.jsaD	1090860740f0bc96_0.0.dr	false		high
http://https://vzas.aioecoin.org/608c21cac5bb6a21736d16e5.js	450054d8515cb280_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ajax.aspnetcdn.com/	Network Action Predictor-journal.0.dr	false		high
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/JXFXa9MMhxCJi	History-journal.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#/	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report?s=2%2FBM5I1eGKrl%2FWCniU%2Fv24dXJ3kLXU%2Bvdf89thoCogTqH9uXfqWhuY	Reporting and NEL.1.dr	false		high
http://https://unpkg.com/lodash	da548456e154dd9b_0.0.dr	false		high
http://https://aadcdn.msauth	4a691c34bd0e3a16_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#857kExKl1FaBcR	History-journal.0.dr, Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauth.net	33c8fea9-8146-4945-be17-a63302c1694e.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/js/c0f5e0dd4f642062f92481ef2bb438191619796418.js	39b04e3570748256_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://appdomain.cloud/M	a95cc66a85cc4def_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	8000fba0-cdc2-4f78-842c-2eabd2170155.tmp.1.dr, 33c8fea9-8146-4945-be17-a63302c1694e.tmp.1.dr	false		high
http://https://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/3b1c23908d0aeec856d06e17c3bd1cd1nbr1619796424.js	f9e631a007138c67_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.jsaD	6ea6b0fd83aa1e1f_0.0.dr	false		high
http://https://unpkg.com/vue	f428b9f7917ec10e_0.0.dr	false		high
http://https://aadcdn.msauth.net	33c8fea9-8146-4945-be17-a63302c1694e.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
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	bcba23f2a537c6bf_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/e430a383a6b882de50a75454faee6e33.js	a95cc66a85cc4def_0.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.1.195	kamppcnddemoiz.web.app	United States		54113	FASTLYUS	false
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
67.199.248.11	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
104.21.91.175	vzas.aioecoin.org	United States		13335	CLOUDFLARENETUS	false
169.62.254.82	jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud	United States		36351	SOFTLAYERUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
104.16.126.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.7
192.168.2.6
192.168.2.255
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond

Analysis ID:	404208
Start date:	04.05.2021
Start time:	19:57:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PaymentAdvice - Copy.htm
Cookbook file name:	default.jbs
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:	35
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.winHTM@47/228@16/14
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm • Browse: https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx#857kExKl1FaBcR34sQCWy0UzgGY • Browse: https://bit.ly/39oebGZ • Browse: https://bit.ly/2Jmn3lA • Browse: https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.64.90.137, 131.253.33.200, 13.107.22.200, 93.184.220.29, 20.82.210.154, 92.122.145.220, 216.58.212.142, 216.58.212.173, 142.250.185.206, 95.168.222.146, 95.168.222.141, 142.250.185.99, 142.250.185.138, 142.250.185.202, 142.250.185.234, 142.250.181.234, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 142.250.184.202, 142.250.184.234, 172.217.18.106, 172.217.23.106, 216.58.212.138, 142.250.185.74, 13.107.246.60, 13.107.213.60, 92.123.151.195, 20.190.160.6, 20.190.160.136, 20.190.160.129, 20.190.160.132, 20.190.160.8, 20.190.160.134, 20.190.160.4, 20.190.160.2, 88.221.62.148, 92.122.145.53, 52.147.198.201, 13.107.246.45, 13.107.213.45, 92.122.213.194, 92.122.213.240, 23.57.80.253, 152.199.19.160, 92.122.213.247, 23.57.80.111, 84.53.167.109, 52.255.188.83, 20.82.209.183, 205.185.216.10, 205.185.216.42, 172.217.23.99, 95.168.222.81, 142.250.185.67, 95.168.222.143, 20.54.26.129, 34.104.35.123, 52.155.217.156, 95.168.222.80, 95.168.222.79, 95.168.222.18, 95.168.222.83, 20.73.194.208, 20.49.150.241, 51.11.168.232 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): assets.onestore.ms.edgekey.net, clientservices.googleapis.com, i.s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, r4.sn-n02xgoxufvg3-2gbs.gvt1.com, a1945.g2.akamai.net, settingsfd-prod-weu2-endpoint.trafficmanager.net, clients2.google.com, statics-marketingsites-eus-ms-com.akamaized.net, au-bg-shim.trafficmanager.net, r7---sn-n02xgoxufvg3-2gbz.gvt1.com, www.bing.com, ris-prod.trafficmanager.net, assets.onestore.ms.akadns.net, r6---sn-n02xgoxufvg3-2gbl.gvt1.com, c-s.cms.ms.akadns.net, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, r4.sn-n02xgoxufvg3-2gbl.gvt1.com,

edgedl.me.gvt1.com, c.s-microsoft.com-c.edgekey.net, clients.l.google.com, dual.part-0032.t-0009.t-msedge.net, r2---sn-n02xgoxufvg3-2gbs.gvt1.com, i.s-microsoft.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, part-0017.t-0009.t-msedge.net, go.microsoft.com, e13761.dscg.akamaiedge.net, arc.trafficmanager.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, accounts.google.com, cs22.wpc.v0cdn.net, cds.d2s7q6s2.hwcdn.net, firstparty-azurefd-prod.trafficmanager.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, c.s-microsoft.com, go.microsoft.com.edgekey.net, r8---sn-n02xgoxufvg3-2gbl.gvt1.com, r7---sn-n02xgoxufvg3-2gbs.gvt1.com, e13678.dspb.akamaiedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, wcpstatic.microsoft.com, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, e13678.dscb.akamaiedge.net, e11290.dspg.akamaiedge.net, r8.sn-n02xgoxufvg3-2gbl.gvt1.com, www.microsoft.com-c-3.edgekey.net, ocsp.digicert.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, r5.sn-n02xgoxufvg3-2gbl.gvt1.com, e10583.dspg.akamaiedge.net, fs.microsoft.com, content-autofill.googleapis.com, ajax.googleapis.com, aadcdnoriginwus2.azureedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, aadcdnoriginneu.azureedge.net, part-0032.t-0009.t-msedge.net, www.tm.a.prd.aadg.akadns.net, www.googleapis.com, dual-a-0001.dc-msedge.net, store-images.s-microsoft.com, r2.sn-n02xgoxufvg3-2gbs.gvt1.com, blobcollector.events.data.trafficmanager.net, aadcdnoriginwus2.afd.azureedge.net, privacy.microsoft.com.edgekey.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, mscomajax.vo.msecnd.net, redirector.gvt1.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, r4---sn-n02xgoxufvg3-2gbl.gvt1.com, r6.sn-n02xgoxufvg3-2gbl.gvt1.com, r7.sn-n02xgoxufvg3-2gbz.gvt1.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, aadcdnoriginneu.ec.azureedge.net, r7.sn-n02xgoxufvg3-2gbs.gvt1.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, privacy.microsoft.com, dual.part-0017.t-0009.t-msedge.net, r5---sn-n02xgoxufvg3-2gbl.gvt1.com, e13678.dscg.akamaiedge.net, r4---sn-n02xgoxufvg3-2gbs.gvt1.com, www.microsoft.com

- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:58:17	API Interceptor	2x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
151.101.1.195	triage_dropped_file.exe	Get hash	malicious	Browse	• www.ndsplan.com/qjnt/?r6q=409VEscksmbemh4psNBSYZ81rwPnbusvlC1+acnRVCvPwVqGWkPGglJQMW6w6KHAVJPl&rTFDm=GBOxAlxXYbRxGd
	jH10jDMcBZ.exe	Get hash	malicious	Browse	• www.covidtracksb.com/goei/?hBZpUr88=xBMInsAuN+E1djdll4AZwIkS2iJ2Ju/hNdjKdY9aIZe6wtX7I1CrmxbEw1ye6jglvUKA0g+SVw==&ofuxZl=yVJLPZsh
	46578-TR.exe	Get hash	malicious	Browse	• www.covidtracksb.com/goei/?jBZx=D8b4q&kfOdRJ=xBMInsAuN+E1djdll4AZwIkS2iJ2Ju/hNdjKdY9aIZe6wtX7I1CrmxbEw2e35jcdm3/W
	remittanceslip_pdf.exe	Get hash	malicious	Browse	• www.devfestindia.com/cu6o/?uN6x=W+WuFBrln1qCfAXJ5xKULfOGff8dAb86Jvk64PlTVVMLGqhT4HhQij0c0Z21Ont+U/Id&Vtx0E=FDHHERlxjn8PMDI
	Project.pdf.exe	Get hash	malicious	Browse	• www.towatchapp.com/ocq1/?lhudJ=s9fWYY+GRE/zu2qn9kCI0m/+x20wNzaZElH9PrG8sfLhi2QQuUQu3XvRAAgtMskCm9iv&1bm=3fhdLbnpevPXqD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	quotation.exe	Get hash	malicious	Browse	• www.fsjdc.com/x2ee/?iBZLH8e=/LfDiPUOWZnyidNro0j70T8JUoHePLB2D+vct3YQB9mB3q5S0iE8mJFwRkJZflqbRhoGi7RzLw==&_RA89r=ZL3D3PvXurq
	DOCX RFQ#2.doc	Get hash	malicious	Browse	• dropb-cfeb2.web.app/white.exe
	DOCX RFQ#2.rtf	Get hash	malicious	Browse	• dropb-cfeb2.web.app/white.exe
	12-4.exe	Get hash	malicious	Browse	• www.cvscarepasscard.com/gwg/
	PAYMENT COPY.exe	Get hash	malicious	Browse	• www.firedoom.com/sbmh/?EjRh0d=C5hy1K5oAHBPrT8N397N//2qVHn6YwjigpXcmeWEXRbnBwwwMsoNEjPCOjfDrGfyrTiG&Bn=8pt0_Nex
	PO987556.exe	Get hash	malicious	Browse	• www.firedoom.com/sbmh/?Yn=ybIHmldXUn88Ur&jfIT64=C5hy1K5oAHBPrT8N397N//2qVHn6YwjigpXcmeWEXRbnBwwwMsoNEjPCOg/57X/Kx0DB
	account confirmation!.exe	Get hash	malicious	Browse	• www.firedoom.com/sbmh/?0Tx43p=zbDHwlRpXFN&DV8X=C5hy1K5oAHBPrT8N397N//2qVHn6YwjigpXcmeWEXRbnBwwwMsoNEjPCOjfDrGfyrTiG
	New Additional Agreement.exe	Get hash	malicious	Browse	• www.erraticer.com/bw82/?J2JxbNH=6vRuuEDvqC5+aa5DVmVINCXZAyoyPzPxPo5XFdu9xcvmHzBmwHK9JJE0E4eNhlSLE1w3&BXEpz=Z2Jd8XTPeT
	00d1gI2vB4.exe	Get hash	malicious	Browse	• www.erraticer.com/bw82/?ET8T=6vRuuEDvqC5+aa5DVmVINCXZAyoyPzPxPo5XFdu9xcvmHzBmwHK9JJE0E4eNhlSLE1w3&URiP=qFQxprRp5PPPOfyp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Additional Agreement.exe	Get hash	malicious	Browse	• www.erraticer.com/bw82/?8p=6vRuuEDvqC5+aa5DVmVINCXZAyoyPzPxPo5XFdu9xcvmHzBmwHK9JJE0E7ykiluzNWFh0m7Gjw==&Bh=H0GxrDp
	Additional Agreement KYC.exe	Get hash	malicious	Browse	• www.erraticer.com/bw82/?Ezrtr2qh=6vRuuEDvqC5+aa5DVmVINCXZAyoyPzPxPo5XFdu9xcvmHzBmwHK9JJE0E7ykiluzNWFh0m7Gjw==&QL3=ojqPsv
	http://roundcubemailagentupdate.web.app	Get hash	malicious	Browse	• roundcubemailagentupdate.web.app/
	http://auto78438787328758792947.web.app	Get hash	malicious	Browse	• auto78438787328758792947.web.app/
	http://salary-bonus.web.app	Get hash	malicious	Browse	• salary-bonus.web.app/
	Client Contact REGISTRATION Sheet.xlsx	Get hash	malicious	Browse	• www.letsdindin.com/mnf3/?9rTpeFt0=G6fRyfWpf4em3a5PxYoprh6KPSSsHaeEr4x3W3Pvzp31VBrhmksxwaIlwF2fZ05EyJsOCg==&rj9L_=qpnTHjlx
67.199.248.11	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864888.doc	Get hash	malicious	Browse	• bit.ly/3vdF5wu
	DHL SHIPMENT NOTIFICATION,6207428452.ppt	Get hash	malicious	Browse	• bit.ly/bdjkasbhdjkasbfasb
	Maersk Shipping dispatch bill43252.doc	Get hash	malicious	Browse	• bit.ly/3gEf8lN
	IMG_Order List 5023075401.doc	Get hash	malicious	Browse	• bit.ly/3xn38Le
	Quotations73280126721_Oriental_Fastech_Manufacturing.doc	Get hash	malicious	Browse	• bit.ly/3nlX6WB
	Maersk Shipping dispatch bill43252.doc	Get hash	malicious	Browse	• bit.ly/3neBGKZ
	reawz09cwj_DOC0107210_AGOSTO.doc	Get hash	malicious	Browse	• bit.ly/3sJ2KTQ
	PurchaseOrder78902AprilOrderNewRoundBars.doc	Get hash	malicious	Browse	• bit.ly/2QT0o7t
	Proforma Invoice PIBWH-02314-20-21.doc	Get hash	malicious	Browse	• bit.ly/3n7fDFY
	RFQ No3756368.ppt	Get hash	malicious	Browse	• bit.ly/asdaksdjqwoddaskdajk
	Payment TT-200422.doc	Get hash	malicious	Browse	• bit.ly/3n7fDFY
	Order_List 86267_032621_HeBei_UNION_Import_Export.doc	Get hash	malicious	Browse	• bit.ly/3eBwmxB
	QuotationQO210421A87356_samples_products_sinoma_internationals.doc	Get hash	malicious	Browse	• bit.ly/3sArBJz
	PO944888299393.pps	Get hash	malicious	Browse	• bit.ly/djaksldqowdihjdam
	130578500.doc	Get hash	malicious	Browse	• bit.ly/3grfMD1
	PO_60360570.doc	Get hash	malicious	Browse	• bit.ly/3trc6ES
	qbsubf8fng_AGOSTO_DOC21408001.doc	Get hash	malicious	Browse	• bit.ly/32iTuLf
	TT_2021ME04LO16.doc	Get hash	malicious	Browse	• bit.ly/3gcNxb5
	Tax Documents or Scanned Documents.doc	Get hash	malicious	Browse	• bit.ly/3uJYftE
	2021BR04IS14.doc	Get hash	malicious	Browse	• bit.ly/3ti2cWf

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bit.ly	NEW PO - CE AUSTRALIA PTY LTD.xls	Get hash	malicious	Browse	• 67.199.248.10
	22f76723_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 67.199.248.11

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2e284555_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 67.199.248.11
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 67.199.248.10
	ATT51630.htm	Get hash	malicious	Browse	• 67.199.248.10
	efax637637637.htm	Get hash	malicious	Browse	• 67.199.248.10
	FedExs AWB 775567403803.doc	Get hash	malicious	Browse	• 67.199.248.10
	.htm	Get hash	malicious	Browse	• 67.199.248.11
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	• 67.199.248.10
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864888.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL SHIPMENT NOTIFICATION,6207428452.ppt	Get hash	malicious	Browse	• 67.199.248.11
	Maersk Shipping dispatch bill43252.doc	Get hash	malicious	Browse	• 67.199.248.11
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO737383866366363.pps	Get hash	malicious	Browse	• 67.199.248.10
	FLP_1037850047.doc	Get hash	malicious	Browse	• 67.199.248.10
	Taewoo Hang Co., Ltd..doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_Order List 5023075401.doc	Get hash	malicious	Browse	• 67.199.248.11
	TNT 169716783.doc	Get hash	malicious	Browse	• 67.199.248.10
	Quotations73280126721_Oriental_Fastech_Manufacturing.doc	Get hash	malicious	Browse	• 67.199.248.11
	DFI_0451_587_032.doc	Get hash	malicious	Browse	• 67.199.248.10
cdnjs.cloudflare.com	DGNTL04052021.2-8864.html	Get hash	malicious	Browse	• 104.16.19.94
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	• 104.16.18.94
	BCJOphish040520219700.html	Get hash	malicious	Browse	• 104.16.18.94
	ATT51630.htm	Get hash	malicious	Browse	• 104.16.18.94
	ATT50279.html	Get hash	malicious	Browse	• 104.16.19.94
	efax637637637.htm	Get hash	malicious	Browse	• 104.16.19.94
	Minebest686.html	Get hash	malicious	Browse	• 104.16.19.94
	afafd.htm	Get hash	malicious	Browse	• 104.16.18.94
	agnesng@hanglung.comOnedrive.html	Get hash	malicious	Browse	• 104.16.18.94
	FAXNIV0MSWBUP.htm	Get hash	malicious	Browse	• 104.16.18.94
	Telex_Copy.html	Get hash	malicious	Browse	• 104.16.18.94
	.htm	Get hash	malicious	Browse	• 104.16.19.94
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	• 104.16.19.94
	FAXQKJEZPA42S.htm	Get hash	malicious	Browse	• 104.16.18.94
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	• 104.16.18.94
	ATT50064.html	Get hash	malicious	Browse	• 104.16.18.94
	Remittance_Advice_-7889x_pdf.HTml	Get hash	malicious	Browse	• 104.16.19.94
	Hanglung872.html	Get hash	malicious	Browse	• 104.16.18.94
	Final_report_202110.htm	Get hash	malicious	Browse	• 104.16.19.94
	775.htm	Get hash	malicious	Browse	• 104.16.18.94
cs1100.wpc.omegacdn.net	DGNTL04052021.2-8864.html	Get hash	malicious	Browse	• 152.199.23.37
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	• 152.199.23.37
	BCJOphish040520219700.html	Get hash	malicious	Browse	• 152.199.23.37
	Master Fund Distributions.pdf.html	Get hash	malicious	Browse	• 152.199.23.37
	efax637637637.htm	Get hash	malicious	Browse	• 152.199.23.37
	Minebest686.html	Get hash	malicious	Browse	• 152.199.23.37
	afafd.htm	Get hash	malicious	Browse	• 152.199.23.37
	efax663663663.htm	Get hash	malicious	Browse	• 152.199.23.37
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	• 152.199.23.37
	New%20order%20contract.html	Get hash	malicious	Browse	• 152.199.23.37
	Hanglung872.html	Get hash	malicious	Browse	• 152.199.23.37
	775.htm	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0129) for nerlyn.cama ibo .html	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0151) for norgaardr sacda .html	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0151) for norgaardr sacda .html	Get hash	malicious	Browse	• 152.199.23.37
	E3761 80251728_03312021.html	Get hash	malicious	Browse	• 152.199.23.37
	AttachementHtm.html	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0155) for umclune myumanitoba .html	Get hash	malicious	Browse	• 152.199.23.37
	1-page-fax-from-+33822822.htm	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0195) for turnerrd pellamw .html	Get hash	malicious	Browse	• 152.199.23.37

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLE-PRIVATE-CLOUDUS	NEW PO - CE AUSTRALIA PTY LTD.xls	Get hash	malicious	Browse	• 67.199.248.10
	22f76723_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 67.199.248.11
	2e284555_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 67.199.248.11
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 67.199.248.11
	ATT51630.htm	Get hash	malicious	Browse	• 67.199.248.10
	efax637637637.htm	Get hash	malicious	Browse	• 67.199.248.10
	FedExs AWB 775567403803.doc	Get hash	malicious	Browse	• 67.199.248.10
	.htm	Get hash	malicious	Browse	• 67.199.248.11
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	• 67.199.248.10
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864888.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL SHIPMENT NOTIFICATION,6207428452.ppt	Get hash	malicious	Browse	• 67.199.248.11
	Maersk Shipping dispatch bill43252.doc	Get hash	malicious	Browse	• 67.199.248.11
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO737383866366363.pps	Get hash	malicious	Browse	• 67.199.248.10
	FLP_1037850047.doc	Get hash	malicious	Browse	• 67.199.248.10
	Taewoo Hang Co., Ltd..doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_Order List 5023075401.doc	Get hash	malicious	Browse	• 67.199.248.11
	TNT 169716783.doc	Get hash	malicious	Browse	• 67.199.248.10
	Quotations73280126721_Oriental_Fastech_Manufacturing.doc	Get hash	malicious	Browse	• 67.199.248.11
	DFI_0451_587_032.doc	Get hash	malicious	Browse	• 67.199.248.10
FASTLYUS	iuCN1LJ980.dll	Get hash	malicious	Browse	• 151.101.1.44
	iwEcXUAues.dll	Get hash	malicious	Browse	• 151.101.1.44
	i6ALtgS6nV.dll	Get hash	malicious	Browse	• 151.101.1.44
	DHL Notification.jar	Get hash	malicious	Browse	• 185.199.111.154
	XmLE5f5wBX.dll	Get hash	malicious	Browse	• 151.101.1.44
	Indeed_Update_File.html	Get hash	malicious	Browse	• 151.101.2.217
	d.exe	Get hash	malicious	Browse	• 151.101.0.249
	d.exe	Get hash	malicious	Browse	• 151.101.0.249
	d.exe	Get hash	malicious	Browse	• 151.101.0.249
	d.exe	Get hash	malicious	Browse	• 151.101.0.249
	6ccd0000.bilper.dll	Get hash	malicious	Browse	• 151.101.1.44
	6bae0000.bilper.dll	Get hash	malicious	Browse	• 151.101.1.44
	6c130000.da.dll	Get hash	malicious	Browse	• 151.101.1.44
	Payment Advice-BCS_ECS9522020909153934_3159_952.jar	Get hash	malicious	Browse	• 185.199.108.154
	valuePasteList.dll	Get hash	malicious	Browse	• 151.101.1.44
	Payment Advice-BCS_ECS9522020909153934_3159_952.jar	Get hash	malicious	Browse	• 185.199.108.154
	MyUY1HeWNL.exe	Get hash	malicious	Browse	• 151.101.0.64
	6a9b0000.da.dll	Get hash	malicious	Browse	• 151.101.1.44
	6ba90000.da.dll	Get hash	malicious	Browse	• 151.101.1.44
	s.dll	Get hash	malicious	Browse	• 151.101.1.44

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	DGNTL04052021.2-8864.html	Get hash	malicious	Browse	• 169.62.254.82
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	• 169.62.254.82
	Tree Top.html	Get hash	malicious	Browse	• 169.62.254.82
	efax637637637.htm	Get hash	malicious	Browse	• 169.62.254.82
	afafd.htm	Get hash	malicious	Browse	• 169.62.254.82
	FedEx Shipment Address Update Form2021.html	Get hash	malicious	Browse	• 169.62.254.82
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	• 169.62.254.82
	FAXQKJEZPA42S.htm	Get hash	malicious	Browse	• 169.62.254.82
	Monday, April 19th, 2021, 20210419034211.37352E088CBDC09B@classactsautobody.com.htm	Get hash	malicious	Browse	• 169.62.254.82
	042021.htm	Get hash	malicious	Browse	• 169.62.254.82
	Maersk_BL Draft_copy_Shipping_documents.html	Get hash	malicious	Browse	• 169.62.254.82
	042021.htm	Get hash	malicious	Browse	• 169.62.254.82
	042021.htm	Get hash	malicious	Browse	• 169.62.254.82
	AttachementHtm.html	Get hash	malicious	Browse	• 169.62.254.82
	1-page-fax-from-+33822822.htm	Get hash	malicious	Browse	• 169.62.254.82

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#U266b VM-Tunes-Playback.html	Get hash	malicious	Browse	• 169.62.254.82
	VoicePlayback (0195) for turnerrd pellamw .html	Get hash	malicious	Browse	• 169.62.254.82
	Monday, April 19th, 2021, 20210419111136.68B7C9F20 FAF4F3F@classactsautobody.com.htm	Get hash	malicious	Browse	• 169.62.254.82
	P A Y M E N T (1).html	Get hash	malicious	Browse	• 169.62.254.82
	Dobra-Dossin.html	Get hash	malicious	Browse	• 169.62.254.82
37f463bf4616ecd445d4a1937da06e19	DGNTL04052021.2-8864.html	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	Proforma adjunta N#U00ba 42037,pdf.exe	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	7D1E.exe	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	5.exe	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	ordine n#U00b0 276.exe	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	statistic-2067311372.xlsm	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	f97e137e_by_Libranalysis.exe	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	e1df57de_by_Libranalysis.xls	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	MV RED SEA.docx	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	MyUY1HeWNL.exe	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	IMG-WA7905432.exe	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages _2202-434.htm	Get hash	malicious	Browse	• 151.101.1.195 • 152.199.23.37

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

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5887976EDAA817EEF5159B09F6FCD000_35673150FB44DAA99337A19E2291E035	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.1425222529285115
Encrypted:	false
SSDEEP:	12:JKtfA5BWm+fgZlPgNOqASxJ2WKhS5cM4pGSGh0W6I6:JiAS/bMdOQ54ptGba
MD5:	E08CA994231ED96D7C7F912D320DE315
SHA1:	FFF01ABA6AAEE0F8FEB3A85B0E7F3683B0397072
SHA-256:	C4C006A37A0B75641FC4760EF6400698D567554F18BAB21FA5BEDE5C0D1A7A8F
SHA-512:	F07CC1FD95973CE63B3C5C673A1B0BB04D50465195C2F538904D82DC623987A5D1ECCA90A0EB670D7FB59782D8778D8BFDAB856E1BEE220F748DEAC58D64E3D0
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....=.P.....J`.e.!.....20210503211301Z0s0q0I0...+.....I.....v....@-h;qj....=.P.....J`.e.!.....s.Co.sz.\M..o....20210503205701Z....20210510201201Z0...*.H.....f...w.1.JEn...LY}E....m(w$.]...f...G...I.....ph.. ..2....\Y..3.F..Uk{z.R.H.x5*h..6.....A..zH.....4.....Ur...&kc.*5-.....(.w..fV.....k.'j.t.G..*.K...v..R.\c..%.I.{.<...[..7.. .a..0.;..E.7j.....B..q>.z_Q.1D..d.\Q....6....#{._3.3....J..H...}.a...]

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.220826706178252
Encrypted:	false
SSDEEP:	12:JY0+5FZJ9swttTgPb+KGAt8ck2oxLUyXWvsbIabz7F:JY0+3ZswTTgPCKGAtbSYEPF
MD5:	BF2AA7A3165EBF872C4B3E795FC58724
SHA1:	135160CD833D697D3C23AD6C30B1D0ECF96423BC
SHA-256:	14CACAD358EF67E1340B1197A3CDDE6A5AF87308FCB010B9656A3DF70B672147
SHA-512:	CDF1004C027AF633D0D16AAE80331C3EC62039EAA83C7E5A808B3B4A2EAF8E4D9268F6DD6016292F2A00600396AAE18EF97083553E8076CEB0AB45D193878E3
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....>.i...G..&....cd+...20210503215359Z0s0q0I0...+.....(..A..B..G@B.X....>.i...G..&....cd+....y.D.... .a_.k.....20210503215359Z....20210510215359Z0...*.H.....$.k...k3...m.U.J..Z..ph2....Z..O..6.O.m.{<T...../]..9h....C...D.w.1Y..n.u..A.#.#...Dvv.....,....j.bLf.tDq..-0.V&....l...M.2[q...h8.l..fbD...N.AN..V"V.{0i.I.....4....Z..D.3.%..=k..b....'..d...7.[K-.....#R.K...Fqc...0...WO"y....2Y....{>b....Y}JA

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5887976EDAA817EEF5159B09F6FCD000_35673150FB44DAA99337A19E2291E035	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.842879097252956
Encrypted:	false
SSDEEP:	12:SkYnNmxMiv8sFq3lCvM710Bf2QEk0mxMiv8sFq3lCvM710Bf2QF:SkYnNmxxvm4vw1Alk0mxxvm4vw1A5
MD5:	A685011717A47BDA9B7100A9FAB9ECF0
SHA1:	F23A22C1476300BEE7F107F3FC6221F7071BACED
SHA-256:	F3E71FF6B042898FD0FF1F74DEB95232C4E7F9EAD97C79EC271278AA51738C22
SHA-512:	B4C628D63A2BD9A9498B15DB64CE51D64FD616EDE19C32BB386CF3B2AF80BD2EF9F26F163CB81C7F8670FAB01E809E650B6F95BC526F0CC11BA7178A5B0699F4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5887976EDAA817EEF5159B09F6FCD000_35673150FB44DAA99337A19E2291E035	
Preview:	p..... .....h..ZA..(..... .....:a@.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.R.J.9.L.2.K.G.L.9.2.B.p.j.F.3.k.A.t.a.D.t.x.a.u.T.m.h.g.Q.U.P.d.N.Q.p.d.a.g.r.e.7.z.S.m.A.K.Z.d.M.h.1.P.j.4.1.g.8.C.E.A.q.N.7.H.P.i.Q.2.%.2.F.4.c.3.r.d.X.E.3.u.H.G.8.%.3.D...".6.0.9.0.6.7.5.d.-.1.d.7."...p..... .....h..ZA..(.....L..^@...>...E.....>...E.. .....:a@.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.R.J.9.L.2.K.G.L.9.2.B.p.j.F.3.k.A.t.a.D.t.x.a.u.T.m.h.g.Q.U.P.d.N.Q.p.d.a.g.r.e.7.z.S.m.A.K.Z.d.M.h.1.P.j.4.1.g.8.C.E.A.q.N.7.H.P.i.Q.2.%.2.F.4.c.3.r.d.X.E.3.u.H.G.8.%.3.D...".6.0.9.0.6.7.5.d.-.1.d.7."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.8631302854365797
Encrypted:	false
SSDEEP:	12:y59DmxMiv8sF1JbqDkwJr0yr+Wl39DmxMiv8sF1JbqDkwJr0yr5:y5FmxxvnFqYwJeWl3FmxxvnFqYwJZ
MD5:	014F0C13CE358233B70425EC559B5D9A
SHA1:	4546BA460FEE09A2818C4D807FB9F4FA1732D075
SHA-256:	F8EE451C72F571E81EBB7617DD33ED47F272F9B718A0855B08E015DAD25F8E5C
SHA-512:	8DDE963183B6034D9342F30ECB91A371781935901281E534F5CD5999F0CB0EF87B168A16695996D0FBF099FEC5301751C12DF0E1DC48B7ED2C9254A6D9D0F09D
Malicious:	false
Reputation:	low
Preview:	p..... .....&..ZA..(..... .....{@.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.x.5.q.U.S.w.j.B.G.V.I.J.J.h.X.%.2.B.J.r.H.Y.M.%.3.D...".6.0.9.0.9.2.e.f.-.1.d.7."...p..... .....&..ZA..(.....O.f@....3..E.....3..E.. .....{@.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.x.5.q.U.S.w.j.B.G.V.I.J.J.h.X.%.2.B.J.r.H.Y.M.%.3.D...".6.0.9.0.9.2.e.f.-.1.d.7."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\034f91bc-a27a-4424-b1ed-0ff5b405e2fb.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):	363813
Entropy (8bit):	6.029632639217598
Encrypted:	false
SSDEEP:	6144:rI2AQ63ApYXpcoManB218Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHmh:MFe8tBXxzurRDn9nfNxF4ijZVtilBd
MD5:	EBDC9E522BB3EFD29D775A9B942158F7
SHA1:	C44374DC55EDA90759D682AF4797B6FD93F5380C
SHA-256:	57F7C05D2628423938CA85D3A60C0C8C914D39789D57FE4AE253266EDB6D68A4
SHA-512:	B5A76D2F51362DEF93D7AE2097779F242CFAB061D6FC081DCF6702AC245F4E3CEF5986D21458305CDE40440B204ECFABB68DF8F000C4A0CF78F2E1A369B4E45E
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":1.620183484177309e+12,"network":1.620151086e+12,"ticks":110148471.0,"uncertainty":4529418.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13

C:\Users\user\AppData\Local\Google\Chrome\User Data\0d72bd6e-f22a-40b6-a462-20887e4c2634.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):	363456
Entropy (8bit):	6.029066313258485
Encrypted:	false
SSDEEP:	6144:cI2AQ63ApYXpcoManB218Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHmh:7Fe8tBXxzurRDn9nfNxF4ijZVtilBd
MD5:	0D5E33C545D7B23478491EA3B0D7F20E
SHA1:	512A1F5600A56D7759EC49328B0958AD2E37C3C1
SHA-256:	365612D7CE580F90C7F2477AF05EB53CB4BF22427D47DB74CD1A4A49A52A0BCF
SHA-512:	B6FD8F1E8456AEDD30BB1821F139006903F20803CF8D45BAB6F51DA423EE8431E8525C514E1D46F493C74DE4EE72A9D996E709BB9391D6CF7F0D82BBFFD6984
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\0d72bd6e-f22a-40b6-a462-20887e4c2634.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620183484177309e+12,"network":1.620151086e+12,"ticks":110148471.0,"uncertainty":4529418.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13

C:\Users\user\AppData\Local\Google\Chrome\User Data\2f655259-717e-45ba-a564-1e986be4bc9b.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):	363717
Entropy (8bit):	6.029465859527414
Encrypted:	false
SSDEEP:	6144:OI2AQ63ApYXpcoManB218Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHmh:VFe8tBXxzurRDn9nfNxF4ijZVtilBd
MD5:	B027628904212535723 32C5ECCBD588C
SHA1:	4304CA1779C1726FA79BD0F3D68E1472DAB756D1
SHA-256:	AB5EF95811269D7938A93F190EFF58C3AF20A4E1084F44F5147AB2DEBD681D36
SHA-512:	A750DD423138F2D99D3C43F40DBA9B6113D5DD19CBFE00FB247E627D75AF56EC50D84121BCEBDD4568744CB1D3A749FD8804886F5BFCA944CC44F068E33C2E DB
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":1.620183484177309e+12,"network":1.620151086e+12,"ticks":110148471.0,"uncertainty":4529418.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13

C:\Users\user\AppData\Local\Google\Chrome\User Data\521059f1-6b6d-4878-a7d2-701806611ec8.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):	359276
Entropy (8bit):	6.015407096699374
Encrypted:	false
SSDEEP:	6144:kI2AQ63ApYXpcoManB218Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHmh:zFe8tBXxzurRDn9nfNxF4ijZVtilBd
MD5:	9869CD3C2E6F9D6A9674D71A4013F4D8
SHA1:	CE15595925A97214AF61A9E4E36507DA23C3A34C
SHA-256:	AF673C90349107D52917F52F11F4F3DCD374679A71E60BDAE50B20CC2AE3E5B0
SHA-512:	0BAF1F475E5325E3D31CAD1E242C56AC400CD258BA4624DC7DFC35598323AB0174660A94DABD02B2C5572CD35BDC8D13F6AC481BAA507FD5725758C2C9A71 D
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":1.620183484177309e+12,"network":1.620151086e+12,"ticks":110148471.0,"uncertainty":4529418.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13264657080908

C:\Users\user\AppData\Local\Google\Chrome\User Data\59778174-316a-4e8a-a05e-8242931403d8.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):	363132
Entropy (8bit):	6.028478413084817
Encrypted:	false
SSDEEP:	6144:0I2AQ63ApYXpcoManB218Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHmh:DFe8tBXxzurRDn9nfNxF4ijZVtilBd
MD5:	8B439A87A00DE2F6EFFDC978B6B89C3E
SHA1:	07B60F161EE42899CCA0BDDD9473A735FB07AB6D
SHA-256:	F8CC701E4C0A589B25EB78F859C2940A191818F5910C694485659562B145F840
SHA-512:	DBD271FCF7C2DDB2C4E29DE5DF71BE0FBBB6170BB0F8A88EDB1F5E1558124C1A470FEBB7BD76B393516EC1A5373943173B3799030055106150AB8569EC1101D 5
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\59778174-316a-4e8a-a05e-8242931403d8.tmp	
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":1.620183484177309e+12,"network":1.620151086e+12,"ticks":110148471.0,"uncertainty":4529418.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075007846"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\59ce7138-89f7-40ad-8324-84f957292cb6.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):	359277
Entropy (8bit):	6.0154070741254175
Encrypted:	false
SSDEEP:	6144:sI2AQ63ApYXpcoManB218Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHmh:LFe8tBXxzurRDn9nfNxF4ijZVtilBd
MD5:	C7628D7B03E9F01ECD7365E32A6FCD77
SHA1:	F897749C93873A52665930824072C7AEFDE9FB44
SHA-256:	8C21C4D12DBB30A40790FACE7422DEA487876675F8526AC9B2F560C5260AC391
SHA-512:	BFC650859747D628EE443BB112D88FB49241E99C7F889A0F40023A691C4B60C34B370885F432052FB28A0FE740D2ABCE62215058FF1CC5ABD83FCEAB6117FC15
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":1.620183484177309e+12,"network":1.620151086e+12,"ticks":110148471.0,"uncertainty":4529418.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13264657080908

C:\Users\user\AppData\Local\Google\Chrome\User Data\63d0b5cb-9fba-4a94-8e70-e43b592746ca.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):	359277
Entropy (8bit):	6.015406662685857
Encrypted:	false
SSDEEP:	6144:eI2AQ63ApYXpcoManB218Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHmh:lFe8tBXxzurRDn9nfNxF4ijZVtilBd
MD5:	44D37D567E84FBBE19CCAE49BD345E8D
SHA1:	B605AB477378BFAD43119759ACA3621571530580
SHA-256:	445C59996F252604FF96DFD21AB4B8FDDB379FE7CA48F34CE58EF3B62182D9F4
SHA-512:	7ECB74BDA851219226122EABDDC9AE5683F5E2C85585767365F61CCDC710972B8B07AB6962A477951CB8B0FBF89A5EE95025B0F8907C3BF47F51E83BE0F9743
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":1.620183484177309e+12,"network":1.620151086e+12,"ticks":110148471.0,"uncertainty":4529418.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13264657080908

C:\Users\user\AppData\Local\Google\Chrome\User Data\87472e30-cdbb-4ee3-8895-1b42d3009255.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):	363289
Entropy (8bit):	6.028834035834344
Encrypted:	false
SSDEEP:	6144:lI2AQ63ApYXpcoManB218Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHmh:mFe8tBXxzurRDn9nfNxF4ijZVtilBd
MD5:	A6600D9BB596C00980204AAE3CFF8D03
SHA1:	BEE4EE6A8CB74A3CB9057BD1E6AB93F1904A060E
SHA-256:	7CBEB19F5C7F359993060FC705565223D7736159E61B54A2FBE0255C9B966D0B
SHA-512:	EAC990AAE9DD1AF85284505CC25A302D405370462CE9F738BF6197F10977C807C8EC6C1F03DB471B2322179A1323545426A86F62CC3D1BCCB49B85F76DE123A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\87472e30-cdbb-4ee3-8895-1b42d3009255.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620183484177309e+12,"network":1.620151086e+12,"ticks":110148471.0,"uncertainty":4529418.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13

C:\Users\user\AppData\Local\Google\Chrome\User Data\8b0d970c-83eb-4965-a458-78d7848eeb63.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):	362848
Entropy (8bit):	6.027979733845686
Encrypted:	false
SSDEEP:	6144:4I2AQ63ApYXpcoManB218Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHmh:HFe8tBXxzurRDn9nfNxF4ijZVtilBd
MD5:	12D63BC2BE26E6B25300A4191B7171F5
SHA1:	89B3F58560360A7D95610E62055A7E97C8F4C215
SHA-256:	B503E48C556FF092B3835198EEB3EA12B74E226208572D4C6C47419CF419E005
SHA-512:	99488C277FD5CFD20F7AD4CAFF174FA52011EAE5493387C9CFFDE82334315C267B61188D6F48DCE1A0021ED142E0D09769FFCC94ADC336C648207ACFAF70DB4
Malicious:	false
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":1.620183484177309e+12,"network":1.620151086e+12,"ticks":110148471.0,"uncertainty":4529418.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075007846"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\93b6f00e-ff7c-4752-b861-d42cca4b7e0c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7491800969622524
Encrypted:	false
SSDEEP:	384:h7/8MeR7KluIVJ7Y7NkrVvAs3v8K7HGbGburpucOx/i6yNrJ0m9xT9e84A7OeCYy:NeKVpKSg/0e/aQKUH/eoKuQIBY
MD5:	904DA576518D007414230A5CBFDFC131
SHA1:	42E06F94F584E202922D0D572642DAB3D28B1E6C
SHA-256:	AEB722C67EB736DCC8EE2C766A95AD3F18C3F0E5940E9B560D3AEADF3CBCBDF2
SHA-512:	287128E118BAB1E25F49D88121DD05EB0F524C67E514D1652CB5A3C24ACD34CAF10794FEFCC4E7F12BD639F65AB9A6909F6AC0B82190F169C857721C9DC6C3
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.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\9efd37f2-bb50-488c-9b04-d0941e3155be.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):	363028
Entropy (8bit):	6.028281623331314
Encrypted:	false
SSDEEP:	6144:fI2AQ63ApYXpcoManB218Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHmh:QFe8tBXxzurRDn9nfNxF4ijZVtilBd
MD5:	E8315F901A6A6F41CA5E3B3A0B2722DE
SHA1:	8EEF6EF6B035F364DAB4C682103E5304E2A5E458
SHA-256:	FC38E7F4270AFF9792C236A563A8BE6A04D1BD3B5C373C431B93493735128DC7
SHA-512:	0E53D8D58A416CD610636CF8F31D7726145C8C88FE1E1E6D70BA758731740B4BABBB40668220C7CE13E5796D8762FCB4B56BB6FE27CCEFBE77DF1802FC32C27
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\9efd37f2-bb50-488c-9b04-d0941e3155be.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620183484177309e+12,"network":1.620151086e+12,"ticks":110148471.0,"uncertainty":4529418.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075007846"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0ca6e21e-d10b-486d-a82f-ca10b887beee.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):	22594
Entropy (8bit):	5.5358106703809815
Encrypted:	false
SSDEEP:	384:RbWtBLlxNXo1kXqKf/pUZNCgVLH2HfDsrUxHGmnTA7b1T4d:yLlfo1kXqKf/pUZNCgVLH2HfgrUlGmn5
MD5:	B835EEDBF8AA9BD1A86F21EB81DD9351
SHA1:	718CB454D1B3C8AB90603667A6336270B1D4CA52
SHA-256:	1913FC42382F5E8B7AC850541B0B35616DEC490C668D8D9C9544AB904C17AD9A
SHA-512:	5D360EDB414FA29E83D32B9B5D83535926E5C89A61BCC98A775D83A3E49D86715A64275454102CE8E215879D4B4C12A1E96CD5EE8744E5DC6283268B145C633
Malicious:	false
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":"13264657081014765","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ba1e188-223e-4127-b1ad-915009d14cad.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
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ff886a2-55ee-49df-9cb5-06159ba5ea82.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):	5362

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ff886a2-55ee-49df-9cb5-06159ba5ea82.tmp	
Entropy (8bit):	5.16467614392561
Encrypted:	false
SSDEEP:	48:YcmkPklq/UcuqAlQq3o3rNeper4lYclQuoTw0/i1bPc8C1Nfct/9BhUJo3KhmeSN:nDFF/Kf3o3oSV8Ik0JCKL8xpbOTQVuwn
MD5:	9536B571FA1AEFF1AD0FD3BF33F8F0DD
SHA1:	917F0EB72CF0A3160D7B45849B63422BDFDFAE3F
SHA-256:	506257AB864CA19905B6B887CD9F5CAE58786B8A95E73A59D2CE85075F1B11BB
SHA-512:	EC8F78F98561A6536C27DBDC21D698C5A7AE0F5EB443442D47BAE3F09F44EF90717F481B7E5B3299B8DA4B193FD5284E6BB8CE9D32B0F29C22D0641B0D7E5B 1
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264657081325013","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcom e_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":1 0,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0"," 0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\25e72e49-a213-4855-ad2f-bdb2987f07b3.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):	5362
Entropy (8bit):	5.164754941155503
Encrypted:	false
SSDEEP:	48:YcmkPklq/rcuqAlQq3o3rNeper4lYclQuoTw0/i1QPc8C1Nfct/9BhUJo3KhmeSN:nDFI/Kf3o3oSVXIk0JCKL8xpbOTQVuwn
MD5:	0A24F7EDF784D4314A583148D75ED18D
SHA1:	48EB4097C6EFBC95D5F61F14D7953B4F38B96788
SHA-256:	29C05F4527D7160DB9ED0E85DE39646A81AF894FE66D66AD59E2464E5E0F0F8F
SHA-512:	90FE99FD8AA7B143813E1A60DB09337408A4227C228BFF2DECDC3BB321FC314A3C3D75882A01177411166D26612CBBD9FF2B051DC82097729361F7A430045921
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264657081325013","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcom e_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":1 0,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0"," 0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\33c8fea9-8146-4945-be17-a63302c1694e.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):	3658
Entropy (8bit):	4.867415730896794
Encrypted:	false
SSDEEP:	96:JnxOTCXDHzqdBTG9TOamrO6NOdo+jFV0Fi+UVmLmVezG7ZuhVD:JnxOTCXDHzqdBTGFOamrO6N+o+j30FTT
MD5:	0117D3D6607FB1E3DA41CD5E7422BD74
SHA1:	4C39968D2F09EFEC74B7D0D82BE75121CDD682D2
SHA-256:	6EB972A1ADF5F3B533A9EC3B565ECBD7D3248EEFBE63E388CBE6B3E203636E62
SHA-512:	8ECA8C9424C54EB43337337AA5D2CF35DF1CBF82D546D899E6C84C3598F2F06CB4B4743BAD88D76B8E2B883AA90E3DA76E6B1BD18FFA2873CFF99EE1185596 C6
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.co m","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolati on":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.goo gle.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267 249084525947","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions": [50],"expiration":"13267249084539196","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\33f51601-5c5b-4bad-be9b-c0eac976cd52.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):	2211
Entropy (8bit):	5.596850738129476
Encrypted:	false
SSDEEP:	48:YIIUiNVwUVTUE6UUhLdUZzeUDUlUiDKUeAUeCAW6wUpwUOUeh:8UiwUBU9UUddUZzeUDUlUiDKUlUHAQUg
MD5:	45012EE03EE55BFFBF575CDC953020BE
SHA1:	1F7FAE0968EE2BA0C8202169D4FE1BD911945B86

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\33f51601-5c5b-4bad-be9b-c0eac976cd52.tmp	
SHA-256:	9F32E38A6736521A510E8AF901F6ACC6D8EE2F9AA71B8E6CDB658052110A829C
SHA-512:	D97D659D5EEFA13C8B78D5C8631AAEA95242B08A326AD3E4D61C769FB6176F5CAAE6E21B996DBD1BC905A76CA7A86FFE8B5C32C849C29E8E64380F461036A7 4C
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1651719501.969066,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620183501.96907},{"expiry":1635963487.632122,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620183487.632126},{"expiry":1651719492.795095,"host":"OOMzAQj4V8d5WazCO66tlzHVLB2WZR4bM8LYzrRexiY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620183492.7951},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1651719504.658352,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620183504.658356},{"expiry":1651719504.710714,"host":"a1ZTYlNSUSrj8xKbRz2eU2pqvpuOBdbHFtk7jbKGSQI=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5986b936-b450-4cdf-9fa5-a8554fbb9b65.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1541
Entropy (8bit):	5.587484357609103
Encrypted:	false
SSDEEP:	48:YYVwUVTUE6UUhtUiDKUeAUeCAW6wUpwUOUeh:eUBU9UUDUiDKUlUHAQUqUOUc
MD5:	18FBF52D96FEF10F32E7800857759647
SHA1:	AA256E3112800A38F54D4F69960E4B0635606224
SHA-256:	7BF80C3A059F0D51103DB09D96E4CD88A2FE19C25182C2917621E299D71F1668
SHA-512:	6CF93966006336BF466F052527631AC3C9CF0592B74DF20DE4445774A92B0225668BCE138BE662B4F690B1FA148D1D90DB9AC4D50971350201FA9686E49AF310
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1635963487.632122,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620183487.632126},{"expiry":1651719492.795095,"host":"OOMzAQj4V8d5WazCO66tlzHVLB2WZR4bM8LYzrRexiY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620183492.7951},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1651719487.478264,"host":"e3SziuwfuO2UvuBno+qkR1ObHAzZmSUoJhrc7dbP1Uo=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620183487.47827},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\72e119b2-5b19-4629-a9ca-e87ec4f28398.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):	5745
Entropy (8bit):	5.181111186209297
Encrypted:	false
SSDEEP:	96:nDFFsKf3o3oSV8Ik0JCKL8EtYkFd/RbOTQVuwn:nDHf3o3oSuC4KLYkFH
MD5:	6299DFB7129C4CE8546902601A2F5944
SHA1:	1D4B613CE958D7B44FC3680A3FC8EFEC8B1B325D
SHA-256:	29F975DF413CB7AAC316F59C21C6E73460EB0059E8546F30B16E332E53864ADD
SHA-512:	715635A4722F80D0C2DE7851C8D878AF5DCA553660879B7F5A1E01A8427A2DF54A44EDD5904E92EC360B6EFC6F82E66575E43EF3ED2465D1C8567E495D60937
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264657081325013","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8000fba0-cdc2-4f78-842c-2eabd2170155.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DB CAA
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8000fba0-cdc2-4f78-842c-2eabd2170155.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.219309524093295
Encrypted:	false
SSDEEP:	6:msV1GFlWM+q2P923iKKdK9RXXTZIFUtpdVmoz1ZmwPdVnGjWMVkwO923iKKdK9Rn:tV4L+v45Kk7XT2FUtpdVdZ/PdVGjLV5D
MD5:	09D4DD8E32FB214518FF552602FBA837
SHA1:	B010B52850239FD1952167542EE362C334132F8E
SHA-256:	29472428AE35C21B94950BE62A761552827D3B52CF3C275CBF027BEBD17AAFFC
SHA-512:	B8C5B804670234A119B80C6240ECE9DBF246316773B58C600646FB810D161EFF968EA981E22C1C7F06A2D22C232F7A3D0E04FE555932788E3BEC02AF5C7A6F47
Malicious:	false
Preview:	2021/05/04-19:58:06.602 1bac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/04-19:58:06.607 1bac Recovering log #3.2021/05/04-19:58:06.608 1bac Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.223702673487059
Encrypted:	false
SSDEEP:	6:msVwmlWM+q2P923iKKdKyDZIFUtpdVxId1ZmwPdVib+WMVkwO923iKKdKyJLJ:tVNL+v45Kk02FUtpdVxIv/PdVib+LV5C
MD5:	12D2B50CDA09F5427D8C8E16DD1D129B
SHA1:	F264E112AAF7919C237D2D77B8DC8F53C648C371
SHA-256:	C67DC66BA712740BDFEA3FD2E8A563F3261A84881B98751AD848505989C41581
SHA-512:	880745804E151782604D70D4C1FCA03B01A30F45B37E9B5173082B3169A117BBB1688A6D8258C21027DED2A675C448E548141FF4D86C2D17C899F2BFA616C856
Malicious:	false
Preview:	2021/05/04-19:58:06.582 1bac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/04-19:58:06.583 1bac Recovering log #3.2021/05/04-19:58:06.584 1bac Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\094e2d6bf2abec98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.55289225609899
Encrypted:	false
SSDEEP:	3:m+lP9Ola8RzYJb9yKlf8QPKxWStHWFvDFYtRP9FelHCDll/xl58tyGdDm/r5tllX:m3VYyK08fNH1Dv1htvyL6/vbK6t
MD5:	D4596E3CD220A9BE4844EA1BD6DC413E
SHA1:	3A59363C0C0CB6E7044917DA5A6FC066795F8248
SHA-256:	E2BFC7A5D4B36252B0C2B0A37A535515EEF5D0CE33D9F7FF60A8AED2918E8F46
SHA-512:	C8B5106CDE73E5655F5D2E14ECE2879D23683F8B8E683E8A04C1BB8525FEA0707933292FB91CE9BC161029A50A2D838DA3E462566B8C4A713F01EF8B9CB6A77
Malicious:	false
Preview:	0\r..m.....W....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js .https://microsoft.com/*)." /.....=.z-.7.K]..~..=..9.....8...A..Eo.....~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1090860740f0bc96_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14147
Entropy (8bit):	5.707600088900297
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1090860740f0bc96_0	
SSDEEP:	192:v0B8oGXY+0fFPAKTYK0GcVVK9GE1iMCZjdGS0IY7QJx+M3Y5:MuHb/GeI8MqBPY7QJBY5
MD5:	8BFF03E72F4631E5FDFA64C001590C60
SHA1:	F43F085BEB8639E623E30A3F5A16EF9C68C93781
SHA-256:	8DC8E4A0F01CC5F4546D329033178B9692CFC4071AA4CBA83A9359A84A71CCFF
SHA-512:	14B7454DF47BDE36BC00F3F1DB21D9C47EC84F0BF9019560FC0F10F0EF801CAEECB4D68EDE34594B10F94757E688785C73E08439DBCF854FB685E9281AAB72C 4
Malicious:	false
Preview:	0\r..m.....c.....n....._keyhttps://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js .https://appdomain.cloud/..." /.....gZHD'.J.....\D*.T.K...B..vp....A..Eo.... .....A..Eo.....'..7....O.....5..d.....(S.<..`4.....L`.....(S.l.`.....L`.....Q.@..M....exports...Q.@Vm$.....module....Q.@Z.."....define.... QbJ}.....amd...Q.@.l.....VueI18n...K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.].....\..&.-...%....(Rc.....l`....Da.....e.....`...p...@.....@.-....TP.A. ....E...https://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js...a.....D`....D`(...D`.....`....&...&....&.(S.m..`.....9.L`.....i.Rc.....P.....QbR}.....t.....Qbb.{..... e.....Qb~Y.]....r.....Qb.../....n.....S...Qb...r....o.....M...QbN.....s.....Qb".....l.....Qb.....c.....R....QbNdn.....f.....Qb...p....h.....Qb..J.....p.....Qb.~.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\15bbcddad0bfbf89_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.893734518098278
Encrypted:	false
SSDEEP:	6:m8+VYSHT8NWQA8SSV316K/G1BC338m4tShZK6tzQVhcNHUdNcjScuwYeG1BC338m:K7z8NWQ93V5Gm338kTlmcN0dNcjScuwx
MD5:	9BDF5AFCE415D0813B5D415A0700BCEA
SHA1:	B3869436FA86765B25C5348377007B419CE0914A
SHA-256:	7B5B1D9B4895B21B672E6F2379E17E3ECD92C6EEE3427D22CACFCB72F071DD36
SHA-512:	07916121948E5CC29CD3BA82BCDDF8D9174DC9B093AE4958F7C48AA119C275403C0FCC21D2A24AE53B99A6A5A539502E0ADC8092E3E7123CC6F8BB59E01741 D
Malicious:	false
Preview:	0\r..m.....^...%26C...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js .https://appdomain.cloud/..." /.....!RV...u.^~;.....sc..:5.c..A..Eo..... .....A..Eo....." /..x..79D04D418A368369ED017912E9D7954CD87C091605DD9C1ADD8ED9FC6F773516...!RV...u.^~;.....sc..:5.c..A..Eo.....c.LL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\328b75cf02d95d5e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.677067177496192
Encrypted:	false
SSDEEP:	6:mcYiRDHwA7eIAX3TH5R2DkT2tqowDgjn5/m4lK6t:XDHXeB3L5gDpTwCmZ
MD5:	2BB95AC732DAB5F102DCDE26C4357F78
SHA1:	69D0FC2B0CA0046A16BDA32D2CB4F03B667981AD
SHA-256:	BFD9788D82335556EFFCB79BEA33A1CB81678520D36F38B412487EB9C895BD39
SHA-512:	FF135393EA3BDB82DC29EDF1740B7B66D1CB7C0E1FAD33A84CB980FABE6DBE837681D29A6F66CB79F1D272FA1C77DB8DCCFAA33C0C1B83133666DAACCA3D 3BCA
Malicious:	false
Preview:	0\r..m.....x...?....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=8c84dc53-9dee-f42a-46b1-5a93c0e43d70 .https://microsoft.com/.l." /.....U..0.. ...\.oQ.8gD.r*{.....A..Eo.....M.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\39b04e3570748256_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	262
Entropy (8bit):	5.697121740910171
Encrypted:	false
SSDEEP:	6:mGuYy74JPCN1FlnD+79XxWbKgJ0pSq1k1YQan9I5ajnK6t:xg4BSF1D+79MWIqDH
MD5:	4C2EBF6B37E4566A4AC089E1CC0056B3
SHA1:	CDFC61E09F3DCAE3C4C9C6ED6F4078E7CABE7DF9
SHA-256:	7DFEB781E28B535E860CFBBDE44DFBA8B8AF567420EE94CE65CB36825A85BD25
SHA-512:	03ACE788C8F2EB28073EBDC847DA0B87FC74212CF23AFB4035258169F786C90420E563F533095E498F11F40918EB143E18A77E1C90D7379E87FDACBCB961590F
Malicious:	false
Preview:	0\r..m.....c~....._keyhttps://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/js/c0f5e0dd4f642062f92481ef2bb438191619796418.js .https://appdomain.cloud/.Y.." /.....Y ..dp..t..g.Eo...l...&.....A..Eo.....u.J.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\450054d8515cb280_0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\450054d8515cb280_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.638782472438937
Encrypted:	false
SSDEEP:	6:mssYJ5T3xQRIXSSv6iltXFLIPJxiYbK6tWssYJ5T3xQRIXSVP9llXFLIPJxi8K6t:BDjS+iyNtVLIP/RLDjS+inlbLIP/X
MD5:	A50A9C28BABEB358CA7BB919E3FEC27F
SHA1:	870A028C7C5EF03C6E95B78CC278E0F79C0BA16F
SHA-256:	ADAE3788C0960D0894839FFEAA16FC2A265E4F49793C842A360BADE7C8B80CCC
SHA-512:	CA9D39BE70B1B4B548A61E4768067A26F630BAF3D8F72BD91ECF7558BC1F66C528227F993A9F24DB28E7735E265E28C6FD5FDE78F6AC4838FFBAB70F3BD55F54
Malicious:	false
Preview:	0\r..m.....S...fy....._keyhttps://vzas.aioecoin.org/608c21cac5bb6a21736d16e5.js .https://appdomain.cloud/.." /.....F.....a... Q..8.p...,.Y?.i..t2...A..Eo.....#9.....A..Eo.....0\r..m.....S...fy....._keyhttps://vzas.aioecoin.org/608c21cac5bb6a21736d16e5.js .https://appdomain.cloud/.{.." /.....a... Q..8.p...,.Y?.i..t2...A..Eo.....".....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\48f565ca8f495c25_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	37160
Entropy (8bit):	5.81020410932405
Encrypted:	false
SSDEEP:	384:3ICthGCb9x1/revxfwb2ADJg/6I2NTKQRZUn+18in0vi8UUwGjlqMJYlroYtcAcM:3PhGm1/revde2n/QtKQ7Jycd20+Y3J
MD5:	58BF5BF2C5C56E1A8BC02241E59CE0E3
SHA1:	180AAA5A01FB48ED2E30C48BA84CD8B05C64851C
SHA-256:	DF5E7DCA49B4CD3A9D8B90DBDA6D5CB455EA338FF6D06050E80CAE0097D35267
SHA-512:	86288822724137335 62C6DED3A74D71EA1E0D1B0532545E48FC4612CB5F049E4CA941BE111E95BAE2F9ADEC3F094E2076E6D80EDB3474CDAD72A658BA74A764F
Malicious:	false
Preview:	0\r..m.....p....W.f...._keyhttps://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js .https://appdomain.cloud/.]..." /.....w.....`.....u...T,..p...S._U2.au.7....A..Eo.....(T.....A..Eo.....'.....O....h...F.(.....(S.<..`4.....L`.....(S.l.`.....L`.....Q.@..M....exports...Q.@Vm$.....module....Q.@Z.."....define....QbJ}.....amd...Q.Pz<.J....VeeValidate...K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.].....\..&.-...%....(Rc.....I`....Da....2.....e.....`...p...@.....@.-....`P.q.....R...https://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js..a.....D`....D`&...D`.....)....`....&...&....&.(S.....`p#.....L`B.....Rc.....`.....S...Qb.../....n.....Qb~Y.]....r.....QbN.....s.....QbRHsT....d.....Qb..J.....p.....O.....Qb..<.....x.....QbB.`.....w.....Qb....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a691c34bd0e3a16_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	50328
Entropy (8bit):	6.496804761561896
Encrypted:	false
SSDEEP:	1536:U69UeU0r0/GfyT7U+pyWNxj2BcM+1KY6K+0:U66eUU0/G7+8W2W70Y6b0
MD5:	9FEBAEB373536712F721546A26319DEA
SHA1:	ACFFEC8049763F4A2F12D12CDDD5A8D2A6FDEFA0
SHA-256:	B10318B9361098420B15DC6E826D58ED0D602B3EDD27F49092EC0F27042C9F39
SHA-512:	D7317ACC4D7CCF35E837D33E957DE50466BBCA938B1E0B025343DB3AC65F19D2C67EDEF4BE23657EAAFAB8A070A190DAC433A6FD0DB971DEE33310E0B9CACF59
Malicious:	false
Preview:	0\r..m....._keyhttps://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301619796417.js .https://appdomain.cloud/..." /.....i.....E..."U.L`D(..O!..(ah.....C.w.+.A..Eo.....&.W.....A..Eo.....'.]z....O.....)=.....(...X).....T.....(S...Y)..`hR.....L`.....(L`.....Qc. .}...._0x2360...QcJ.X....._0x213f...Qd."....._0x588238.....Qd&;....._0x4b5539....(S.....Ia.9...;....Qd.....animatePip..E.@.-....pP.....d...https://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/js/a3107e4d4ae0ea783cd1177c52f1e6301619796417.jsa.....D`....D`2...D`.....`N...&...&.(S.@.`6.....L`.....0Rc.....Qb.....f...`$...l`....Da.h..Vi...(S.P.`X.....L`.....Qb...7....push..Qc.....shift.....K`....Dn .....%.M.&..$..&.(...&...&.(...&.X...&.Y.....'.....,Rc.....I`....Da.i..Ji.....)....c.....`."d.....K`....Dj.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a7b0a16eebe4c59_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19454
Entropy (8bit):	6.011085894730163
Encrypted:	false
SSDEEP:	384:exGlAxqkpF6H1cwJvB1eFS5GWdRID8qKvaf:rlsQK1W/GKs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a7b0a16eebe4c59_0	
MD5:	FCFF24DAB8D7384AD5E8F3E05B122803
SHA1:	E83578F1E307FFB3B78924A9CCF1DA83D7ACC6E2
SHA-256:	111024E8D60214480400296624786FBA6EC63872C8281EBD10F010CDEFB25F5B
SHA-512:	13037BF10EB732056833FB56398ABA219E341E865A4FE5102AB38D55FF48892722A7EE17D0A9CC712EC68537165CD548AB8E451F71C07EF25F9F654BC68DE777
Malicious:	false
Preview:	0\r..m.....z.a...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/b7-0ad59f/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1 .https://microsoft.com/.`|." /.....M.....o..r&.@..I.....a._.?f..~...A..Eo.....-^.....A..Eo.....'.z....O.....H..6..2.....4.....(S.0..`.....L`.....(S....`.....L`.....LRc".....Qd2.....requirejs.....Qc2.....require...Q.@.....define....Q.P.Ul....__ext ends...d.....l`....Da..... ...(S...`.....L`>.....Rcf.....*.....Qb.....n.....Qb..L....r.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6ea6b0fd83aa1e1f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8643
Entropy (8bit):	5.625515052620326
Encrypted:	false
SSDEEP:	192:pHFNuc0QHFhO9fCglS+htW6JOs2MLgtIOjsuV5Z0Uov4HJnj:pnlFlhO9aitHnLlKLTov4Htj
MD5:	2F58ABEF4BC8A8AF245346A4677B3932
SHA1:	7655F0177CCD481F91B5DEFB2CC1662D2B1B7315
SHA-256:	D4C6A97960F3F1413C67D07687EE299C91E8DEE6D21AF10350396A35CFF88A48
SHA-512:	4619E3A759ED42153C60496146A093F7D709817A087B0D9E852AF49367013858309B36A53E5327C14DB5C3CC25BBA6BF622A378564454FA9189DB49FDB1FAC37
Malicious:	false
Preview:	0\r..m.....[.....5d...._keyhttps://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js .https://appdomain.cloud/...." /.....8Sw2G/.?.,6.a4t....l..}.lU...A..Eo.....l.....A..Eo.....'..)....O....@ ...o.....L.....(S.<..`4.....L`.....(S.l.`.....L`.....Q.@..M....exports...Q.@Vm$.....module....Q.@Z.."....define....QbJ}....amd...Qb.Tv ....Vuex..K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.]....\..&.-...%....(Rc.....l`....Da.....e.....`...p...@.....@.-....LP.!.....=...https://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js...a.....D`....D`"...D`.....`....&...&....&.(S.%..`.....L`.....Rcp.....0.....QbR}.....t....Qbb.{.....e.....Qb.../....n.....Qb...r....o.....Qb~Y.]....r.....S...QbN.....s.....M...R....Qb.....c.....QbNdn.....f.....Qb".....l.....Qb..J....p.....Qb...p....h.....QbRHsT....d.....Qb.~.....m.....Qb..q...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\781980b07f1bb38f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.670926491500853
Encrypted:	false
SSDEEP:	6:mql9YiRDHwA7qYsDpNdNFvNgDszFppR0QK4bFbK6t:RTDHXqn/xNgDsppIQHz
MD5:	19C5D653D08619A0B4CB924034B31F2A
SHA1:	4991A971D10840B59B79D20C76A3767A4CBD355B
SHA-256:	96263A3A9ADA71161CE081EDC3BB675F5016F0EB7AC2518EC5ECC3716F51A76C
SHA-512:	3812C76CEBEDF9B6D6DFCB5D8C4BADA03E9FDA83ABF66BD33BF1BEBF7DAABF1CDA6AF688F08670E111558482500564DBD9D2CAD26B5E80FE21832FFBBFA62A41
Malicious:	false
Preview:	0\r..m.....x...0.v...._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4 .https://microsoft.com/...." /.....5...a.....S...s5.O..8O....F$.|3F.A..Eo.....#hG.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7df541af6f0604ae_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	31166
Entropy (8bit):	5.606981074794055
Encrypted:	false
SSDEEP:	768:b2cgiBdZEZ7SsOZUOLQ6zZqfquseHQ5GtzkZ:ycgkOhrDOLQ8WGboc
MD5:	95560847BCAEB0E1C7A5E81840A45316
SHA1:	3E8A524A76269F092C69D9159E1C7F4190F6D1E4
SHA-256:	D3D74C95AB2DC2909102EC8D871CA3D067790192F0E82E696DBDC872E3B9AA7B
SHA-512:	95C64B2531D67F902D5214F822F22340BC03CAC713B28DCD8E12916D40B3EDF15B1AFA0583E3722316D644385C080FB9819FF8D25C10B94944DD1E5DB5274A2(
Malicious:	false
Preview:	0\r..m.....N...^....._keyhttps://unpkg.com/axios@0.16.1/dist/axios.min.js .https://appdomain.cloud/...." /.....|.....t.c.i.<.1....N...V....)...S..?.A..Eo.....{}.....A..Eo.....'.....O....(x..h4.....(S.<..`4.....L`.....(S...`.....L`.....Q.@..M....exports...Q.@Vm$.....module....Q.@Z.."....define....QbJ}....amd...Q.@.....axios.....K`....D}.....s.....s.....&.\..&.-...%..H...s.....&.(.....&.\|.&.^....&...s.....&.\..&.-...%...\..&.-...%.....(Rc.....l`....Dat..... ..f.....`...p...0.....@.-....<P.....0...https://unpkg.com/axios@0.16.1/dist/axios.min.jsa.....D`....D`....D`.....`....&...&....&.(S....`.....L`>....(S.`.`x.... L`.....@Rc.....QbR}.....t.....Qbb.{.....e.....Qb~Y.]....r...b$.....l`....Da.....(S...`.....L`.....!..$..a.....a.....Qb.....id..C..Qc>.....loaded..H..a+..Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3c2e2c260a7099_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.360465715640021
Encrypted:	false
SSDEEP:	3:m+lSd7ta8RzY/VW4McTtRAJOlGQHLRSVNRFYtRCxlKNlHCWkcWUBl0iPy2wd1Um9:mXYI4McTDsJegDCxzWkc1TrlEQmK6t
MD5:	60399675390B4BA8A401C80FE7189697
SHA1:	AF0DBEFBC009C90EC3AE87B1C76C4E74D100F52F
SHA-256:	CCB70B83D5372B342D688D3CD3396F1A57FE4594C9802C1368B8B184D1F16709
SHA-512:	0A268615A86F5261DBD54A8B34CBD48067153FEE2F50DD7AC357F59D722A78548202B1F7F55AA0FD4924BC7CDB17C897070F31B3F7C897C26427A5DFE5E7007
Malicious:	false
Preview:	0\r..m.....V...|.L\...._keyhttps://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js .https://microsoft.com/..}." /.....J.....<.S....l....*.W.U\..E?`..r.A..Eo.....-.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a95cc66a85cc4def_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	498
Entropy (8bit):	5.649344564707727
Encrypted:	false
SSDEEP:	12:JN4BSFvEW2D+ILlwhp6vN4BSFvEW2D+IiUBhpTG:OSFcW2DHLmwMSFcW2DHietG
MD5:	DD3F0632A3C24B653699E0B375B5AC94
SHA1:	94EBB5D1515B68237B93C82A95986C11B24B4D76
SHA-256:	200847DC8163D77BE083196E155884FA3844B62B419C7579980FC7DE63C9C2B2
SHA-512:	483DD029BF6E519DDA1BAC36FB1C0276F2DBA02E3AD1D2F073AEBD5A233D0FBE0981A816273D335D60C97BD221411D802949B47490383EBAB1DDFE855639B78
Malicious:	false
Preview:	0\r..m.....u...M....._keyhttps://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/e430a383a6b882de50a75454faee6e33.js .https://appdomain.cloud/M.." /.....J.. .vn..8.x...o.J.wkOl.j1.D.....A..Eo.....J.....A..Eo.....0\r..m.....u...M....._keyhttps://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/e430a383a6b882de50a75454faee6e33.js .https://appdomain.cloud/...." /.....J...vn..8.x...o.J.wkOl.j1.D.....A..Eo.....SJ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bcba23f2a537c6bf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42901
Entropy (8bit):	6.212491590782263
Encrypted:	false
SSDEEP:	768:6snIDTbn6rO0UVJU9U4xW1B/aLWePr722JCz2xSJnDbtT6zLS4LX3JS2dJ4fpIE6:3sTbn6rO0UVy9UQYJaLWePr722JC5JnK
MD5:	F116864E03E801D941EC77B194A6342A
SHA1:	7D376FFB23BEF52F9F9C1610E0EB3060DE25D719
SHA-256:	D9BBD71CAF81616C97B77B0AC1139E18BF8989BE0AA4193B41ADF1986660AEE2
SHA-512:	6B754BC3EA52B9DDEB3973D1377CDFEB871373EE147B909D09C626748EC8AE6B774A8F84BB6633962C7EC9EF3CFC7A3A5632A799EF7B24440F2EF665CC8214E
Malicious:	false
Preview:	0\r..m.....m....9....._keyhttps://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.js .https://appdomain.cloud/u.." /.....z1f...F....dj...r.XL.T.;s.`t..A..Eo.....y.....A..Eo.....'.A.....O.....@.....p.....0.....(S.<..`2.....L`.....(S.8.`*.....L`.....0Rc.....O.`....I`....Da....f$...(S....`.....M.L`.....dRc.....M...Qb.....c.....QbRHsT....d.....Qbb.{.....e.....QbNdn.....f.....Qb...p....h...f.....I`....Da....b$.....(S.....Ia.....a..@.-....\P.a.....O...https://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.js.a.....D`....D`,...D`.....`J...&...&....&..Q.&..1.&.(S...Ia....c.....d.....@.....&.(S.|..`.....L`.....Qb.o."....call.....S...K`....Dy`.....%..Tw.....&.....E.....7&.&...&.(...&.Z.....!...&.%.*..&...&.%.e....&.0...%..&..E.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c7ac401a91b7fb3b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19447
Entropy (8bit):	5.692610358086308
Encrypted:	false
SSDEEP:	384:+NW732A2yBDc0lYfczXU2Gc/EIEjbaAuN4VNjUko5w/V99:+N8DFc9YfczwIabaGz9
MD5:	A7AE321BEFC98DF71AB6B04AF33600F0
SHA1:	4818280D0276668B78260C2E90C7D7D436612D02
SHA-256:	BC693671C71CA172A6EE4C55276DAA08C9E053C1F742B5B0B8BC4480B78910FA
SHA-512:	86EF756CC4982C01D85867C83544A8AC897D441FD08FEFCB8896863ED173018D33D381C0F498359ABFA699E01B2BEE3E33F03CB5DB89B1D683ACB97E06F0671

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c7ac401a91b7fb3b_0	
Malicious:	false
Preview:	0\r..m.....W....*^...._keyhttps://unpkg.com/vue-router@2.7.0/dist/vue-router.min.js .https://appdomain.cloud/.(.." /.....E....6..$P.\|....c9.Nx....@...%.e.A..Eo.....A..Eo.....'.Z\....O....hJ...zE.....(S.<..`4.....L`.....(S.l.`.....L`.....Q.@..M....exports...Q.@Vm$.....module....Q.@Z.."....definе....QbJ}.....amd...Q.P..DW....VueRouter.....K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.]....\..&.-...%....(Rc.....l`....Da.....e.....`...p...@.....@.-....HP.....9...https://unpkg.com/vue-router@2.7.0/dist/vue-router.min.js...a.....D`....D` ...D`.....a....`....&...&....&.(S....`<.....L`x.....Q.Rc.....QbR}.....t.....Qbb.{.....e.....Qb~Y.]....r.....Qb.../....n.....Qb...r....o.....S....M...R....Qb.....c.....QbN.....s.....Qb..J.....p.....QbNdn.....f.....Qb...p....h.....Qb"....l.....QbRHsT....d.....Qbv..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d6607ac3a7d89a68_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96664
Entropy (8bit):	5.81894351656283
Encrypted:	false
SSDEEP:	1536:bvYWCOeMOEylKRrCjgTXGyoGB8dWufFoihbUS9C3cCy:bQWCqryHsTXGyidrFZASI3c
MD5:	036EB2B28791777D9638BE1B95628B08
SHA1:	2527BE89A0DC0611AA1A8DBAB3B24FBED49E2717
SHA-256:	6E793583CCB536070122742D2817985E9ABF2452FC779BC6EFA4C3931B020D80
SHA-512:	463E43571721EDD89085D33D94236A12F4EEB4B537DC7A9BAC88F1A56122563D5F3DD1BA5C4E0604D05C6515B90CA8062142E29308B5C45EC99D433970AB715
Malicious:	false
Preview:	0\r..m.....@....=i3....79D04D418A368369ED017912E9D7954CD87C091605DD9C1ADD8ED9FC6F773516.....'..R....O!...@x....%.....X...."....(.....l.....(S.H..`L.....L`....(S.p.`.....L`.....0Rc.....O.`....I`....Da....j.....Q.@Vm$.....module....Q.@..M....exports..Qcz..R....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa..../...I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.jsa.....D`....D`$...D`.....M....`....&...&..!.&....&.(S...."..`.E.....L`.....Rc`.....(.....M...QbRHsT....d.....Qbb.{.....e.....QbNdn.....f.....Qb...p....h.....S...Qb.....j.....Qb.O.W....k.....Qb".....l.....Qb.~.....m.....Qb.../....n.....Qb...r....o.....Qb..J.....p.....Qb~Y.]....r.....QbN.....s.....QbR}.....t.....R....Qb..q....v.....QbB.`.....w.....Qbv...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\da548456e154dd9b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	87720
Entropy (8bit):	5.640517867299548
Encrypted:	false
SSDEEP:	1536:xwEno6NEqn2RJd7FmQ81lHP85HrwNXF9E6cDV+pyRP5KTNqdf3zUu:xPFJAn7FLrwN1TcDxRP5R3r
MD5:	248C05DCA6D074DDD8AC675FB49DC02C
SHA1:	59429130B9F6F6DEFE94195863B1F64F8CD2EBDF
SHA-256:	15DDDF82E082F69562E514272B5DCDF3D16D94E2A8B38C7B4716B1196A55C769
SHA-512:	FEF44221ACF23C4CB6470BB5019B304F172F1CA1DCD8E20F34561498CB5A557BF6C325DA141850D7BEE3298F8A8B8D59BCF18E066074890842A3D813256BCA8
Malicious:	false
Preview:	0\r..m.....@.....Q....89E85C213FA34F6F3618C902D2E2217F488B6CD383565BA55BE5436EC7A64AF8.....'.D.....O....`U.."....5.....(S.<..`2.....L`.....(S....`.....Y.L`(....a.Rc.....Qb.../....n.....QbR}.....t.....Qb~Y.]....r.....Qbb.{.....e.....R.....S...Qb...r....o....QbNdn.....f.....Qb.....c.....M...Qb".....l.....QbN.....s.....Qb...p....h.....Qb..J.....p.....Qb.g0....._.....Qb..q....v.....QbRHsT....d.....Qbv.....y.....O...Qb..<.....x.....Qb.....j..Qb.~.....m.....Qb.....A.....Qb.O.W....k.....Qb.....E.....Qb.....O.....Qb.....S.....Qb"i.....I.....QbB.w.....R.....Qb.W%\....z.....Qb.o&.....W.....Qb.b.....B.....Qb.&v.....L.....Qb.EOS....U.....Qb..W6....C.....Qb...|....D.....Qb.....M.....Qbn.....T.....Qb.....F.....Qb.K.U....N.....Qb.`.....P.....Qb.....Z.....Qb2.\.....q.....Qb..1.....V.....Qb..z....K.....QbN

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f07074a526b61413_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	339
Entropy (8bit):	5.844874513819796
Encrypted:	false
SSDEEP:	6:m+lVY0OCZI5B5LZzySpzf7M5zOj6P4AnK6tSDEWzJgEYxwzOj6P4/:3VnI5BLpyKjopOEWNowKjH
MD5:	80D1D02CD793870B6DA23049DF1B235F
SHA1:	F611C3DCDE39B2E2143694258AA3361F237624C6
SHA-256:	CEBEF9487C75121DBC8F9F8EDB2FF26FC1839845B10511B9AA5B06010D310B0D
SHA-512:	751B282C1B05DC5A0C24E1F5085363CF8DFCBE9EF56E63765026F7197B72DB7FCC758A43EFAA74CA2F3F7570E425DE7946141787887C40A4CAA159364D41B7C
Malicious:	false
Preview:	0\r..m.....K...z.{....._keyhttps://unpkg.com/lodash@4.17.4/lodash.min.js .https://appdomain.cloud/.4." /.....:.....d.....=b3.....L.OB&z..LR|Bt...A..Eo.....h.:.....A..Eo.....4." /..V..89E85C213FA34F6F3618C902D2E2217F488B6CD383565BA55BE5436EC7A64AF8d.....=b3.....L.OB&z..LR|Bt...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f428b9f7917ec10e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f428b9f7917ec10e_0	
Size (bytes):	63106
Entropy (8bit):	5.844770705317598
Encrypted:	false
SSDEEP:	768:VX+q5G40I3GfHLGs+Jjj1YeC+CI2MBiNGhs5rj9ic2kggYlOM8qi:Fv5pPUH7+JK2NaGkH9isggYhji
MD5:	4D3117A190D4B9819461E9E0CD3DC461
SHA1:	01D38CD903D54BE070D02C13E0C4A5AD40ED5612
SHA-256:	B48BA954969795D5C4AD6BEBA230FD2DADA320A0D7602E26FA9639A7E7330A88
SHA-512:	64B4B88989F66E28B8C4E2520052B41363891CC48EC98CE5B5CF53DEDD15C59AD492CEE6E493612999446F5931663F4DDFC632A893A5E94FB7A862949A92494A
Malicious:	false
Preview:	0\r..m.....J.....8...._keyhttps://unpkg.com/vue@2.6.11/dist/vue.min.js .https://appdomain.cloud/[p..'' /.....''.....=...7N....|.....%.[.A.o..`XOOX.A..Eo.....A..Eo..... .....'..m....O.....`.2.....!..|.....(S.<..`4....L`.....(S.x.`..... L`.....Q.@..M....exports...Q.@Vm$.....module.... Q.@Z..''....define....QbJ}.....amd...Qb.....self..Qb..V.....Vue...K`....Dx.....s.....s.....&.\..&.-...%..3...s.....&.(.....&.]....%.....&.\..&.-...%.....(Rc.....I`....Da..... .....e.....`...p...@... ..@.-....8P.....,...https://unpkg.com/vue@2.6.11/dist/vue.min.jsa.....D`....D`....D`.....`....&...&....&.(S....!.`.C.....}.L`:.....i.Rc0.....Qbb.{.. ...e.....QbR}.....t.....Qb.../....n.....Qb~Y.]....r.....S...Qb...r....o.....M...QbN.....s.....Qb.....c.....R....Qb''.....l....QbNdn.....f.....Qb..J.....p.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f46ad1d2652b0b43_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.543407563659742
Encrypted:	false
SSDEEP:	3:m+lSxla8RzYJb9yKIf8QPKxQBHWFvDFYtRDnHglHCF/dyq5EzDHz4m2GklXpK5kt:mfYyK08fUH1DvNoq5EfzrKDK6t
MD5:	46CC5D3E7E848A9DF719AE33052F8DED
SHA1:	38545B18F1F412F5AAED2FAB80445643AB793282
SHA-256:	2597D4FFF1C555DDCF157349C511AA18830DB85AAD295CDB9FC62C0F461E5733
SHA-512:	DC9201AC197466CF36D36D080701C7B0FED1B81C65F8C72BF4D519E9AB18314E317BE5914825CCC18990E215D3FA52A81AB4F4F9C03878BFEBD6E69EA5C0A4 8
Malicious:	false
Preview:	0\r..m.....V...T....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js .https://microsoft.com/..~." /.....@.....f....cB..cWhT..6..(..$....G..A..A..Eo.....g#..... ...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f9e631a007138c67_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	524
Entropy (8bit):	5.713287895742411
Encrypted:	false
SSDEEP:	6:mxYy74JPCN1F+sVJSJ/ELySTTWt7+H4B8K6tWxYy74JPCN1F+sVJSJ/ELySuittl:S4BSF+J/ELXTatiDE4BSF+J/ELXjtig
MD5:	8EFD0E9E9E8C29E0208978757240A792
SHA1:	90580154A981B59F54EBB77709F637F9A03C4343
SHA-256:	7BB67EC4FE97F0968A8C7F2E45730E10C802A06A994849D2DC08C5517D80396A
SHA-512:	B5E755FEA5AD59DAA74F1C94F8FF7FA10FB6E0A4BC4136F4FA2DEA61CF6562FBF87BED4057685821C9FDE150BA4D1D7C73CBE07653899760825F6930D7214E2 9
Malicious:	false
Preview:	0\r..m....._keyhttps://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/3b1c23908d0aeec856d06e17c3bd1cd1nbr1619796424.js .https://appdomain.cloud/...." /.....6...|.0<..-."e...=.f(....|.fc...A..Eo.....A..Eo.....0\r..m....._keyhttps://kamppcnddemoiz.web.app/xchgjghfvxczx/themes/3b1c23908d0 aeec856d06e17c3bd1cd1nbr1619796424.js .https://appdomain.cloud/..." /.....p.....6...|.0<..-."e...=.f(....|.fc...A..Eo.....v.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ff3254c380ce1732_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1103
Entropy (8bit):	4.989878817199146
Encrypted:	false
SSDEEP:	24:MjXJaGN4zXk16FHPtJ8dtUUuzi19EJkuLUkl5E/9RLFePp++pSp:M9aGQXi6OdCzLJk+UkeE1nePpvK
MD5:	BB410E703718A8A6307E5B02F5E77FF9
SHA1:	BD9A32A33B234B6486E09699C6AF5DCD4CEB0986
SHA-256:	75CF2548674D8EA2F8426F3113A98A54A3AC19A6E9F0A65475188EFDB2D72746
SHA-512:	B73B0D5D5D2038F3574A6729BEA67FB11553C06A78743E03027BC4B61D29DD2F0EF3BD908B4E3AC3648BAE2770933A2440A331797EA0ADE3C85360B4B8D9A50
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ff3254c380ce1732_0	
Preview:	0\r..m.....'....._keyhttps://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=0502864a-b6ef-2f14-9f8e-267004d3a4e0_c5ea3348-55af-729a-2641-14f0312bacf3_742bd11f-3d7c-9955-3df5-f02b66689699_cb9d43d2-fbae-5b5c-827f-72166d6b87fc_49488e0d-6ae2-5101-c995-f4d56443b1d8_7dea7b90-4334-c043-b252-9f132d19ee19_38aa9ffb-ddb5-75be-6536-a58628f435f5_e3e65a0a-c133-43e7-571d-2293e03f85e6_4ca0e9dc-a4de-17ba-f0de-d1d346cb99e2_06310cd8-41c6-3b11-4645-b4884789ed70_5c27e8aa-9347-969e-39ac-37a4de428a8d_d6872b5a-5310-a73c-7cb3-227a3213a1c5_be92d794-4118-193f-9871-58b72092a5ac_64c742e2-b29c-b6c1-fdd9-accf33ec40bd_cf2ceca9-3467-a5b3-d095-68958eee6d4c_cec39dd8-f1d3-56f1-abfc-a7db34ff7b46_ec5fa2c9-3950-ff57-a5c3-1fa77e0db190_d19f9592-65df-bcc9-e30e-439b875c3381_76a3d06f-f11f-77ef-9bfd-6227ba750200_5e1caa45-461c-3b04-f88b-8cd50af16db5_c2dceda8-20b4-7d3f-13b6-9cac67d7df17_914fa41b-cc86-d3b0-4e15-2fdfa357bcc7_40c6c884-da6e-7c2c-081f-4a7dfe7c7245_ae79ba96-1a9d-debd-a5b1-f3067213b9b8 .https://microsoft.com/%..."

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.072255823339335
Encrypted:	false
SSDEEP:	12:2rSeMueK0Y7/5SXz6bire2PCZFwXcA7F7ahsbSESXrUB:2meMbK0U/5SXz6+re/ZFWshsWESXQB
MD5:	6D41EE4D72D053C6C0520080319A5BD8
SHA1:	372035C11B7159AFC771974B3CF5160B244D6AC0
SHA-256:	84A723DBF713FF99375F38423CA258D996FCFE182BD684961EBDE35A98F557EA
SHA-512:	9E8E3D027EA457617B2438DCCD2AF7CB0E9EB6F05780998EA4D50FD5FF53A61DC4A7B11C14EE7776CD8DC4CE3789FB2D0D4CC23AF6475B2E371C32EFC679C20
Malicious:	false
Preview:	.....oy retne.....^]...u.2@.." /.....k-N.@.." /.....x.K.." /.....2...T2...t." /.....YL....{J@.." /..P.....p.&,.<...t." /.....C.+e..j...t." /.....:..4.iJ.9.." /.....V.tp5N.9.9.." /.....M.j.\..9.." /.....T.V.T..9.." /..X.....h...z`..9.." /..{.....g....1...9.." /.....\Q.T.E.9.." /.....7..#...9.." /.....&.tp..." /.....@.....9.." /..8.....%\I..e.H.9.." /....." /.....n.9.." /..#.....;....@...9.." /..M.....~...(..9.." /.....o.A.}.9.." /..{...../...3...5../.....^}.Np.....5../.....I.." /.

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):	24576
Entropy (8bit):	0.9018299267090576
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7UTSZMZLLOpEO5J/Kn7UMMf7SZ7i:dNw3SZaNwwMDSZ7i
MD5:	D3AC82E71B18431798CC37687AF7F2E1
SHA1:	3DD8FC98B70D975B1C4D1338F9E84DBC773F15CD
SHA-256:	33B29F75544EF09EF31E6B8B08A07D70871F79D0EC11760966423ED5ADE2801A
SHA-512:	A07692F45CBEA0A204CF5588183E3CF8069ADF51924D3B527139A860FD09829688B4CB8B5F192238DDBDB73F238BEDD7E0239D6764D588FD636E26DDC018FD2
Malicious:	false
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):	25672
Entropy (8bit):	0.9006276926944337
Encrypted:	false
SSDEEP:	48:mrI+rq5LLOpEO5J/Kn7UTqSZ0qekLLOpEO5J/Kn7Ur8:T+rcNwKSZ0MNwU
MD5:	EBE602743A1C298BA1B10E2EEFD75968
SHA1:	2C37055951571DC63356E5E02415087D7D3F6EE2
SHA-256:	EA7ABB8375E8FB92C9A48B5687CB5A2A456917F4D3B5E54E1B92F5EDB62D44C0
SHA-512:	94F1A323F0A0A5A20305AE14310AE4D85503EACEDF9EE2701957A4EBD8A7F93EB26302847F49295B62391888CD741F9309D6E4168EF5E4D9C7754F0E6E596F34
Malicious:	false
Preview:	.....`-..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Size (bytes):	10212
Entropy (8bit):	4.153061921949023
Encrypted:	false
SSDEEP:	192:3onRnuoRmTuhPomuXRHRsRfYfu2Nqu2tRKRARNbRf7tu2Nqu2kRKRARNCoyO:Yn74yoNJOsIt0eDb/Ik0eDCW
MD5:	713E27EA9F7C0155B5BE4A157AF703EC
SHA1:	70E5508C4AD0CA569F0B3A908871D1EE549070D1
SHA-256:	61D169EC85F056CEC46D5293E59D5221340F73CE0DE1DE8E96A14F11CED014F7
SHA-512:	5AF1CF32B8B9E2EA24AA4B3B333D7679BF8AF43C9D2502CE285CDBC898126A80F6D61C35431AECF64824EEA4AB3E1AE2CE9E9D9C6115235B8D0CCC259840BA8
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...c085f6cf_a3cf_45c5_9a1b_af4e2af2d055.....c.....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....<...file:///C:/Users/user/Desktop/PaymentAdvice%20-%20Copy.htm.....h.....`.....I.\....I.\.... .....8.....<...f.i.l.e.:././.C.:./.U.s.e.r.s./.a.l.f.o.n.s./.D.e.s.k.t.o.p./.P.a.y.m.e.n.t.A.d.v.i.c.e.%.2.0.-.%.2.0.C.o.p.y...h.t.m.....8.....0.....8..... .....<...file:///C:/Users/user/Desktop/PaymentAdvice%20-%20Copy.htm.....9v." /.....

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
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	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
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):	322
Entropy (8bit):	5.210768176632467
Encrypted:	false
SSDEEP:	6:msVvSJcM+q2P923iKKdK8aPrqIFUtpdVvQgEJZmwPdVvQgEcMVkwO923iKKdK8a4:tVzM+v45KkL3FUtpdV4gm/PdV4gpMV5M
MD5:	7731BE415D9B6CE08298087BCF96D390
SHA1:	5601DB46A827B7F08E68DFD2C2ED4FA2B031FD6C
SHA-256:	40AE8059DAE79BEBBCECC8D2A35E2A402B170805698C6422581AEA4C89F64BA9
SHA-512:	FE3E718ACD9A1B7D52CFDB69A411DC39A132E1FE633D744FFC02744EC998F50622675B2128319104BFE85C874919302C3DBB71B1C843DCFF1E18151A3A87289
Malicious:	false
Preview:	2021/05/04-19:58:01.330 186c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/04-19:58:01.332 186c Recovering log #3.2021/05/04-19:58:01.332 186c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.22281995155448
Encrypted:	false
SSDEEP:	6:msVUVq2P923iKKdK8NIFUtpdVpgZmwPdVpIkwO923iKKdK8+eLJ:tVsv45KkpFUtpdVm/PdVa5L5KkqJ
MD5:	25EF0A49F1877294FD043B569DE774CC
SHA1:	4969F5F4FEEAAB31C1CF5A08BCF56B07018FD7A6
SHA-256:	F47407292607E8CFA5534669EFE2A223F1E3654504E146BE8F5711554463BAC2
SHA-512:	2CDCC73BA080113772F8EF0CC6441AF22644C34B0D63E825672951672F1A6634B50F0F66BFE431918C90C758B629A4DF49E0FE4CDD23DDF34DBB52D97F2450D
Malicious:	false
Preview:	2021/05/04-19:58:03.478 1854 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/04-1 9:58:03.479 1854 Recovering log #3.2021/05/04-19:58:03.479 1854 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:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclJ5 n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
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=","hqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	2.539361461363952
Encrypted:	false
SSDEEP:	384:zYbGh8VPUHIM+Yb1PlwGO8VouHIM+YbeAPVvwGO8V5V:X+mPVRAPVVV
MD5:	9C2DEC70713AA87860DD64702589F39D
SHA1:	195F9C81457B25CD2D3AC1B6392A4A84F78B1643
SHA-256:	5A48857680FB883525E3ABCA30D496B59A6BA942C8290435D96A642B0C0E1A55
SHA-512:	6A88B520CA72E53FA6E9E14862BD202B8ED2B30F7C97AFF7B488CBD4C918AACD45C467D751B8246BAD764604DEDD86C4379E5A3F9B0630B356ACD4A14E44C81
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	46804
Entropy (8bit):	1.6141687415172894
Encrypted:	false
SSDEEP:	192:VL6ReRJ1RZRaR9Rh4Xk4u4tAVRfeRkRgReRJ1RT14HRfqRaRkRaR9RI:Vu8VXYbIXZPKwGO8VwHIM+Yb2
MD5:	1DAA767DA6CEB411C7402932A2798DA2
SHA1:	3054B5F261AF45A6B76C8D315E5603EBC661B25D
SHA-256:	F61846955D3E0537130935B82D9AFC6CE9F77C9555219636F9A20AA95CEF51C1
SHA-512:	D15F0D800837F7817E42172686FA5B419C8F7AFBF20974762EE99DD9DBD663906C245D45217687BEAF55383F6F3C08722D34E465C46CFFCF7AAD6A7C69B6BAC
Malicious:	false
Preview:	.....4..... ....

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
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):	374
Entropy (8bit):	5.266991016921828
Encrypted:	false
SSDEEP:	6:msVadlWM+q2P923iKKdK25+Xqx8chI+IFUtpdV9Fc1ZmwPdV9FKWMVkwO923iKKN:tVWL+v45KkTXfchI3FUtpdVnC/PdVnKE
MD5:	C9D103AD7922BA9E57307D64BDB63477
SHA1:	EF4EBDEA9888305F49882D17DA36718F1CD86DBA
SHA-256:	A3A6299051DB3003ACF78B5C020A9BEADC247D7754EC674876B356A4651FB550
SHA-512:	56DAC3F20F46BCDDF8B588168E27F20D38001166337307238 5C99B02B3CE3240490C32F9587D70449B8A5F60BE5258EB937D6E4B2DD319F267E256A8C2156609
Malicious:	false
Preview:	2021/05/04-19:58:06.262 1bac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/05/04-19:58:06.338 1bac Recovering log #3.2021/05/04-19:58:06.338 1bac Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.234359394977519
Encrypted:	false
SSDEEP:	6:msV/LWM+q2P923iKKdK25+XuoIFUtpdVs1ZmwPdVHdlWMVkwO923iKKdK25+Xuxo:tVDL+v45KkTXYFUtpdVS/PdVHLLV5L5X
MD5:	9D58572C2497EFFBF97B37CE91AC1449
SHA1:	7CCF46086851113281FCD97AA04EE2D5A5852D4D
SHA-256:	4F6ABC6CF5B5FA24FD9AF7784304D5F76A2F0E1776884B8EFFF0A722FDEE8591
SHA-512:	CF74E81817C1EF5B5F36F02811B621C15E674D5A20A0385229D9FF922B715E54951AD195366A8C98E198356E1C47996567EAB222FEFBD9A6D4D620865E136580
Malicious:	false
Preview:	2021/05/04-19:58:06.179 1bac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/04-19:58:06.231 1bac Recovering log #3.2021/05/04-19:58:06.250 1bac 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):	332
Entropy (8bit):	5.255098825767274
Encrypted:	false
SSDEEP:	6:msVWk+WM+q2P923iKKdKWT5g1IdqIFUtpdV5dz1ZmwPdV1+WMVkwO923iKKdKWTk:tVWrL+v45Kkg5gSRFUtpdV5v/PdV4LV5
MD5:	B2BF39987E6F00F4C08F66FB9C04FBA1
SHA1:	B15CF770EA0D67E16B062D71498C418C1337BFDC
SHA-256:	30381AD6AC836671F96C2C2152C82845936B4679764F885835EF9A364A276A3F
SHA-512:	9C1521BEB782F7F32D58038A2819CA52DB721A2C01A1E7B20645A3A043AAD7B743B96731467CED35C649ED3F33E5CB805FCDB03640566DF5F3318796F80D34A
Malicious:	false
Preview:	2021/05/04-19:58:05.968 1bac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/04-19:58:06.032 1bac Recovering log #3.2021/05/04-19:58:06.048 1bac 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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8EflQB:8p
MD5:	A7B5DC8A9583BE50CD29E3DCC9C1A244
SHA1:	B51460C14DEC95B39EA7873B27F53ABD15C1C2F0
SHA-256:	6DDA55EE32994519C4DB2C4981B700C1A0843AF1D75D713474CC508E636EC423
SHA-512:	BA17B510FD940F52CBC92209A852BF05C138C2A903FB4B1B6D7F88452F201460CE701660D5A1381B373F505151BDAB95B00CE59BBCF684A55F39E6A2AC0B0EB
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Preview:	.'..(.....4." /.....

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):	1.2899098616351816
Encrypted:	false
SSDEEP:	384:QlvD1N8VCmQQW8vDXitKN8VZmQQW8vDM2PtKN8VP:TRZL
MD5:	6E697EF2E13A6D2D54FD12F9ED804EF5
SHA1:	15407D5E9222B17A5AC8A098DDF8D81FFD862513
SHA-256:	B43469E8B84F0C45622CDCC8B8AB2060AC10BE669444767BB84740E69596F201
SHA-512:	AB7D2BB9B0DDB25CCDAAB59513F0D29DFFF8B25BD9FD0E240355D42CE605868112038438453EDC5DAFD169CF3BCAD54C2365E3E5A45628684313B41F2FF651 7
Malicious:	false
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):	1152
Entropy (8bit):	5.554468744430809
Encrypted:	false
SSDEEP:	24:z+qQJxLYWFQc0MvhhyWXi7ASUWZ0j0SyK4thTyo7nQBrxzkrjytW05BKyv/PNQ:YJxLYaQVMOdszTj07K4AJFQ2RMKa
MD5:	AA72C31B5C49B1478F20DF8E54B80B2D
SHA1:	821D6AB23AC3AED8D40E96F1202AE24903DC796A
SHA-256:	4C3D4409F096D8D47D5C0B47B62726877EA9D4D3802109B2A86A8E7A2DDB7024
SHA-512:	D977D9342F545159FEA0554A9A0B63DFCDEE3F9EEC00383BF43E778A9260385E95C208C5E7B3195DA18B989862D68F6A8A6A6E1AD9BCBB9DDB3AF41C1312F5 F
Malicious:	false
Preview:	.....".....appdomain..bbre..cf..cheerful..cloud..https..impala..jgauozxiisaozxs..ms..south..us..zoisaizx..user..c..copy..desktop..file..htm..paymentadvice..users*.....u ser.....appdomain.....bbre.....c.....cf.....cheerful.....cloud.....copy.....desktop.....file.....htm.....https.....impala.....jgauozxiisaozxs.....ms.....paymentadvice.....sou th.....us.....users.....zoisaizx..2.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p..... ..r.....s.....t.....u.....v.....x.....y.....z...:..... .....B.....y..... .....*Uhttps://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/?bbre=zoisaizx2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	100580
Entropy (8bit):	0.7421071961416568
Encrypted:	false
SSDEEP:	192:SZrFRfReRJ1RGRLRlR1R7jRffRsRfReRJ1RUoRYRf/GQWR6RlR1ReDv:S3N8VIlvDttKN8VqomQQW8vD0T
MD5:	AC07396BDC95959F56BE5C56454C53ED
SHA1:	E6E232AFDC7B358CE3C633408EA3963906C3605F
SHA-256:	CED102504E3E60C54400B9BD715878B086FC91E6BF403A88E23CBCAE81198C9E
SHA-512:	481D91DE2F37A40F5853A843F508CFF651FF99769ED4CD8D7CB439618036FD0FBCC25FB0EF25EC72FB4D66F8FF2E8FDC12EE75C77EA52BA1B227E9A22F046E 4
Malicious:	false
Preview:	.....[~X..... ....

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):	3919

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Entropy (8bit):	5.555523555907314
Encrypted:	false
SSDEEP:	96:DRmRoRadR7Rkpa7QMQdbOgwNbQ5fgGmrS0vRhR7Rp:DRmRoRadR7RkpyQHdagwNE5fgzvRhR7z
MD5:	EF6948168294B8A8E093EE47E6DB44DA
SHA1:	C1BB0FD71E9840B2B45E42F1CB2C889B4AA385F9
SHA-256:	243308701675E5BEA5619D6B33979082965C0AB11154F790360EA9AAD36FC984
SHA-512:	8B39A9092B4125978F7636FA0C2EC3E4F5E6403C2E021C6C073FF84F88D9116D5F1B2846DEF31BEEA2A6FB5D81944D30F626FEDEF591AA18E3DD25C6A6792E3B
Malicious:	false
Preview:	.....*.....KMETA:https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud.....S_https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud..browserkeyN.{"browser":{"detect_browser":"","detect_browser_detail":"","detect_btan":""}}.P_https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud..userkey...{"user":{"keepLoginLongtime":0,"AuthNBR":false,"AuthKeyNBR":false,"tk_nbr_uc_frv":"","br_nbrcheck":"","br_utcheck":"","testlist":[]}}.`_https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud..._canWriteToLocalStorage.R_https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud..nbrteststst...../.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.Reque

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):	334
Entropy (8bit):	5.194341424108093
Encrypted:	false
SSDEEP:	6:msVGL+q2P923iKKdK8a2jMGIFUtpdVa1ZmwPdVeFLVkwO923iKKdK8a2jMmLJ:tVbv45Kk8EFUtpdVa1/PdVO5L5Kk8bJ
MD5:	E1BFE15D5F69CCB8067A06FFB780777F
SHA1:	F0DDC57458E7D080C1D7BF5707A70378DC759D34
SHA-256:	9B1C3D8D15633C04453116D43F558CBDA454EB3201059602BE39E43A089612ED
SHA-512:	0AFE429CE325347DE40FF1DFEBAADF7FB5573A8F120829D8EBB31C1ED2F51C86B90770331047954DC121C338C539DC8DECCE04496E277F4B4D1710B0B754DDE
Malicious:	false
Preview:	2021/05/04-19:58:01.032 1758 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/05/04-19:58:01.034 1758 Recovering log #3.2021/05/04-19:58:01.036 1758 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	1.3882220955421123
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOOcRz0OqAuhjspnWOP1mt9dT9on/9Fnh9XUlY9pEOqAuhjspnWODR:HhESBmUTCUxTmUaV
MD5:	EB0882374CDC8D4C91A453710A80EDE2
SHA1:	7C33D1C2EEB3BFBF867C72383EE713E97587361C
SHA-256:	731CE6EEA25363B8CC7232FF59B146C8B2408FD029E165E5F72C031478F9EF02
SHA-512:	F4EA1116495EE6EF4ED5CBB4243F40BC1A7E66B4BBDFB845B2A412601ACDDC8BBE3674C41605C5AAD9CEE09A348E6666B14347923590D6B9A96A54544DCA19A4
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38508
Entropy (8bit):	1.1384205435509043
Encrypted:	false
SSDEEP:	96:bIUOqAuhjspnWO8kOqAuhjspnWOx7k1mt9dT9on/9Fnh9XUlY9u0OqAuhjspnWOG:8y5iCmU5SLJ
MD5:	0A2E8A676198184378BF4CAAA9923CEC
SHA1:	9557A31A8EBEB52700265F09E88100DAACEC423C
SHA-256:	FE5812739FE588AB49873F17E84B6C2DA67AD193BA9A41457598963690A0858A
SHA-512:	9612C552ED2044633E443DC3682B7C1B9D367B028771085B3779DA91FF072FE1BB9C197BD580B9895003BCBE9DD94F42A712442584D53AB5261D7877CF7D5A96

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Malicious:	false
Preview:	.....FS..... ....

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):	336
Entropy (8bit):	5.212522482941581
Encrypted:	false
SSDEEP:	6:msVvoVq2P923iKKdKgXz4rRIFUtpdVvVYgZmwPdVvUYIkwO923iKKdKgXz4q8LJ:tVIv45KkgXiuFUtpdV9h/PdVc75L5Kkt
MD5:	660564C54A2A787504F84E4D1C1DEC75
SHA1:	2371391096AF2E191AAE6C65978D96906D7E56B0
SHA-256:	DF31D81B3A45FCBC148BEBAD70F4008369FAD1E47B2C3D26D380A58E5912C160
SHA-512:	C462636DDD518CCCE2034FA958D5EC7C1692A6CF03215A37E88701E5F504A7C0C2554B6E48555B4DE3EB119E3D49716239EAFAAB0FC763C663F2855EB7B263C B
Malicious:	false
Preview:	2021/05/04-19:58:01.368 1870 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/ 05/04-19:58:01.384 1870 Recovering log #3.2021/05/04-19:58:01.385 1870 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Noti fications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.0817899082368019
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUhWncK+KPJKUiY:wIElwQF8mpcSs91PZibPniKDFM
MD5:	A7DC53733BA110E67FBD46ED25EA9278
SHA1:	7DC6F3583C5E96BAAEAA00D9B0019CCB464A55A0
SHA-256:	08884D341F70ACF06D18AE03B9ABF817AD56FA6F4C0167370B6BFBD686EF542C
SHA-512:	30A5203FC066A5B2415BA512EEDEFC54CB9C1A5821DDD7B362DD20BB6F1BBE2CC6D9889B5E20A991C04ED6F947DE9CA8E0FE8AFA7D724A7FD2758634B1E7E 7E8
Malicious:	false
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):	0.6272921194899845
Encrypted:	false
SSDEEP:	48:yvYqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUw4:yvYhIElwQF8mpcS7
MD5:	F3AE176D2DAD7DC8EACCCBE408E0BA90
SHA1:	B34360D964B38ECA79E589E1380431CAE8A95525
SHA-256:	EDA634432B7F194F024008501A15B6FDE026CCA713EA7ABDBDC93E1CC51E419B
SHA-512:	4D15A9C223DEF46F3D316C634B01F48247F3601B8FE2E12DC02EC209F2918CE0D937C7F7D173040376469A7ECA07123AE28E7729B770744088B42EE7AA8E73CC
Malicious:	false
Preview:	.....g..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Size (bytes):	542
Entropy (8bit):	5.0352658871689036
Encrypted:	false
SSDEEP:	12:5IlbtWaRW0jlwJKMnXcl85CcJ0W0jlgDrtl2GjUXzkzkzkzk:7FtWaRW05wJKMnXcl84cSW05GZlLlj8x
MD5:	BF0800C29DA10E04580CF67ED40899B0
SHA1:	DFB374A5821DEDFCE14A04DB2183D75612E0E91D
SHA-256:	C5461F2738F349477D86AB5F1CEC303357E54E1DDB0296F147CDB8EFA61B324B
SHA-512:	D92C13AD06F101A88012362C083D5A3E4C87505A2433B8511DAE3E6D8582ADD5F59868E76B11BB7053369A2EEB228F3427A9198B3C96DA8579C2F4463373E3AA
Malicious:	false
Preview:	..&f.....`j.....next-map-id.1.vnamespace-c085f6cf_a3cf_45c5_9a1b_af4e2af2d055-https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/.0&U.93.....map-0-ReadyFIle.{.}...map-0-nbrteststr.....next-map-id.2.vnamespace-961ff405_4ca4_4ea5_ac07_7ee64bf2bc1e-https://jgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud/.1...a3.....map-1-ReadyFIle.{.}...map-1-nbrteststst.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.1725498654521855
Encrypted:	false
SSDEEP:	6:msVVScM+q2P923iKKdKrQMxIFUtpdVP3JZmwPdVhocMVkwO923iKKdKrQMFLJ:tVVM+v45KkCFUtpdVPZ/PdVLMV5L5Kkf
MD5:	329EA90B4D561A73DB6B63B9F39C70F6
SHA1:	2C1BF9B8D0D0CC31D3BC7CE7FEF4EB94B4442AF5
SHA-256:	67AD51129DCE6A61AA395AB33D4E63A69184119682D881FAD88FD8A5A7835280
SHA-512:	7FF515EFE6C667D2ACA3DCCF6440BA6A8FF8C8834637EEB627E82B06D1381E0F9EE74AAEFB7E3F999FD81765258A6F091A0B89479C22AD251E1C57401F36671
Malicious:	false
Preview:	2021/05/04-19:58:01.282 186c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/04-19:58:01.283 186c Recovering log #3.2021/05/04-19:58:01.284 186c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.182482591472518
Encrypted:	false
SSDEEP:	6:msVNFLEL+q2P923iKKdK7Uh2ghZIFUtpdVH11ZmwPdVDFkHlLVkwO923iKKdK7UT:tV7Zv45KklhHh2FUtpdVV1/PdVDF45LI
MD5:	DEDCD8CFC689D6003D993896DC073295
SHA1:	066C1E07BB48D754295B67242120058889EA32EF
SHA-256:	B852CB6785B4D453FAF537F96285FB5495FAF3FCDE881C53045609AFE31A42AB
SHA-512:	7B7E5B04EE04A7028AA6BBCA5F637384140DBA2FCF8CC6260CB1DFD0655FE93B68D367A944AFE770F7306FD21AEFA633B23D79C470AE299F08CB5C3B6A9971C
Malicious:	false
Preview:	2021/05/04-19:58:00.996 1758 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/05/04-19:58:00.997 1758 Recovering log #3.2021/05/04-19:58:00.998 1758 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\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
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):	432
Entropy (8bit):	5.229943287312913
Encrypted:	false
SSDEEP:	6:msVa9+q2P923iKKdKusNpV/2jMGIFUtpdVvwJZmwPdVvv9VkwO923iKKdKusNpV0:tV5v45KkFFUtpdV6/PdVD5L5KkOJ
MD5:	89C6562B80CAFFACE37C30EA02289CFB
SHA1:	F1455AB8A6EEAB3ECF350857CDB101592C1F00EF
SHA-256:	631807C9122D334B031D231453A4BB2C35B115DF2C7BC438957AA10711020262
SHA-512:	0A06A7C8EA978D054F5553ABC77D2B44DFAD51588560C7B50C4E81989A27387DC0096B01AB5A8C22897112E2F6415FA0F01BE08E23268A6518C511CEBE452307
Malicious:	false
Preview:	2021/05/04-19:58:01.298 1808 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-19:58:01.300 1808 Recovering log #3.2021/05/04-19:58:01.301 1808 Reusing old log C:\Users\user\A ppData\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):	434
Entropy (8bit):	5.29544879240401
Encrypted:	false
SSDEEP:	6:msVvY99+q2P923iKKdKusNpqz4rRIFUtpdVv0nJZmwPdVvP9VkwO923iKKdKusN9:tVJv45KkmiuFUtpdV8J/PdVj5L5Kkm2J
MD5:	DFFA69A449099A339309714F9149E9A3
SHA1:	3A7024E7A6C55AC6684471B31D3116DD292CCD71
SHA-256:	A2027EE20EA4A495552D822276750AC8BBDE33DF5290F7A13FD8A90174F5E80C
SHA-512:	7BD86FBAB8EE7CE42453DEDB21D44DCB99CD3753F827A593EE9C101AB8036C4EF0EB992E3BB64DC7370DA29EA824075FBE148E54BD6ABC76C184052A5816F DFE
Malicious:	false
Preview:	2021/05/04-19:58:01.359 1808 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/05/04-19:58:01.364 1808 Recovering log #3.2021/05/04-19:58:01.367 1808 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
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):	420
Entropy (8bit):	5.310177310158121
Encrypted:	false
SSDEEP:	6:msVUeltSVq2P923iKKdKusNpZQMxIFUtpdVUenggZmwPdVUehgIkwO923iKKdKuG:tVKv45KkMFUtpdVbp/PdV95L5KkTJ
MD5:	3EDF18162703EBB1695373F6E1FF56B2
SHA1:	20533A1FC31E78B34718EDCD876F2B6CE628ED2C
SHA-256:	FFFB77CCD87D429D905AD8CAB63A38EE0481CC2907B2D0D0ABDD6512219CF752
SHA-512:	4FDECE075F32ECF07E20E0F952AE1BFDFC6AD094FAE81C4353A9067AA32D276A05A92AF50CA244B08B7B68145E73BF9F51EC155B1F256515364B24769D145CE D
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Preview:	2021/05/04-19:58:17.691 1854 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/05/04-19:58:17.693 1854 Recovering log #3.2021/05/04-19:58:17.695 1854 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\gfdkimpbcpahaombhbimeihdjnejgicl\def\ebcf7c00-8d14-46ae-b44b-5b5422f7c826.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):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","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\0e7836c0-b7f5-444c-a4ca-4d07e7980df0.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):	325
Entropy (8bit):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FBI27
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","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
Malicious:	false
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):	432
Entropy (8bit):	5.238552149478161
Encrypted:	false
SSDEEP:	12:tVJM+v45KkkGHArBFUtpdVWS6/PdVOMV5L5KkkGHAryJ:td45KkkGgPgTgSehL5KkkGga
MD5:	3691C68C1A8BC1AAB55E0F94F0CD6FA7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
SHA1:	C3BFEBC129848D51373C5CE80B284DCAF5975F25
SHA-256:	8A4EAEA2E9065A795DAF0D91B8079D054CE1C706EF8A1422C41524CCE5A4AD21
SHA-512:	685B38905B77067B11882437C7E228C052CD292D9A95AC0ECBEB426BE280A9063BB34D1C73D9C3A6B3696A242E96516E3CEBF0C66472673D40D4B8FEE0473A9
Malicious:	false
Preview:	2021/05/04-19:58:06.472 186c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-19:58:06.474 186c Recovering log #3.2021/05/04-19:58:06.475 186c 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):	434
Entropy (8bit):	5.250080767953239
Encrypted:	false
SSDEEP:	12:tVRv45KkkGHArqiuFUtpdV+t/PdVpF5L5KkkGHArq2J:t/45KkkGgCgTg7HXL5KkkGg7
MD5:	448061E495C92D18D443B2B7AD4AAC0C
SHA1:	6E973E2FDF1EC61BBBD6E82B89557FE48DB72BA7
SHA-256:	3E2D12F054E36F6EC3DCDB86BBBDD33519F7CE7482E20DC3E80B1412522200AE
SHA-512:	8B6FE89EE571C47707C381A407A8838759889FFA6D38CE0BFBA6E35E900D641CD128D7371B0C3F6CA95A3DF6B3A0AADDEFB09BCF2AC2828F9F625003114CDA A2
Malicious:	false
Preview:	2021/05/04-19:58:06.494 1858 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/05/04-19:58:06.496 1858 Recovering log #3.2021/05/04-19:58:06.497 1858 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
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.187693271480641
Encrypted:	false
SSDEEP:	12:tVzv45KkkGHArAFUtpdVp/PdVj5L5KkkGHArfJ:tR45KkkGgkgTd3L5KkkGgV
MD5:	F8205A5508C15403A258CD5A4362C58E
SHA1:	6F4E0FF3EB774AA7A0709B7FF6573C2839F4E1FF
SHA-256:	0E26C20564FE4EBC16925972ED55B6198CEFE5C054087F416558C073E430B518
SHA-512:	8FCEB07563CF0DD4B2A576DAF67852B07ECB0FB4CA26F938CF6E8893BF282CB2DE1C8F60B689382654971DB4068815D1E8C946A01BC699E0A42A7E6CFAFE5A D
Malicious:	false
Preview:	2021/05/04-19:58:21.999 1860 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/05/04-19:58:22.001 1860 Recovering log #3.2021/05/04-19:58:22.001 1860 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
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):	326
Entropy (8bit):	5.21337839258027
Encrypted:	false
SSDEEP:	6:msVTdjL+q2P923iKKdKpIFUtpdVwW1ZmwPdVxd4lLVkwO923iKKdKa/WLJ:tVTdOv45KkmFUtpdVp1/PdVxKz5L5Kk7
MD5:	722D50ACF251EDE0CFB2F7D4E8D8B81A
SHA1:	BDB599CEB7A15168FA464461B7E9E04E0804341A
SHA-256:	6A5E548B55BB8B5C841DF1AF87272841411E6D11470584BE8879FF23C2BEA8A3
SHA-512:	A3B1158612872F48FD73E6E74A6169F6301080C4FBCA5164454B413E3E61F4103A360C578F4FDB068A629683949A170E905927EC389A8185070672B234B22EBB
Malicious:	false
Preview:	2021/05/04-19:58:01.019 1758 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/05/04-19:58:01.022 1758 Recovering log #3.2021/05/04-19:58:01.023 1758 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.316374556204126
Encrypted:	false
SSDEEP:	12:tVEUv45KkkOrsFUtpdV/8/PdV/85L5KkkOrzJ:tt45Kk+gTlQlmL5Kkn
MD5:	21D1D3D3B6638E7FAF09CF9F798F4CFF
SHA1:	70D8678BD3BB8F59BA30D1F41865B6A795B6DDCE
SHA-256:	B87AE6685BC6F27E149C4046A8580A537E2243446D2E2CD34B21B747A0B3008D
SHA-512:	0A513388E08F202046AAC4BD7D393F71EBA53B525411A78E1FFAF1003DA3AC319174DEDF5973AA4D97A714D189290CFE0D7AF43F61D4BF8D02D0A436F9A3B61C
Malicious:	false
Preview:	2021/05/04-19:58:08.141 1860 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/05/04-19:58:08.143 1860 Recovering log #3.2021/05/04-19:58:08.143 1860 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	180
Entropy (8bit):	5.6926403880550005
Encrypted:	false
SSDEEP:	3:Cigaw8xtrE61UjlKlA8yllHXRb6tVlbazFwv/1lLzKlOt3e/RkRow:bw8xtrEMH4lxKlgGv/vLzK08Xw
MD5:	9A6259D1E8F6BC8B0F4AF6D5B31C7730
SHA1:	6767E083ECE5A947D04FEB918DC9AA516FF3C736
SHA-256:	FCD4C711EBC417E51B9ACF2B2FDDA2E549D5CF5DC05A66E4384E4F7844794AC9
SHA-512:	4C708CDBC8736D957AA05AF4F6F00DE9709716A4372663F626B4C939575F3A100FC834E49ED5568FD6B1819C2D5AFF7CD6ABBAB4FFEFCC5CC36AA6928F556EF
Malicious:	false
Preview:	....&.....;.....j...Xd.....9m.-.&.....O#.....b...9]d.....O.]...I....0f.O..w.....Z2.q...../..io#.....G..C'h.....n-.....D+.NB$.....I(.vg..q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b6ecae21-7447-4aba-9bba-344f3571b4f1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b6ecae21-7447-4aba-9bba-344f3571b4f1.tmp	
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535718098817934
Encrypted:	false
SSDEEP:	384:RbWtULlxNXo1kXqKf/pUZNCgVLH2HfDsrUxHGdnTj7F1T4xp:lLlfo1kXqKf/pUZNCgVLH2HfgrUlGdnI
MD5:	8CB7E4C4B1AE084F3F84D12C334F38D3
SHA1:	A21A25B45CE2B3A40E442CB9E7EFDD5829567905
SHA-256:	692CDD14DC680B1D53F0615BD22186A95B8BCD93F392FA4AEFD83385649F458D
SHA-512:	600E74BAB210F18332576901159E6E10A82DFE7A2B98629066754E0C61C93C7D2A1EA208F519D352352C305A87AF3B8FD173D4563E1355A865B21DD6372E83AC
Malicious:	false
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":"13264657081014765","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Preview:	MANIFEST-000004.

Static File Info

General

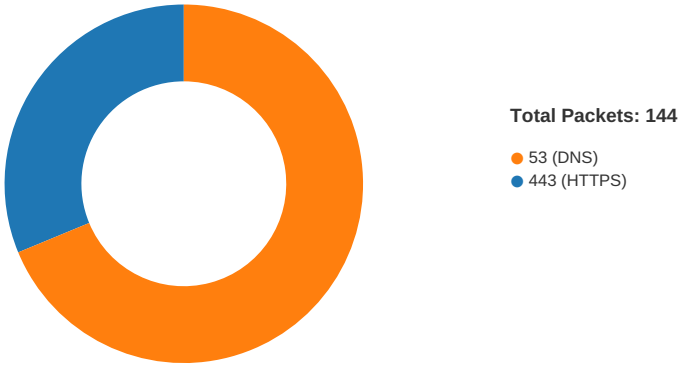
File type:	HTML document, ASCII text, with no line terminators
Entropy (8bit):	5.052992049009961
TrID:	
File name:	PaymentAdvice - Copy.htm
File size:	237
MD5:	d4db2888082b56c8f23bd9c5be33df2c
SHA1:	617f8f0b10e6ecf6cac39dd1e4d9ac342aa00d33
SHA256:	efa07c2136f6a05babbcd3b39e8b9213af742d7e34b79b08fa86634f4743674d
SHA512:	73e72080f11053fa4a78118438b08754f10f2a00caf5b29fe79d8fcdad05d08967bc10d449dfe896c1c53789b9320f0ab2f402b67a022f2233fbd7ab287aca94
SSDEEP:	6:S0/7LAdqkiWbFAHXW9UH6Muz6UGMWEKcIGxBPNeTswAO3BXlfOhAb:Su70dqk5/2an3W0jlw/R1Oyb
File Content Preview:	<script language="javascript">document.write(unescape('%3Cmeta%20http-equiv%3D%20%22refresh%22%20content%3D%221%3Burl%3Dhttps%3A%2F%2Fjgauozxiisaozxs-cheerful-impala-ms.us-south.cf.appdomain.cloud%2F%3Fbbre%3Dzoisaizx%22%3E '));</script>

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:58:04.243839979 CEST	49708	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.244513035 CEST	49709	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.283982038 CEST	49710	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.403073072 CEST	443	49709	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.403197050 CEST	49709	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.403579950 CEST	49709	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.404943943 CEST	443	49708	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.405061960 CEST	49708	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.405348063 CEST	49708	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.443026066 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.443139076 CEST	49710	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.443691969 CEST	49710	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.561671019 CEST	443	49709	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.565543890 CEST	443	49708	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.572361946 CEST	443	49709	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.572392941 CEST	443	49709	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.572405100 CEST	443	49709	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.572499990 CEST	49709	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.576086044 CEST	443	49708	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.576113939 CEST	443	49708	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.576129913 CEST	443	49708	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.576210976 CEST	49708	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.602360964 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.614579916 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.614604950 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.614618063 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.614679098 CEST	49710	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.642538071 CEST	49709	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.644764900 CEST	49708	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.648329973 CEST	49710	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.800740957 CEST	443	49709	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.802254915 CEST	443	49709	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.804810047 CEST	443	49708	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.806488991 CEST	443	49708	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.806754112 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.808839083 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:04.859703064 CEST	49708	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.859750986 CEST	49709	443	192.168.2.5	169.62.254.82

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:58:04.861409903 CEST	49710	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:04.927153111 CEST	49710	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:05.107702971 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:05.107734919 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:05.107749939 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:05.107760906 CEST	443	49710	169.62.254.82	192.168.2.5
May 4, 2021 19:58:05.107810020 CEST	49710	443	192.168.2.5	169.62.254.82
May 4, 2021 19:58:05.610898018 CEST	49715	443	192.168.2.5	104.21.91.175
May 4, 2021 19:58:05.652760983 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:05.652920008 CEST	49715	443	192.168.2.5	104.21.91.175
May 4, 2021 19:58:05.653225899 CEST	49715	443	192.168.2.5	104.21.91.175
May 4, 2021 19:58:05.694061995 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:05.701309919 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:05.701334000 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:05.701395035 CEST	49715	443	192.168.2.5	104.21.91.175
May 4, 2021 19:58:05.713526011 CEST	49715	443	192.168.2.5	104.21.91.175
May 4, 2021 19:58:05.713685036 CEST	49715	443	192.168.2.5	104.21.91.175
May 4, 2021 19:58:05.713968039 CEST	49715	443	192.168.2.5	104.21.91.175
May 4, 2021 19:58:05.755574942 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:05.755593061 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:05.755599976 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:05.758718967 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:05.758995056 CEST	49715	443	192.168.2.5	104.21.91.175
May 4, 2021 19:58:05.802444935 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:06.089185953 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:06.089204073 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:06.089220047 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:06.089231968 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:06.089246035 CEST	443	49715	104.21.91.175	192.168.2.5
May 4, 2021 19:58:06.089272976 CEST	49715	443	192.168.2.5	104.21.91.175
May 4, 2021 19:58:06.159692049 CEST	49715	443	192.168.2.5	104.21.91.175
May 4, 2021 19:58:06.167627096 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.210926056 CEST	443	49721	151.101.1.195	192.168.2.5
May 4, 2021 19:58:06.211019039 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.211604118 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.257469893 CEST	443	49721	151.101.1.195	192.168.2.5
May 4, 2021 19:58:06.257503986 CEST	443	49721	151.101.1.195	192.168.2.5
May 4, 2021 19:58:06.257523060 CEST	443	49721	151.101.1.195	192.168.2.5
May 4, 2021 19:58:06.257543087 CEST	443	49721	151.101.1.195	192.168.2.5
May 4, 2021 19:58:06.257561922 CEST	443	49721	151.101.1.195	192.168.2.5
May 4, 2021 19:58:06.257574081 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.257576942 CEST	443	49721	151.101.1.195	192.168.2.5
May 4, 2021 19:58:06.257600069 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.283750057 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.283958912 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.284107924 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.290230036 CEST	49722	443	192.168.2.5	216.58.212.129
May 4, 2021 19:58:06.330873013 CEST	443	49721	151.101.1.195	192.168.2.5
May 4, 2021 19:58:06.330904961 CEST	443	49721	151.101.1.195	192.168.2.5
May 4, 2021 19:58:06.330925941 CEST	443	49721	151.101.1.195	192.168.2.5
May 4, 2021 19:58:06.330945969 CEST	443	49722	216.58.212.129	192.168.2.5
May 4, 2021 19:58:06.330987930 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.331038952 CEST	49722	443	192.168.2.5	216.58.212.129
May 4, 2021 19:58:06.331377029 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.331556082 CEST	49722	443	192.168.2.5	216.58.212.129
May 4, 2021 19:58:06.342796087 CEST	49721	443	192.168.2.5	151.101.1.195
May 4, 2021 19:58:06.373636007 CEST	443	49722	216.58.212.129	192.168.2.5
May 4, 2021 19:58:06.379606962 CEST	443	49722	216.58.212.129	192.168.2.5
May 4, 2021 19:58:06.379647017 CEST	443	49722	216.58.212.129	192.168.2.5
May 4, 2021 19:58:06.379671097 CEST	443	49722	216.58.212.129	192.168.2.5
May 4, 2021 19:58:06.379693031 CEST	443	49722	216.58.212.129	192.168.2.5
May 4, 2021 19:58:06.379723072 CEST	49722	443	192.168.2.5	216.58.212.129

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:57:52.797283888 CEST	54302	53	192.168.2.5	8.8.8.8
May 4, 2021 19:57:52.848886013 CEST	53	54302	8.8.8.8	192.168.2.5
May 4, 2021 19:57:53.181952953 CEST	53784	53	192.168.2.5	8.8.8.8
May 4, 2021 19:57:53.259314060 CEST	53	53784	8.8.8.8	192.168.2.5
May 4, 2021 19:57:53.431231022 CEST	65307	53	192.168.2.5	8.8.8.8
May 4, 2021 19:57:53.480134010 CEST	53	65307	8.8.8.8	192.168.2.5
May 4, 2021 19:57:53.866444111 CEST	64344	53	192.168.2.5	8.8.8.8
May 4, 2021 19:57:53.916564941 CEST	53	64344	8.8.8.8	192.168.2.5
May 4, 2021 19:57:54.325776100 CEST	62060	53	192.168.2.5	8.8.8.8
May 4, 2021 19:57:54.382895947 CEST	53	62060	8.8.8.8	192.168.2.5
May 4, 2021 19:57:54.475996971 CEST	61805	53	192.168.2.5	8.8.8.8
May 4, 2021 19:57:54.527570963 CEST	53	61805	8.8.8.8	192.168.2.5
May 4, 2021 19:57:56.432337999 CEST	54795	53	192.168.2.5	8.8.8.8
May 4, 2021 19:57:56.500030041 CEST	53	54795	8.8.8.8	192.168.2.5
May 4, 2021 19:57:56.629874945 CEST	49557	53	192.168.2.5	8.8.8.8
May 4, 2021 19:57:56.678436995 CEST	53	49557	8.8.8.8	192.168.2.5
May 4, 2021 19:58:00.477924109 CEST	61733	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:00.531573057 CEST	53	61733	8.8.8.8	192.168.2.5
May 4, 2021 19:58:04.003758907 CEST	62176	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:04.012444973 CEST	59596	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:04.020462990 CEST	65296	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:04.032215118 CEST	63183	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:04.070250034 CEST	53	59596	8.8.8.8	192.168.2.5
May 4, 2021 19:58:04.076916933 CEST	53	62176	8.8.8.8	192.168.2.5
May 4, 2021 19:58:04.080560923 CEST	53	65296	8.8.8.8	192.168.2.5
May 4, 2021 19:58:04.105186939 CEST	53	63183	8.8.8.8	192.168.2.5
May 4, 2021 19:58:05.023894072 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:05.084049940 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 19:58:05.494652987 CEST	55161	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:05.510960102 CEST	54757	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:05.553252935 CEST	53	55161	8.8.8.8	192.168.2.5
May 4, 2021 19:58:05.609563112 CEST	53	54757	8.8.8.8	192.168.2.5
May 4, 2021 19:58:05.640003920 CEST	49992	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:05.688662052 CEST	53	49992	8.8.8.8	192.168.2.5
May 4, 2021 19:58:05.923970938 CEST	60075	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:05.984836102 CEST	53	60075	8.8.8.8	192.168.2.5
May 4, 2021 19:58:06.104861021 CEST	55016	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:06.165692091 CEST	53	55016	8.8.8.8	192.168.2.5
May 4, 2021 19:58:06.229470968 CEST	64345	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:06.287605047 CEST	53	64345	8.8.8.8	192.168.2.5
May 4, 2021 19:58:06.422621965 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:06.483633041 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 19:58:06.935664892 CEST	54791	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:06.992909908 CEST	53	54791	8.8.8.8	192.168.2.5
May 4, 2021 19:58:07.238526106 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:07.299071074 CEST	53	50463	8.8.8.8	192.168.2.5
May 4, 2021 19:58:08.082194090 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:08.146444082 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 19:58:08.535706043 CEST	57344	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:08.538836002 CEST	54450	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:08.595817089 CEST	53	57344	8.8.8.8	192.168.2.5
May 4, 2021 19:58:08.604020119 CEST	53	54450	8.8.8.8	192.168.2.5
May 4, 2021 19:58:09.831655979 CEST	59261	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:09.833849907 CEST	57151	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:09.894503117 CEST	53	57151	8.8.8.8	192.168.2.5
May 4, 2021 19:58:09.899532080 CEST	53	59261	8.8.8.8	192.168.2.5
May 4, 2021 19:58:10.907677889 CEST	59413	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:10.958286047 CEST	53	59413	8.8.8.8	192.168.2.5
May 4, 2021 19:58:11.029644012 CEST	60516	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:11.035439968 CEST	51649	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:11.088042021 CEST	53	60516	8.8.8.8	192.168.2.5
May 4, 2021 19:58:11.100893021 CEST	53	51649	8.8.8.8	192.168.2.5
May 4, 2021 19:58:12.096960068 CEST	52929	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:12.147624969 CEST	53	52929	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:58:16.416390896 CEST	61004	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:16.466298103 CEST	53	61004	8.8.8.8	192.168.2.5
May 4, 2021 19:58:17.578094959 CEST	56895	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:17.631582975 CEST	53	56895	8.8.8.8	192.168.2.5
May 4, 2021 19:58:18.092778921 CEST	62372	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:18.152647018 CEST	53	62372	8.8.8.8	192.168.2.5
May 4, 2021 19:58:18.521040916 CEST	61515	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:18.579607010 CEST	53	61515	8.8.8.8	192.168.2.5
May 4, 2021 19:58:18.825511932 CEST	56675	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:18.859819889 CEST	57172	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:18.891694069 CEST	53	56675	8.8.8.8	192.168.2.5
May 4, 2021 19:58:18.909553051 CEST	53	57172	8.8.8.8	192.168.2.5
May 4, 2021 19:58:19.808794022 CEST	55267	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:19.808865070 CEST	50969	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:19.813520908 CEST	64362	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:19.814378977 CEST	54766	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:19.862503052 CEST	53	64362	8.8.8.8	192.168.2.5
May 4, 2021 19:58:19.867018938 CEST	53	55267	8.8.8.8	192.168.2.5
May 4, 2021 19:58:19.868964911 CEST	53	50969	8.8.8.8	192.168.2.5
May 4, 2021 19:58:19.876194000 CEST	53	54766	8.8.8.8	192.168.2.5
May 4, 2021 19:58:20.204222918 CEST	61446	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:20.262847900 CEST	53	61446	8.8.8.8	192.168.2.5
May 4, 2021 19:58:20.595036983 CEST	57515	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:20.652297974 CEST	53	57515	8.8.8.8	192.168.2.5
May 4, 2021 19:58:20.659662008 CEST	58199	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:20.708355904 CEST	53	58199	8.8.8.8	192.168.2.5
May 4, 2021 19:58:23.370300055 CEST	65221	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:23.371669054 CEST	61573	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:23.378405094 CEST	56562	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:23.431828976 CEST	53	65221	8.8.8.8	192.168.2.5
May 4, 2021 19:58:23.441555023 CEST	53	56562	8.8.8.8	192.168.2.5
May 4, 2021 19:58:23.458292007 CEST	53	61573	8.8.8.8	192.168.2.5
May 4, 2021 19:58:23.471261978 CEST	53591	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:23.521636963 CEST	53	53591	8.8.8.8	192.168.2.5
May 4, 2021 19:58:24.788321018 CEST	59688	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:24.848807096 CEST	53	59688	8.8.8.8	192.168.2.5
May 4, 2021 19:58:25.094299078 CEST	56032	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:25.153497934 CEST	53	56032	8.8.8.8	192.168.2.5
May 4, 2021 19:58:25.689374924 CEST	61150	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:25.750926018 CEST	53	61150	8.8.8.8	192.168.2.5
May 4, 2021 19:58:26.403817892 CEST	63458	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:26.453344107 CEST	53	63458	8.8.8.8	192.168.2.5
May 4, 2021 19:58:27.439894915 CEST	50422	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:27.501265049 CEST	53	50422	8.8.8.8	192.168.2.5
May 4, 2021 19:58:38.312638998 CEST	53247	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:38.384459019 CEST	53	53247	8.8.8.8	192.168.2.5
May 4, 2021 19:58:40.201464891 CEST	58544	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:40.252995968 CEST	53	58544	8.8.8.8	192.168.2.5
May 4, 2021 19:58:48.522587061 CEST	51305	53	192.168.2.5	8.8.8.8
May 4, 2021 19:58:48.573553085 CEST	53	51305	8.8.8.8	192.168.2.5
May 4, 2021 19:59:01.740093946 CEST	53670	53	192.168.2.5	8.8.8.8
May 4, 2021 19:59:01.805172920 CEST	53	53670	8.8.8.8	192.168.2.5
May 4, 2021 19:59:02.463128090 CEST	61414	53	192.168.2.5	8.8.8.8
May 4, 2021 19:59:02.520473957 CEST	53	61414	8.8.8.8	192.168.2.5
May 4, 2021 19:59:02.642467022 CEST	63847	53	192.168.2.5	8.8.8.8
May 4, 2021 19:59:02.700001001 CEST	53	63847	8.8.8.8	192.168.2.5
May 4, 2021 19:59:02.848979950 CEST	61523	53	192.168.2.5	8.8.8.8
May 4, 2021 19:59:02.870873928 CEST	50551	53	192.168.2.5	8.8.8.8
May 4, 2021 19:59:02.906244040 CEST	53	61523	8.8.8.8	192.168.2.5
May 4, 2021 19:59:02.922346115 CEST	53	50551	8.8.8.8	192.168.2.5
May 4, 2021 19:59:34.111673117 CEST	62847	53	192.168.2.5	8.8.8.8
May 4, 2021 19:59:34.162790060 CEST	53	62847	8.8.8.8	192.168.2.5
May 4, 2021 19:59:43.942996025 CEST	57712	53	192.168.2.5	8.8.8.8
May 4, 2021 19:59:44.008671045 CEST	53	57712	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:59:44.175081968 CEST	61064	53	192.168.2.5	8.8.8.8
May 4, 2021 19:59:44.223762989 CEST	53	61064	8.8.8.8	192.168.2.5
May 4, 2021 19:59:45.138119936 CEST	61891	53	192.168.2.5	8.8.8.8
May 4, 2021 19:59:45.196934938 CEST	53	61891	8.8.8.8	192.168.2.5
May 4, 2021 20:00:09.815442085 CEST	61585	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:09.881057024 CEST	53	61585	8.8.8.8	192.168.2.5
May 4, 2021 20:00:13.034563065 CEST	65163	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:13.066395998 CEST	58969	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:13.100459099 CEST	53	65163	8.8.8.8	192.168.2.5
May 4, 2021 20:00:13.128741980 CEST	53	58969	8.8.8.8	192.168.2.5
May 4, 2021 20:00:13.244867086 CEST	53977	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:13.293607950 CEST	53	53977	8.8.8.8	192.168.2.5
May 4, 2021 20:00:26.033425093 CEST	57147	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:26.104652882 CEST	53	57147	8.8.8.8	192.168.2.5
May 4, 2021 20:00:28.445039034 CEST	52381	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:28.504301071 CEST	53	52381	8.8.8.8	192.168.2.5
May 4, 2021 20:00:39.889164925 CEST	49231	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:39.950972080 CEST	53	49231	8.8.8.8	192.168.2.5
May 4, 2021 20:00:40.600815058 CEST	53217	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:40.661916971 CEST	53	53217	8.8.8.8	192.168.2.5
May 4, 2021 20:00:41.226511955 CEST	52554	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:41.365565062 CEST	53	52554	8.8.8.8	192.168.2.5
May 4, 2021 20:00:41.795389891 CEST	49603	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:41.855396986 CEST	53	49603	8.8.8.8	192.168.2.5
May 4, 2021 20:00:42.411045074 CEST	64476	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:42.460021973 CEST	53	64476	8.8.8.8	192.168.2.5
May 4, 2021 20:00:43.377372026 CEST	49975	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:43.427515030 CEST	53	49975	8.8.8.8	192.168.2.5
May 4, 2021 20:00:44.231189966 CEST	57701	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:44.291028976 CEST	53	57701	8.8.8.8	192.168.2.5
May 4, 2021 20:00:45.105926037 CEST	60334	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:45.163045883 CEST	53	60334	8.8.8.8	192.168.2.5
May 4, 2021 20:00:48.738329887 CEST	64958	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:48.791620970 CEST	53	64958	8.8.8.8	192.168.2.5
May 4, 2021 20:00:49.269808054 CEST	58504	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:49.327389002 CEST	53	58504	8.8.8.8	192.168.2.5
May 4, 2021 20:00:52.094105005 CEST	64971	53	192.168.2.5	8.8.8.8
May 4, 2021 20:00:52.142719984 CEST	53	64971	8.8.8.8	192.168.2.5
May 4, 2021 20:01:00.974759102 CEST	58041	53	192.168.2.5	8.8.8.8
May 4, 2021 20:01:01.032089949 CEST	53	58041	8.8.8.8	192.168.2.5
May 4, 2021 20:01:19.866734028 CEST	57764	53	192.168.2.5	8.8.8.8
May 4, 2021 20:01:19.936726093 CEST	53	57764	8.8.8.8	192.168.2.5
May 4, 2021 20:01:20.074657917 CEST	57973	53	192.168.2.5	8.8.8.8
May 4, 2021 20:01:20.134001017 CEST	53	57973	8.8.8.8	192.168.2.5
May 4, 2021 20:01:34.357065916 CEST	63286	53	192.168.2.5	8.8.8.8
May 4, 2021 20:01:34.414170027 CEST	53	63286	8.8.8.8	192.168.2.5
May 4, 2021 20:01:34.447459936 CEST	54875	53	192.168.2.5	8.8.8.8
May 4, 2021 20:01:34.518305063 CEST	53	54875	8.8.8.8	192.168.2.5
May 4, 2021 20:01:34.660295010 CEST	49862	53	192.168.2.5	8.8.8.8
May 4, 2021 20:01:34.727643013 CEST	53	49862	8.8.8.8	192.168.2.5
May 4, 2021 20:01:42.626220942 CEST	50119	53	192.168.2.5	8.8.8.8
May 4, 2021 20:01:42.693659067 CEST	53	50119	8.8.8.8	192.168.2.5
May 4, 2021 20:01:42.832545042 CEST	60159	53	192.168.2.5	8.8.8.8
May 4, 2021 20:01:42.890000105 CEST	53	60159	8.8.8.8	192.168.2.5
May 4, 2021 20:02:07.800952911 CEST	49464	53	192.168.2.5	8.8.8.8
May 4, 2021 20:02:07.874074936 CEST	53	49464	8.8.8.8	192.168.2.5
May 4, 2021 20:02:08.020525932 CEST	64650	53	192.168.2.5	8.8.8.8
May 4, 2021 20:02:08.078047991 CEST	53	64650	8.8.8.8	192.168.2.5
May 4, 2021 20:02:13.217659950 CEST	52633	53	192.168.2.5	8.8.8.8
May 4, 2021 20:02:13.266197920 CEST	53	52633	8.8.8.8	192.168.2.5
May 4, 2021 20:02:29.713059902 CEST	56124	53	192.168.2.5	8.8.8.8
May 4, 2021 20:02:29.773000956 CEST	53	56124	8.8.8.8	192.168.2.5
May 4, 2021 20:02:47.591795921 CEST	55552	53	192.168.2.5	8.8.8.8
May 4, 2021 20:02:47.643362999 CEST	53	55552	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:03:02.070738077 CEST	60813	53	192.168.2.5	8.8.8.8
May 4, 2021 20:03:02.132055044 CEST	53	60813	8.8.8.8	192.168.2.5
May 4, 2021 20:03:06.111313105 CEST	50930	53	192.168.2.5	8.8.8.8
May 4, 2021 20:03:06.174993038 CEST	53	50930	8.8.8.8	192.168.2.5
May 4, 2021 20:03:06.480741024 CEST	51582	53	192.168.2.5	8.8.8.8
May 4, 2021 20:03:06.538043976 CEST	53	51582	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 19:58:04.032215118 CEST	192.168.2.5	8.8.8.8	0x9f1b	Standard query (0)	jgauozxiisaozxs-cheerful-impala-ms.us-so uth.cf.app domain.cloud	A (IP address)	IN (0x0001)
May 4, 2021 19:58:05.510960102 CEST	192.168.2.5	8.8.8.8	0xf8a1	Standard query (0)	vzas.aioecoin.org	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.104861021 CEST	192.168.2.5	8.8.8.8	0x580	Standard query (0)	kamppcnddemoiz.web.app	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.229470968 CEST	192.168.2.5	8.8.8.8	0x8295	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.422621965 CEST	192.168.2.5	8.8.8.8	0x5d98	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.935664892 CEST	192.168.2.5	8.8.8.8	0x8cd	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 4, 2021 19:58:08.535706043 CEST	192.168.2.5	8.8.8.8	0x9d18	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
May 4, 2021 19:58:08.538836002 CEST	192.168.2.5	8.8.8.8	0x88b0	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
May 4, 2021 19:58:09.833849907 CEST	192.168.2.5	8.8.8.8	0xaf30	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
May 4, 2021 19:58:10.907677889 CEST	192.168.2.5	8.8.8.8	0x577e	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
May 4, 2021 19:58:11.029644012 CEST	192.168.2.5	8.8.8.8	0x74eb	Standard query (0)	kamppcnddemoiz.web.app	A (IP address)	IN (0x0001)
May 4, 2021 19:58:11.035439968 CEST	192.168.2.5	8.8.8.8	0xd398	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
May 4, 2021 19:58:16.416390896 CEST	192.168.2.5	8.8.8.8	0xbec6	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
May 4, 2021 19:58:19.814378977 CEST	192.168.2.5	8.8.8.8	0x5ec	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 19:58:25.689374924 CEST	192.168.2.5	8.8.8.8	0xa7b5	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
May 4, 2021 19:58:38.312638998 CEST	192.168.2.5	8.8.8.8	0x52db	Standard query (0)	consentreceiverfd-prod.azurefd.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 19:58:04.105186939 CEST	8.8.8.8	192.168.2.5	0x9f1b	No error (0)	jgauozxiisaozxs-cheerful-impala-ms.us-so uth.cf.app domain.cloud		169.62.254.82	A (IP address)	IN (0x0001)
May 4, 2021 19:58:04.105186939 CEST	8.8.8.8	192.168.2.5	0x9f1b	No error (0)	jgauozxiisaozxs-cheerful-impala-ms.us-so uth.cf.app domain.cloud		169.46.89.154	A (IP address)	IN (0x0001)
May 4, 2021 19:58:04.105186939 CEST	8.8.8.8	192.168.2.5	0x9f1b	No error (0)	jgauozxiisaozxs-cheerful-impala-ms.us-so uth.cf.app domain.cloud		169.47.124.25	A (IP address)	IN (0x0001)
May 4, 2021 19:58:05.609563112 CEST	8.8.8.8	192.168.2.5	0xf8a1	No error (0)	vzas.aioecoin.org		104.21.91.175	A (IP address)	IN (0x0001)
May 4, 2021 19:58:05.609563112 CEST	8.8.8.8	192.168.2.5	0xf8a1	No error (0)	vzas.aioecoin.org		172.67.176.224	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 19:58:06.165692091 CEST	8.8.8.8	192.168.2.5	0x580	No error (0)	kamppcnddemoiz.web.app		151.101.1.195	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.165692091 CEST	8.8.8.8	192.168.2.5	0x580	No error (0)	kamppcnddemoiz.web.app		151.101.65.195	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.287605047 CEST	8.8.8.8	192.168.2.5	0x8295	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:58:06.287605047 CEST	8.8.8.8	192.168.2.5	0x8295	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.483633041 CEST	8.8.8.8	192.168.2.5	0x5d98	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.483633041 CEST	8.8.8.8	192.168.2.5	0x5d98	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.483633041 CEST	8.8.8.8	192.168.2.5	0x5d98	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.483633041 CEST	8.8.8.8	192.168.2.5	0x5d98	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.483633041 CEST	8.8.8.8	192.168.2.5	0x5d98	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.992909908 CEST	8.8.8.8	192.168.2.5	0x8cd	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 4, 2021 19:58:06.992909908 CEST	8.8.8.8	192.168.2.5	0x8cd	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 4, 2021 19:58:08.595817089 CEST	8.8.8.8	192.168.2.5	0x9d18	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:58:08.595817089 CEST	8.8.8.8	192.168.2.5	0x9d18	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
May 4, 2021 19:58:08.604020119 CEST	8.8.8.8	192.168.2.5	0x88b0	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:58:09.894503117 CEST	8.8.8.8	192.168.2.5	0xaf30	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:58:10.958286047 CEST	8.8.8.8	192.168.2.5	0x577e	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:58:11.088042021 CEST	8.8.8.8	192.168.2.5	0x74eb	No error (0)	kamppcnddemoiz.web.app		151.101.1.195	A (IP address)	IN (0x0001)
May 4, 2021 19:58:11.088042021 CEST	8.8.8.8	192.168.2.5	0x74eb	No error (0)	kamppcnddemoiz.web.app		151.101.65.195	A (IP address)	IN (0x0001)
May 4, 2021 19:58:11.100893021 CEST	8.8.8.8	192.168.2.5	0xd398	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:58:11.100893021 CEST	8.8.8.8	192.168.2.5	0xd398	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
May 4, 2021 19:58:16.466298103 CEST	8.8.8.8	192.168.2.5	0xbec6	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
May 4, 2021 19:58:16.466298103 CEST	8.8.8.8	192.168.2.5	0xbec6	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
May 4, 2021 19:58:18.152647018 CEST	8.8.8.8	192.168.2.5	0x143f	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:58:19.862503052 CEST	8.8.8.8	192.168.2.5	0xab5c	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:58:19.876194000 CEST	8.8.8.8	192.168.2.5	0x5ec	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:58:25.750926018 CEST	8.8.8.8	192.168.2.5	0xa7b5	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 19:58:38.384459019 CEST	8.8.8.8	192.168.2.5	0x52db	No error (0)	consentrec eiverfd-pr od.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 19:58:04.572405100 CEST	169.62.254.82	443	192.168.2.5	49709	CN=*.us-south.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
May 4, 2021 19:58:04.576129913 CEST	169.62.254.82	443	192.168.2.5	49708	CN=*.us-south.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
May 4, 2021 19:58:04.614618063 CEST	169.62.254.82	443	192.168.2.5	49710	CN=*.us-south.cf.appdomain.cloud, OU=IBM Cloud, O=International Business Machines Corporation, L=Armonk, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 27 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Sep 01 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
May 4, 2021 19:58:11.205343962 CEST	152.199.23.37	443	192.168.2.5	49742	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 19:58:11.208992958 CEST	151.101.1.195	443	192.168.2.5	49740	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		
May 4, 2021 19:58:11.210835934 CEST	151.101.1.195	443	192.168.2.5	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		
May 4, 2021 19:58:14.733496904 CEST	152.199.23.37	443	192.168.2.5	49753	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 2200 Parent PID: 4672

General

Start time:	19:58:00
Start date:	04/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\PaymentAdvice - Copy.htm'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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: 6196 Parent PID: 2200

General

Start time:	19:58:01
Start date:	04/05/2021
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=1572,7685515081326957322,28580 13151591642698,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1688 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly