ID: 458904
Sample Name: Project Proposal and Analysis.html
Cookbook: default.jbs
Time: 21:03:42
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

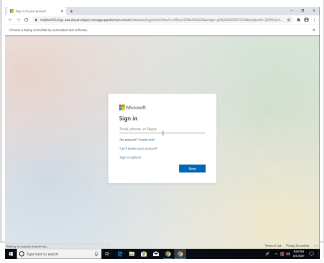
Windows Analysis Report Project Proposal and Analysi…

Overview

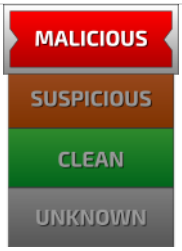
General Information

Sample Name:	Project Proposal and Analysis.html
Analysis ID:	458904
MD5:	acb86ccd1bb408…
SHA1:	f2db12da0432d93.
SHA256:	b452a456c1db4a..
Infos:	

Most interesting Screenshot:



Detection



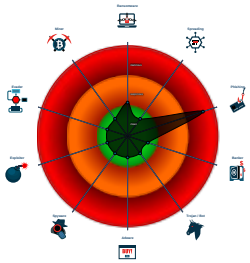
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- HTML document with suspicious title
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- No HTML title found
- Submit button contains javascript call

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5996 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\Project Proposal and Analysis.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5424 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,17296826692838302678,18007796765270658976,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1664 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

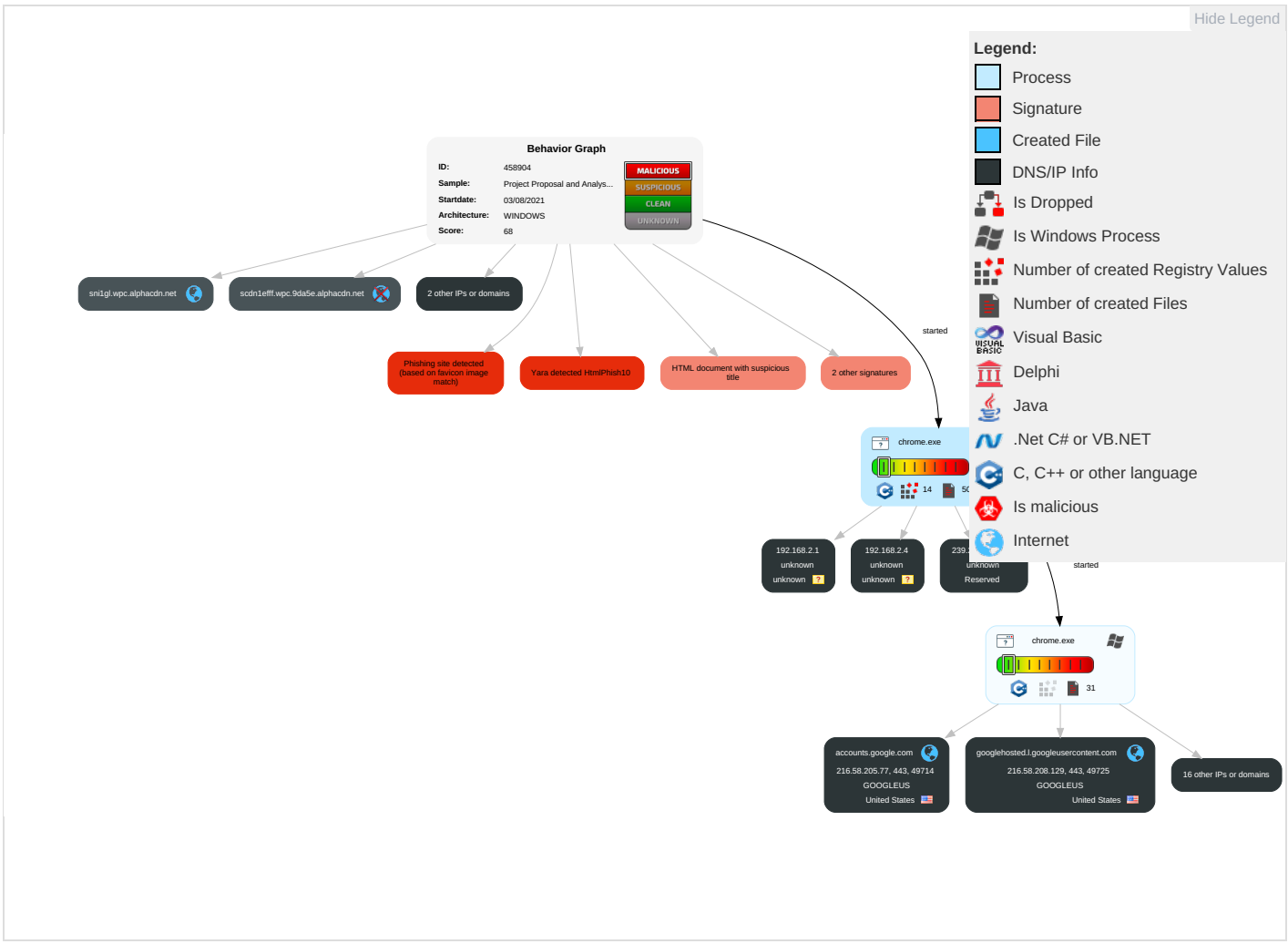
System Summary:

HTML document with suspicious title

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	Scripting 1	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 Partition
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)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

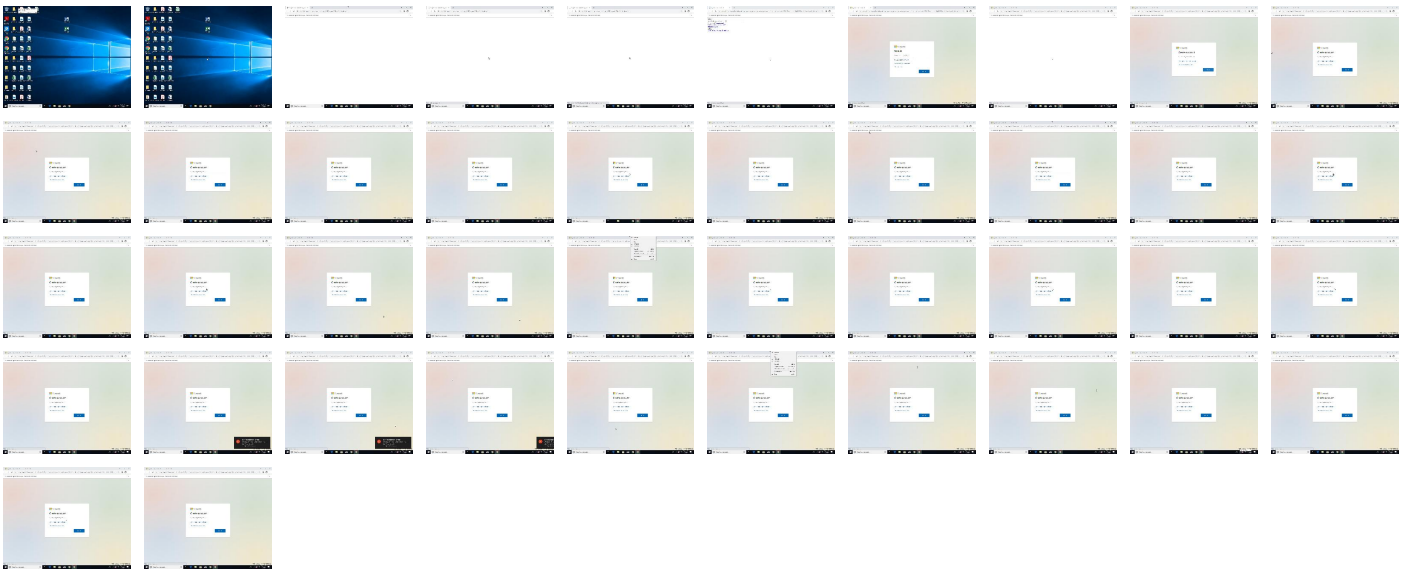
Behavior Graph

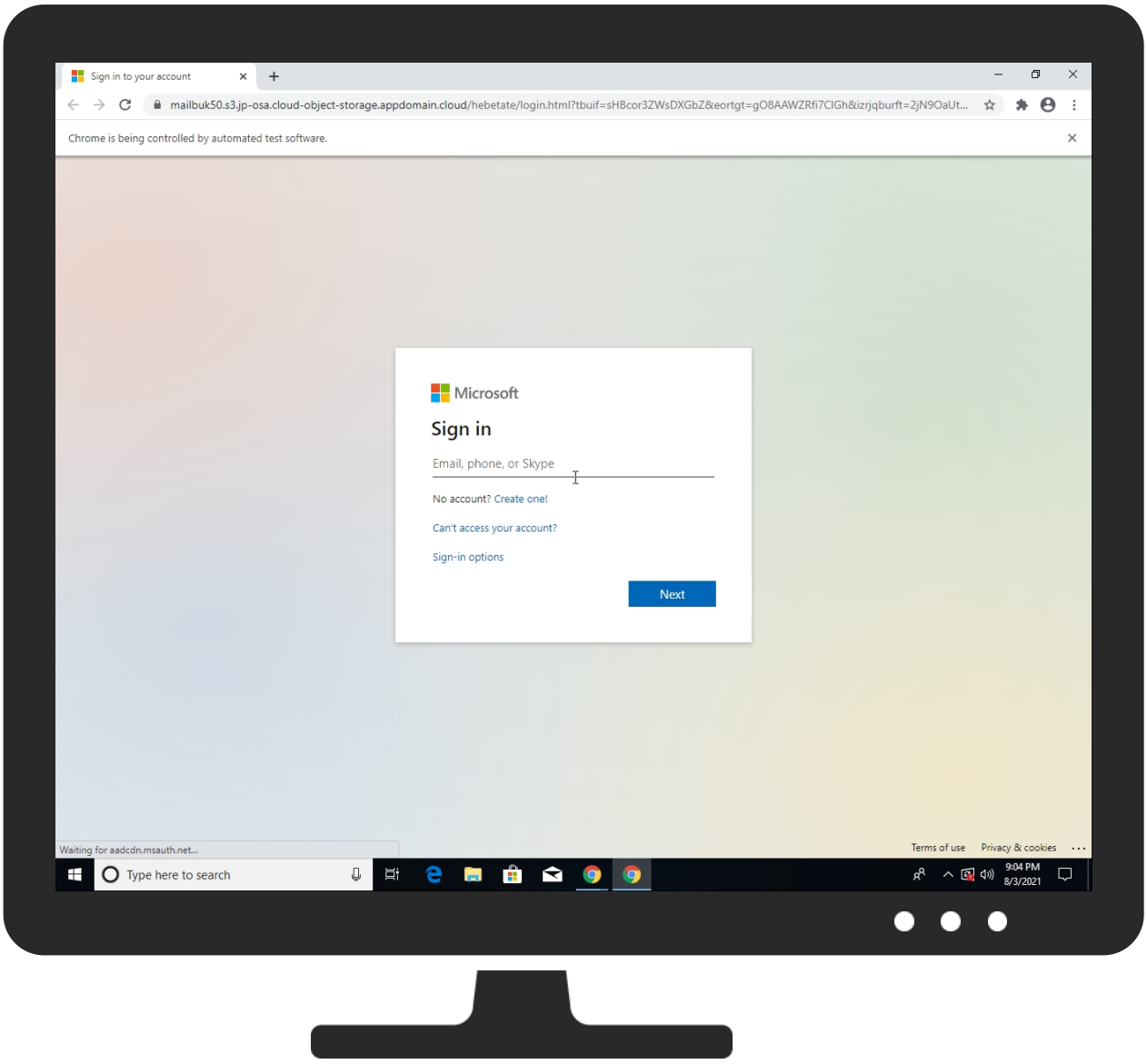


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sni1gl.wpc.alphacdn.net	0%	Virustotal		Browse
s3.jp-osa.cloud-object-storage.appdomain.cloud	5%	Virustotal		Browse
aadcdn.msauth.net	2%	Virustotal		Browse
acctcdn.msauth.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msauth.net/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://acctcdn.msauth.net/lightweightsignuppackage_2AvLXlM9Do2tIgiv0FDCDg2.js?v=1	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js	0%	URL Reputation	safe	
http://https://mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud/hebetate/index.html	0%	Avira URL Cloud	safe	
http://https://mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud/hebetate/index.html5	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud/	0%	Avira URL Cloud	safe	
http://https://mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud/hebetate/login.html?tbuif=sHBcor3ZW	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/	0%	URL Reputation	safe	
http://https://mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud/hebetate/index.htmlSign	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	0%	URL Reputation	safe	
http://https://mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud	0%	Avira URL Cloud	safe	
http://https://mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud/hebetate/index.htmlP	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_Hu9XQvsxbdtI5Cn8ywiXCA2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	0%	URL Reputation	safe	
http://https://appdomain.cloud/	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.205.77	true	false		high
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	216.58.208.174	true	false		high
s3.jp-osa.cloud-object-storage.appdomain.cloud	163.68.118.49	true	false	• 5%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
signup.live.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud	unknown	unknown	false		unknown
aadcdn.msauth.net	unknown	unknown	false	• 2%, Virustotal, Browse	unknown
fpt.live.com	unknown	unknown	false		high
acctcdn.msauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
acctcdn.msftauth.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud/hebetate/login.html?tbuif=sHBcor3ZWsDXGbZ&eortgt=gO8AAWZRfi7ClGh&izrjqburft=2jN9OaUtQbOToDiD2&welygot=BSnCu4Pw8wRPJF9qJXebOTu3bF3hjV&axhrm=vYn7eCukD52W8boRtlM7yT8&floywhix=2pHOlZLUuTVAcbQ7El9YY&ajm=t3pKqCucGSJH2hNfMr9aVBP5CWa&gid=ToojiO2cjpBvMOP1h7S	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
163.68.118.49	s3.jp-osa.cloud-object-storage.appdomain.cloud	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
152.199.21.175	sni1gl.wpc.alphacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.1
192.168.2.4
192.168.2.255
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458904
Start date:	03.08.2021
Start time:	21:03:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Project Proposal and Analysis.html
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:	29
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:	mal68.phis.winHTML@41/252@11/10
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html • Browse: https://login.live.com/oauth20_authorize.srf?response_type=code&client_id=51483342-085c-4d86-bf88-cf50c7252078&scope=openid+profile+email+offline_access&response_mode=form_post&redirect_uri=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2ffederation%2foauth2&state=rQIIAYWSO2_TUABG47QNtOItBsSAOjAgkNPre_2IIyHhxEmTJo7zsOvYi2UnfuVhp44dOxETLAxIMHeDASFgQiAhJuZKSGwgFlbEhBADGxT-AMsZvjN-Z-sEnafzIA-urxF5oniVRCRlMCaLswaNcJIlAG6QkMYRhWgEATGkAAovbJ3r3Ln3-vaNj7ful35-enD594tDbFOfeAsrPwimz7ArbhTN5sWdnSRJ8oFte4N_Ymdi-EPPd95g2AcM-4phh9kNy8fl3rPsnEYMoliaoQjAQAhZAPOaJKQqFBJR4iJ1KhCaB4CqqGlTqRxv9UjY7U4E2IHirjbV-EEiKDJqKfVUU4RIHe176hIAUVGXTclJRd6JBF6AmqQSrdE4EVZ19Dl7VuTiyIV_EYTeyvqR3bSDcKrPgnl0uPY8u-rOO6bqr6yewFMsQxpdvxFynE60XbO7X476HjoQpm7VWUbGEmdDhtGjJVUd9GtKXA_50N3nwiBI-0bS7uEHtNlolFtjRE8WNrk7phdWrU3ynGkoiRn4U9mMyWadcZqGw1eVAy2lR31aTkVN1r1-OeCFg2QRJAnpkIzKOMG8AyaVVVreowg9xR2Zr01hEzfnfBssxwHuV0BvIboDJwVwUGuMQ8ZxZcEsN1m9MEQFX5NGQ6XJeWy1W2qD0mxhU4G9VyposYuq3WTVUHflhSXLZivq-a4y5-KJgNdQFDsMO7SYZm1UsyS0KnE62ZMKtPNyLXf88DTwj9bOBDPL94bbszCwvYn1YR37tn7qZO5c7lJmO3PtIjjzax17vHEc0dP3XzbY5ZPy3UekHcmvMkcbOyq_Qou-VQFSTE3SAjKBMqLL7mxPrcRLUYyHHdZGzn4dAO4mUSQe5rCHudxR7nyd11sVqSdxLZ7r8lAH33PYvROZt5v_SfHz1kUIIMABixPMNgRFgihSQHt3OvMH0&estsfed=1&uaid=b58882512b7c40d78c42f4d88f1affac&signup=1&lw=1&fl=easi2&fci=4345a7b9-9a63-4910-a426-35363201d503&mkt=en-US
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
239.255.255.250	Dosusign_Na_Sign.htm	Get hash	malicious	Browse	
	sbcss_Richard.DeNava_#inv0549387TWQYqzTP aYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	Get hash	malicious	Browse	
	Fake.HTM	Get hash	malicious	Browse	
	6dAzFehHE6.doc	Get hash	malicious	Browse	
	vcufsCgeP2.doc	Get hash	malicious	Browse	
	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm	Get hash	malicious	Browse	
	ATT66004.HTM	Get hash	malicious	Browse	
	0803_0212424605.doc	Get hash	malicious	Browse	
	psconstruction.ca Attachment.htm	Get hash	malicious	Browse	
	minha-conta-06082021.msi	Get hash	malicious	Browse	
	BadFile.HTM	Get hash	malicious	Browse	
	OneDrive-besked.htm	Get hash	malicious	Browse	
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	
	Xerox Scan_367136092111.html	Get hash	malicious	Browse	
	_vm000_294943583.HtM	Get hash	malicious	Browse	
	QlOyDcDypy.exe	Get hash	malicious	Browse	
	ATT17444.HTM	Get hash	malicious	Browse	
	ATT75446.HTM	Get hash	malicious	Browse	
	ATT23582.HTM	Get hash	malicious	Browse	
152.199.21.175	yx8DBT3r5r.exe	Get hash	malicious	Browse	• www.mobilityconsignment.com/W4C1yQ.php?m=xl59elj25q8m
	http://https://u.to/r9nvGQ	Get hash	malicious	Browse	• s.c.dk/fonts/yousee-iconfont.woff
	http://cdn2.driversupport.com/dsone/gppc_ds1/DSOne.exe	Get hash	malicious	Browse	• cdn2.driversupport.com/dsone/gppc_ds1/DSOneApp.exe
	http://cdn2.driversupport.com/dsone/gdn_ds1/DSOne.exe	Get hash	malicious	Browse	• cdn2.driversupport.com/dsone/gdn_ds1/DSOneApp.exe
163.68.118.49	Audio Message.html	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sni1gl.wpc.alphacdn.net	OneDrive-besked.htm	Get hash	malicious	Browse	• 152.199.21.175
	AUTORIZAR_ITEM3884795BR.msi	Get hash	malicious	Browse	• 152.199.21.175
	minha-conta-06082021.msi	Get hash	malicious	Browse	• 152.199.21.175
	bl.51676685_61299322_95868579.pdf.msi	Get hash	malicious	Browse	• 152.199.21.175
	ATT22486.htm	Get hash	malicious	Browse	• 152.199.21.175
	ATT07001.htm	Get hash	malicious	Browse	• 152.199.21.175
	ATT26728(1).htm	Get hash	malicious	Browse	• 152.199.21.175
	.htm.htm	Get hash	malicious	Browse	• 152.199.21.175

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	.htm.htm	Get hash	malicious	Browse	• 152.199.21.175
	ATT96756.htm	Get hash	malicious	Browse	• 152.199.21.175
	Prosserhealth.html	Get hash	malicious	Browse	• 152.199.21.175
	DCBR.msi	Get hash	malicious	Browse	• 152.199.21.175
	#U00e2_#U00e2_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.21.175
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.21.175
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.21.175
	banload.msi	Get hash	malicious	Browse	• 152.199.21.175
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.21.175
	Globalfoundries.htm	Get hash	malicious	Browse	• 152.199.21.175
	INV_289553.html	Get hash	malicious	Browse	• 152.199.21.175
	Voice0033pm.htm	Get hash	malicious	Browse	• 152.199.21.175

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	AEOjFHGJAr	Get hash	malicious	Browse	• 27.36.92.105
	EKH4PZIAwO	Get hash	malicious	Browse	• 163.82.163.173
	z4zrCaJCJg	Get hash	malicious	Browse	• 163.4.170.49
	557IyF5NeE	Get hash	malicious	Browse	• 112.93.141.65
	FTFGYpE43O	Get hash	malicious	Browse	• 163.106.10.218
	l0TgMeBzkj	Get hash	malicious	Browse	• 163.179.54.167
	oqG1fmow77	Get hash	malicious	Browse	• 101.233.214.223
	ZXuptcXTmx	Get hash	malicious	Browse	• 163.95.33.126
	NhqS8NmjUh	Get hash	malicious	Browse	• 163.112.118.177
	qBkJfZZTh3	Get hash	malicious	Browse	• 163.110.186.254
	r00dCFKSa4	Get hash	malicious	Browse	• 163.106.22.20
	Kot8HtIH3m	Get hash	malicious	Browse	• 163.92.96.138
	2iZFiz8mkB	Get hash	malicious	Browse	• 119.43.71.210
	arm7	Get hash	malicious	Browse	• 163.67.217.42
	oRXNEf9CXn	Get hash	malicious	Browse	• 163.84.64.202
	8xVa4UKUer	Get hash	malicious	Browse	• 163.81.44.145
	U9ZCIleOAC	Get hash	malicious	Browse	• 163.98.149.250
	nFXksLiE0m	Get hash	malicious	Browse	• 163.97.135.58
	DO3yEscfl8	Get hash	malicious	Browse	• 157.148.165.59
	N3pBzXZZne	Get hash	malicious	Browse	• 163.67.217.45
EDGECASTUS	Dosusign_Na_Sign.htm	Get hash	malicious	Browse	• 93.184.220.66
	Fake.HTM	Get hash	malicious	Browse	• 152.199.23.72
	minha-conta-06082021.msi	Get hash	malicious	Browse	• 192.229.221.185
	OneDrive-besked.htm	Get hash	malicious	Browse	• 152.199.23.37
	phish.html	Get hash	malicious	Browse	• 152.199.23.37
	HTM.html	Get hash	malicious	Browse	• 152.199.23.72
	minha-conta-06082021.msi	Get hash	malicious	Browse	• 192.229.221.185
	AUTORIZAR_ITEM3884795BR.msi	Get hash	malicious	Browse	• 152.199.21.175
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 93.184.221.240
	minha-conta-06082021.msi	Get hash	malicious	Browse	• 192.229.221.185
	minha-conta-06082021.msi	Get hash	malicious	Browse	• 152.199.21.175
	Medius.html	Get hash	malicious	Browse	• 152.199.23.37
	Aging invoice.html	Get hash	malicious	Browse	• 152.199.23.37
	LM6QUd7sMJ.exe	Get hash	malicious	Browse	• 93.184.220.29
	bl.51676685_61299322_95868579.pdf.msi	Get hash	malicious	Browse	• 152.199.21.175
	globalfoundries_MNT484_XEROStubs_XjJzNZsjSWLmtRAHrKczAOlwztYjTcVMspUZaJnMJERgMTdevl.HTML	Get hash	malicious	Browse	• 152.199.23.37
	It.servicedesk-it.servicedesk@ovolohotels.com.html	Get hash	malicious	Browse	• 152.199.23.37
	MIN56KgzBN.exe	Get hash	malicious	Browse	• 93.184.221.240
	ATT22486.htm	Get hash	malicious	Browse	• 152.199.21.175
	ATT07001.htm	Get hash	malicious	Browse	• 152.199.21.175

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Fake.HTM	Get hash	malicious	Browse	• 152.199.21.175
	Ban.exe	Get hash	malicious	Browse	• 152.199.21.175
	TpZ10Hfjov.exe	Get hash	malicious	Browse	• 152.199.21.175
	ATT66004.HTM	Get hash	malicious	Browse	• 152.199.21.175
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 152.199.21.175
	OneDrive-besked.htm	Get hash	malicious	Browse	• 152.199.21.175
	PdQwZoWgs2.ppt	Get hash	malicious	Browse	• 152.199.21.175
	Wyzntjzprmmvqdtdrthurezrzhdavabchs.exe	Get hash	malicious	Browse	• 152.199.21.175
	Wyzntjzprmmvqdtdrthurezrzhdavabchs.exe	Get hash	malicious	Browse	• 152.199.21.175
	1As0Ink4Td.exe	Get hash	malicious	Browse	• 152.199.21.175
	9HEOWXnwTj.exe	Get hash	malicious	Browse	• 152.199.21.175
	SzjLrAw2pL.exe	Get hash	malicious	Browse	• 152.199.21.175
	8dll.dll	Get hash	malicious	Browse	• 152.199.21.175
	8dll.exe	Get hash	malicious	Browse	• 152.199.21.175
	j4OPkAytMi.exe	Get hash	malicious	Browse	• 152.199.21.175
	Tzcyxxestkakhuvtmvfdserywturrfjrye.exe	Get hash	malicious	Browse	• 152.199.21.175
	Xerox Scan_367136092111.html	Get hash	malicious	Browse	• 152.199.21.175
	mal.docx	Get hash	malicious	Browse	• 152.199.21.175
	ATT75446.HTM	Get hash	malicious	Browse	• 152.199.21.175
	ATT23582.HTM	Get hash	malicious	Browse	• 152.199.21.175

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	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\Local\Google\Chrome\User Data\072bd3ae-c1ab-4d57-afa1-57ad110c0b4d.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):	166478
Entropy (8bit):	6.050818154377323
Encrypted:	false
SSDEEP:	3072:SGaYTJQE+mugy9+QV1T7IRwdfLSNPVLA7bV/nYorVcI8XIssElYTRe:HxaV+QfT7GSmhVgbV/njhcI8II6Re
MD5:	898D47DE930DEFADF5970DE6AF5AA795
SHA1:	CD83273F5ACAC6B668CCE8B34FA6ABC212DA52F4
SHA-256:	CFECFF11B9F102A4179CFC7C0315B19228BA46CFA04C178852B38424D91A9C98

C:\Users\user\AppData\Local\Google\Chrome\User Data\072bd3ae-c1ab-4d57-afa1-57ad110c0b4d.tmp	
SHA-512:	B23D969453FB08AD52E63C485860D22D1AFDC97EEB3D49C9E0D5EA024BFB1B9CF2C6ADAE62108E37FC95933A64B48A6B35940443307E876AC3E1E690800FDF 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":1.62804988194663e+12,"network":1.628017484e+12,"ticks":5998863256.0,"uncertainty":5260958.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAAB BmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN 50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqk TQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13

C:\Users\user\AppData\Local\Google\Chrome\User Data\0905d002-c630-47fd-9177-c0c5de23f6e7.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):	166749
Entropy (8bit):	6.05144601435433
Encrypted:	false
SSDEEP:	3072:kGaYTJQE+mugy9+QV1T7IRwdfLSNPVLA7bV/nYorVcI8XIssElYTRe:VxaV+QfT7GSmhVgbV/njhcI8II6Re
MD5:	8338D676F19BA7CA0B3E158AF9DBE96A
SHA1:	E4F69E7BC24C8D6C9DEB05E95C09102D2E570D10
SHA-256:	AB4214D5FC361EB1957292F301096DFB9F5C0E182D176DC8A5625B8723CDF43F
SHA-512:	73781E2AED351040EFC52D4992AE00E1A9CFFF34467A9BE8EEE1E59E37D354A5078471F88D7BEE125C522EBE3A4124B979DC758259806313B4690BDC0EBAD53 0
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":1.62804988194663e+12,"network":1.628017484e+12,"ticks":5998863256.0,"uncertainty":5260958.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAAB BmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN 50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqk TQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13

C:\Users\user\AppData\Local\Google\Chrome\User Data\162bcb75-8048-4e9d-b63f-f80499b697a9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.749562338447069
Encrypted:	false
SSDEEP:	384:nX9SSsvpYMbW1Nqrfvem3Nm0pHk9Gx4rTwCUx94ow7rjimvUTAKm2VOgUmNr1qrV:fWRhCE19Qevsu0M/z2GKs2Wxu
MD5:	35ABB9A74DFDBD384D80070542F2DD71
SHA1:	042A247B0F07F28EDBAA6A72A46FF7CBADCBE4EF
SHA-256:	9C5FE4888BC3469CBC4CC9D4E08699CD50D9B535FA7FD4F68D317A5344E4B56A
SHA-512:	949954F67FC328583263E88E21980AB5D56819EAC6A93DCA2724FA00CEE0F140A52D0CC09E77CA8AD87194C1C645DE74B94F2969B8F7F0E51AD099569C1B675
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.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\3528511f-b6fc-4156-aee1-272847bcf05e.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):	174333
Entropy (8bit):	6.079017288623916
Encrypted:	false
SSDEEP:	3072:RkSGaYTJQE+mugy9+QV1T7IRwdfLSNPVLA7bV/nYorVcI8XIssElYTRe:+HxaV+QfT7GSmhVgbV/njhcI8II6Re
MD5:	6BECF2BCF866250DE1EEF12604BC822C
SHA1:	6C6A8F8AB9D82159AFEB48D0D5F1913D23F0980E
SHA-256:	21456DCA52C67777814B0DBBBD86CA4D1B9CF15AB8A0678717F28ED3CE03EC10
SHA-512:	3567A60DF85069A2E4E3D1962E2B3DAF702226001E2795E102988EC0F6975F9E3C3F16A0003A677E23CE274B17EF75781AC1758C379A54464487F821C184EBB2

C:\Users\user\AppData\Local\Google\Chrome\User Data\3528511f-b6fc-4156-aee1-272847bcf05e.tmp

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":1.62804988194663e+12,"network":1.628017484e+12,"ticks":5998863256.0,"uncertainty":5260958.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\4bd52f32-f80d-47c4-8fc8-c1637740570b.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):	174333
Entropy (8bit):	6.079017443233412
Encrypted:	false
SSDEEP:	3072:ZktGaYTJQE+mugy9+QV1T7IRwdfLSNPVLA7bV/nYorVcI8XIssElYTRe:mIxaV+QfT7GSmhVgbV/njhcI8II6Re
MD5:	0EBB2153A6A1052DC607C3ACF642AF69
SHA1:	00E658CAB31FCDDA4ACFFCC1153DF2B4880F7358
SHA-256:	AFE8593E2298647DC261462F19C7CCDE7D2F1E5A9035644882F5FA0610BDAC65
SHA-512:	D209D5EEEB3AC27F02A3DC1339B40276055F5337466E1222291C0CA8DC5EEB035F52326FB8850B89A7832F3F54AD6DC3D3EA2FE924F4620A773ED76DA8824BE
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":1.62804988194663e+12,"network":1.628017484e+12,"ticks":5998863256.0,"uncertainty":5260958.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909204239"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5c64f41e-784c-47c1-8dfe-c7f9efdfb6e9.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):	165870
Entropy (8bit):	6.049276256238569
Encrypted:	false
SSDEEP:	3072:hGaYTJQE+mugy9+QV1T7IRwdfLSNPVLA7bV/nYorVcI8XIssElYTRe:MxaV+QfT7GSmhVgbV/njhcI8II6Re
MD5:	A60B1C039952F9D8EF301AE6F8839711
SHA1:	B1C520FCE3C4B7563BC349448100FE18DBE8BBBE
SHA-256:	D5C1265E7E09C79E78F5B318225037FDA425AA3F82FEC696A8B8141067F6DB4F
SHA-512:	7597F0F1D2FCC7DA56176BB830A117CC929321D9C86A9F55C61A190C3749FCA680D6A2D1A48B6252829CF0013E04C6C08348C0FE0530AFCD6A42D6FB5E1FFE
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":1.62804988194663e+12,"network":1.628017484e+12,"ticks":5998863256.0,"uncertainty":5260958.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909204239"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6ce4d940-ec74-408b-b472-d66424e2e7f8.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):	166570
Entropy (8bit):	6.051059428387296
Encrypted:	false
SSDEEP:	3072:ZGaYTJQE+mugy9+QV1T7IRwdfLSNPVLA7bV/nYorVcI8XIssElYTRe:UxaV+QfT7GSmhVgbV/njhcI8II6Re
MD5:	C83B7FA3D42380ACD76CDAA9D5DFB119
SHA1:	2804898FEDBFF1044BE8F5CD623271C81E10EBAB
SHA-256:	1A217DE0E3979AD29791215DE9DFB60C09CCAAB10A4284CA01C639CF7CAD5EB2
SHA-512:	7BC889A14BEA2EFB462C0ACAEC57474A46E1573D1E76451C6354AAAF1F3C93FE267CF9DC621088FD7BAA4BD73104F06480006815F3A4BA0BABB9F736F95F992 7

C:\Users\user\AppData\Local\Google\Chrome\User Data\6ce4d940-ec74-408b-b472-d66424e2e7f8.tmp

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":1.62804988194663e+12,"network":1.628017484e+12,"ticks":5998863256.0,"uncertainty":5260958.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13

C:\Users\user\AppData\Local\Google\Chrome\User Data\8692ceb9-bffa-4565-a44f-db279e2bc348.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):	165870
Entropy (8bit):	6.049276256238569
Encrypted:	false
SSDEEP:	3072:hGaYTJQE+mugy9+QV1T7IRwdfLSNPVLA7bV/nYorVcI8XIssElYTRe:MxaV+QfT7GSmhVgbV/njhcI8II6Re
MD5:	A60B1C039952F9D8EF301AE6F8839711
SHA1:	B1C520FCE3C4B7563BC349448100FE18DBE8BBBE
SHA-256:	D5C1265E7E09C79E78F5B318225037FDA425AA3F82FEC696A8B8141067F6DB4F
SHA-512:	7597F0F1D2FCC7DA56176BB830A117CC929321D9C86A9F55C61A190C3749FCA680D6A2D1A48B6252829CF0013E04C6C08348C0FE0530AFCD6A42D6FB5E1FFE4
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":1.62804988194663e+12,"network":1.628017484e+12,"ticks":5998863256.0,"uncertainty":5260958.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909204239"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\973d2688-c16b-4391-865a-4f80eb8cff59.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7497091420802264
Encrypted:	false
SSDEEP:	384:hX9SSsvpkvMSVHZW1Nqrfvem3Nm0pHk9Gx4rTwCUx94ow7rjimvUTAKm2VOgUmNQ:N6WRhCE19Qevsu0M/z2GKs2Wxw
MD5:	80932DFBC63167699512FA433F1E7563
SHA1:	60E619B29F8C970F0A757225D6A36077B5BD8044
SHA-256:	DD80EC15D52AC1E17F25CA16FAFE55FCEC2516CAC3AAE5CDCE52F594540A89C7
SHA-512:	D07753C3ED82267328205787DEA14E27162CF7ED7003919603A88FF0EE78EAD30B872EB59A8F2C14874F5F782FC2DF27AAC68A7F12C4FC022539C17F808FAFCE
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.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\9f3e468a-98a1-4497-8873-c52b0e63117c.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.749799337109411
Encrypted:	false
SSDEEP:	384:RX9SSsvpkvMSVHZW1Nqrfvem3Nm0pHk9Gx4rTwCUx94ow7rjimvbJTAKm2VOgUmi:d6WRhCE89Qevsu0M/z2GKs2Wxs
MD5:	B675BDBF39239FBB1AB531E276EBD77D
SHA1:	D3477FBDBB1E1BBDD7E687A1AD9B3A07D5BFDD0A
SHA-256:	E704A024654033A1684014BBA16BF96E77815CB1B686AF18834478A5AEEE699F
SHA-512:	E0C7A057225BA8CD8D3FC99B6DC63C2446AE3C93B0FB59275C2A79761317ACF1DB83F304275F6E4C8EE838F42513EA3843E4EACF52224E05023A5BFDAA4BE26

C:\Users\user\AppData\Local\Google\Chrome\User Data\9f3e468a-98a1-4497-8873-c52b0e63117c.tmp	
Malicious:	false
Reputation:	low
Preview:	.t.............*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\...... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.......1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXJFIsz6VVJFIsz6VVJFIsz6I:+rJsrJsrJJ
MD5:	E4C3A0CCEDB71D53052C719DE30FD750
SHA1:	C89D101217D4AA05AD9C6FB24DB2037B3BCC630E
SHA-256:	B9ABED457F567199890198C9CE3B20954C73C458014CEB77C5E4514B1A8D8BF9
SHA-512:	D248EFCFA1BA3BA433A7A8D57B432F13D968DCF82A29535295BF03044982E69F441E6455EE7E6E7E4E902794B6D1B9CDAACBC92050B73062C0FDD33C4058034
Malicious:	false
Preview:	sdPC.......................@.*.L..nM._bMsdPC.......................@.*.L..nM._bMsdPC.......................@.*.L..nM._bM

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\135eb369-fdd5-4744-adf0-e75278f2ac5f.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):	5777
Entropy (8bit):	5.190513999327844
Encrypted:	false
SSDEEP:	96:na3hEyKU495mJD9YKI4ik0JCKL8vkshKbOTQVuwn:nOhmz95mrYKk4KOksy
MD5:	3AE1EC4A2202C3B6F604F5BB8F697571
SHA1:	0923C261C9B5C5BBBA3873948E0FCF187BDB0F62
SHA-256:	2BFBE42D958E3C311019D88366C98A8615E15EFD2567EC28923E7A5FF214A491
SHA-512:	9D30B14613375F255268877F9B64219BCA433B460CBF0DBC840A4CDC20051E0C4AF3ABDB9966F424DBE92A48655BC3EDD2DC3330104F251ACC1287F96088E41
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"co untryid_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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\13c16ad6-c8d0-48a3-83e4-c1ac25ad3598.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):	5.536221021665821
Encrypted:	false
SSDEEP:	384:MaJKtQLlS/XS1kXqKf/pUZNCgVLH2HfDzrUlHGQnTjSw45:7LlMS1kXqKf/pUZNCgVLH2HfvrU5GQny
MD5:	9EF9321CC8031D0D4F14C61CD5046CF7
SHA1:	39B9B91DA6EEDBB49175E62DD3704D62A1A4D197
SHA-256:	02A54A1AFC5A7EE07086155D7E5F3091E1221EC6004543F34778FB7DD3D8B588
SHA-512:	B1407FEFCBFF52165E49AAB85DB3A2EA605DE5634797DA9F3CB06F2D6129F5C13A2851636BFF7B7280AE4592EEAD49867A49630ECD1473C51517A609ACC495C 4
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272523478212116","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\13c16ad6-c8d0-48a3-83e4-c1ac25ad3598.tmp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\278ec475-abd7-486f-9800-57ffa61cb045.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):	1210
Entropy (8bit):	5.584337713834093
Encrypted:	false
SSDEEP:	24:YU6H0UhvqJkubUPRlG1KUevuoSwUHThUeT7D7wUrNRUevxQ:YU6UUhvyUqKUevnSwUtUenwUHUev2
MD5:	600E64441F428F79ED1D26EEE4B5B7B1
SHA1:	3E179BFA0D374B37622508C43EF5626B384FFBE3
SHA-256:	ED82F67F1001DF3A043512CE0046E1157D7FE37F9C8DF82207B00922590EDFBF
SHA-512:	F801F5E3C80E674CFE6AD75FE8A5051BCB0198DDF964C13F5A2C668AE26001BB3B0F09CDFC988C9E2DEB7545C334AE96F226459DF5058127A49AE79A0237052C
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1659585889.967863,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049889.967869},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1659585894.586709,"host":"rsvP85efofCgzU0Jm7B+b3hbNROo+MvFXBHkw7mYqac=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628049894.586716},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1659585883.769997,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3f7747bf-38de-4800-9572-e91c847d6394.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):	5515
Entropy (8bit):	5.179891459714669
Encrypted:	false
SSDEEP:	96:na3hEVKU495mJD9YKI4ik0JCKL8+bOTQVuwn:nOhVz95mrYKk4Kv
MD5:	244AA57027CC0EAE6FD87277E511BE01
SHA1:	8B75D2601E2388A610D078E9D1E0272DC0CC4FA1
SHA-256:	BD417FADD0CBAD1EAE078AF313F606E0B436FB094C5235AED74156401AB16F53
SHA-512:	55A8311AB8C565EC3C598390307240EDAA2C982BE172B58E8752FC3ABF5F040E3B0BED54A0BA2A16D0A7C81B6FE2E9F4718EBF9A39F948AAE63D2212A447079D
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4b203e18-c1f7-4205-b3c2-81faafbd8c4b.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):	5777
Entropy (8bit):	5.190513999327844
Encrypted:	false
SSDEEP:	96:na3hEyKU495mJD9YKI4ik0JCKL8vkshKbOTQVuwn:nOhmz95mrYKk4KOksy
MD5:	3AE1EC4A2202C3B6F604F5BB8F697571
SHA1:	0923C261C9B5C5BBBA3873948E0FCF187BDB0F62
SHA-256:	2BFBE42D958E3C311019D88366C98A8615E15EFD2567EC28923E7A5FF214A491
SHA-512:	9D30B14613375F255268877F9B64219BCA433B460CBF0DBC840A4CDC20051E0C4AF3ABDB9966F424DBE92A48655BC3EDD2DC3330104F251ACC1287F96088E41
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4b203e18-c1f7-4205-b3c2-81faafbd8c4b.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ef6881f-d542-4f41-a875-790d27716203.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):	5777
Entropy (8bit):	5.190513999327844
Encrypted:	false
SSDEEP:	96:na3hEyKU495mJD9YKI4ik0JCKL8vkshKbOTQVuwn:nOhmz95mrYKk4KOksy
MD5:	3AE1EC4A2202C3B6F604F5BB8F697571
SHA1:	0923C261C9B5C5BBBA3873948E0FCF187BDB0F62
SHA-256:	2BFBE42D958E3C311019D88366C98A8615E15EFD2567EC28923E7A5FF214A491
SHA-512:	9D30B14613375F255268877F9B64219BCA433B460CBF0DBC840A4CDC20051E0C4AF3ABDB9966F424DBE92A48655BC3EDD2DC3330104F251ACC1287F96088E41
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6506ddb1-0f3d-41be-818c-bf4a54262c2c.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):	2724
Entropy (8bit):	4.858441642519087
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swIMHlYhj:XGiQGBGFGJ12LLHDwGyGkGihj
MD5:	9E0C31BCE1C83C78981EB86A29E2879B
SHA1:	3973E5D4DA1BC0BB99B78D1DFA7BEA045C85E173
SHA-256:	3D1BDA968D1CFF79DBD0C4B9D2A22367E9D9B8374622CD4263BD39137D8FE584
SHA-512:	D196B2993F4A46AFFD38DBA59866B048221D5CF6EAB1574846D1799B748BD71B09BE28D8154B16D97AEA300C7EE13719DC2E5034EC9D8913C6A6B399BDEBC2E
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345624305","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7197c501-fe76-4e7c-a927-78f6762dc3c7.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):	5777
Entropy (8bit):	5.1904779385832756
Encrypted:	false
SSDEEP:	96:na3hEVKU495mJD9YKI4ik0JCKL8vkshKbOTQVuwn:nOhVz95mrYKk4KOksy
MD5:	A92ED24CD456066C23EFC8A8CFB9F824
SHA1:	AB423E3C275F714CA4EC94E33DF61896C9E6F7A2
SHA-256:	7045227AB6240C8D3DBB81CD917BF2BB78B86777B3EE1DD3E69D51546FFDEAA8
SHA-512:	5120B2A8311E12BDCA3EDBCE56DC2BAED4C8F5B39F6E3A66AE1D5AFF4DD30A20B740D0F4C02405C95965EE1885615B259EBDFB3EB20D7B77D933C7161FEA734A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7c137eee-a0aa-4813-9384-55748a83664e.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):	2776
Entropy (8bit):	4.876565559930106
Encrypted:	false
SSDEEP:	48:Y2nCDHXT6qtwz5sQDsYTsrRLsnATSPspyKsG7t8zso3qoPACksxMHbgYhbyD8:JnCDHXTxOz7d+DTBp5CaoPACNGFhj
MD5:	88E8F8C858A0E524DFCD7193C134666F
SHA1:	9F1C396811DDD241B050DD90CD94E57CDAEB2888
SHA-256:	CBEF70A474FED91889263F4F870D10ECCF4F69D5ED1270D152A414283BD779FB
SHA-512:	34B31694D51B81D712E69A9A7EF7986CD6C56B97DBEE8D08175B888DADB64C68839D98FD13C9F019DE82A8823F495468901A299DA975EEC5862CAEFE2C05FE 9
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275115483758874","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275115483769355","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8080bccf-8863-48a5-b156-cc9080489d38.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):	5777
Entropy (8bit):	5.190513999327844
Encrypted:	false
SSDEEP:	96:na3hEyKU495mJD9YKI4ik0JCKL8vkshKbOTQVuwn:nOhmz95mrYKk4KOksy
MD5:	3AE1EC4A2202C3B6F604F5BB8F697571
SHA1:	0923C261C9B5C5BBBA3873948E0FCF187BDB0F62
SHA-256:	2BFBE42D958E3C311019D88366C98A8615E15EFD2567EC28923E7A5FF214A491
SHA-512:	9D30B14613375F255268877F9B64219BCA433B460CBF0DBC840A4CDC20051E0C4AF3ABDB9966F424DBE92A48655BC3EDD2DC3330104F251ACC1287F96088E41
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8c5c62a0-ef61-4478-961e-e6c97a2098ed.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):	5489
Entropy (8bit):	5.177049184241513
Encrypted:	false
SSDEEP:	96:na3hEMKU495mJD9YKI4ik0JCKL81bOTQVuwn:nOhgz95mrYKk4Ku
MD5:	04EBAEA150A62187116E8D2A23D30868
SHA1:	0240E755AD1A935D6C7C7F521C70FBDC40A48F25
SHA-256:	C065BF6370E1631A74B2CF12872318C5F0FEF8F00896E3BA5519A901DE96EE10
SHA-512:	48D4C02BA665691D24B01F03F66347978EC55915CF896336139E2033531F94ECD6C2DB01FAFF9249F588CF791520446A7EEBB98A9B479D6BBB14D73B89ABBF6F
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\974f35ef-0fd4-404f-badb-817eb7b5799b.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\974f35ef-0fd4-404f-badb-817eb7b5799b.tmp	
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\9cc3dfae-55b0-4509-bfe0-e8717fc3c3cf.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):	1209
Entropy (8bit):	5.584713749060036
Encrypted:	false
SSDEEP:	24:YU6H0UhvqJkubUPRlG1KUev3oSwUohUeT7D7wUrNRUevxQ:YU6UUhvyUqKUev4SwU6UenwUHUev2
MD5:	F858E4303605BDDF9C28307CB4FC022B
SHA1:	5E7FA0BA56C771C1ADE1719E166263CC58B1558A
SHA-256:	DFB4A7F9308CE4F4A200EDD49148D95E1E9CDF554D89AFA7AE95AF6E765B2E07
SHA-512:	8AE87A20D3C2814905AE28B6704BBFA72AC4BAAE56B1E0604B664C4AAD07B34D3716E7D70EDA9B30A7024F17295EB9C2CE0D90A48994EB499EDC8E2738E1C675
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1659585889.967863,"host":"PKqosHGXLFTwexcsjC+UXTkKV3GWWHwtzKz/ULb9ssM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049889.967869},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1659585892.278085,"host":"rsvP85efofCgzU0Jm7B+b3hbNROo+MvFXBHkw7mYqac=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628049892.27809},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1659585883.769997,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_o

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):	342
Entropy (8bit):	5.138701689066789
Encrypted:	false
SSDEEP:	6:mHYVq2PcNwi23iKKdK9RXXTZIFUtpA3KgZmwPA3KIkwOcNwi23iKKdK9RXX5LJ:QYVvLZ5Kk7XT2FUtpA3Kg/PA3KI54Z51
MD5:	E3CD4BAE360E9D10EEE09FBD38028A88
SHA1:	9471645ABA7E53ACBC9D08C7221BE127A889C48E
SHA-256:	A1A7BBFD6C209319FDF2F5E935F65B918A4CE9CDFE4D29477BD2677F9D296B6D
SHA-512:	1888ACEB69B6489F2127743C354E68CFCFADE47B81CF64507C0121BF7EF684C64B90629DF385E60433B8FEDA8EA8C8900712D0FAF03823B4DAFEBB8D0636BBF4
Malicious:	false
Preview:	2021/08/03-21:04:43.481 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-21:04:43.483 1200 Recovering log #3.2021/08/03-21:04:43.483 1200 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\AutofillStrikeDatabase\LOG.oldCK (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	342
Entropy (8bit):	5.138701689066789
Encrypted:	false
SSDEEP:	6:mHYVq2PcNwi23iKKdK9RXXTZIFUtpA3KgZmwPA3KIkwOcNwi23iKKdK9RXX5LJ:QYVvLZ5Kk7XT2FUtpA3Kg/PA3KI54Z51
MD5:	E3CD4BAE360E9D10EEE09FBD38028A88
SHA1:	9471645ABA7E53ACBC9D08C7221BE127A889C48E
SHA-256:	A1A7BBFD6C209319FDF2F5E935F65B918A4CE9CDFE4D29477BD2677F9D296B6D
SHA-512:	1888ACEB69B6489F2127743C354E68CFCFADE47B81CF64507C0121BF7EF684C64B90629DF385E60433B8FEDA8EA8C8900712D0FAF03823B4DAFEBB8D0636BBF4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.oldCK (copy)	
Preview:	2021/08/03-21:04:43.481 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-21:04:43.483 1200 Recovering log #3.2021/08/03-21:04:43.483 1200 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):	326
Entropy (8bit):	5.155929288061919
Encrypted:	false
SSDEEP:	6:mHFVq2PcNwi23iKKdKyDZIFUtpA8YgZmwPAsY/SIkwOcNwi23iKKdKyJLJ:QFVvLZ5Kk02FUtpAHg/PAsYSI54Z5Kky
MD5:	B57CEF51209749B024601DA2045C7AEA
SHA1:	CE4D2B0B840E31FB0D17BE5DDE73A7D80FC5FF13
SHA-256:	C9F12016CAB26F3A99E1ECDC9B562332DAEA83DA78CAD23727DB54248AE95C6F
SHA-512:	D94F8E001CFADAF2AC568A6AA71DE5A045B772B9B71A50263B54DF799A4CEC332E4D62332F9AC14E0B1A826CEA6CC47D6F45F56B9ABAA795525810E91423EC87
Malicious:	false
Preview:	2021/08/03-21:04:43.471 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-21:04:43.473 1200 Recovering log #3.2021/08/03-21:04:43.474 1200 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\BudgetDatabase\LOG.old.G (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.155929288061919
Encrypted:	false
SSDEEP:	6:mHFVq2PcNwi23iKKdKyDZIFUtpA8YgZmwPAsY/SIkwOcNwi23iKKdKyJLJ:QFVvLZ5Kk02FUtpAHg/PAsYSI54Z5Kky
MD5:	B57CEF51209749B024601DA2045C7AEA
SHA1:	CE4D2B0B840E31FB0D17BE5DDE73A7D80FC5FF13
SHA-256:	C9F12016CAB26F3A99E1ECDC9B562332DAEA83DA78CAD23727DB54248AE95C6F
SHA-512:	D94F8E001CFADAF2AC568A6AA71DE5A045B772B9B71A50263B54DF799A4CEC332E4D62332F9AC14E0B1A826CEA6CC47D6F45F56B9ABAA795525810E91423EC87
Malicious:	false
Preview:	2021/08/03-21:04:43.471 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-21:04:43.473 1200 Recovering log #3.2021/08/03-21:04:43.474 1200 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\4278acc4333443e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.790496552611154
Encrypted:	false
SSDEEP:	3:m+l7vTLA8RzYcRKIQlM6lpjwIR5NTJQCK1lHCPE/lJiKqkozK5mSEpK5kt:miJYcRTSMiqIR5NdQC18tbwK4DK6t
MD5:	E52578B5AC44E8F93117BF296543C657
SHA1:	E92E4396BC01A2226443AA87A55A5A622D0865B4
SHA-256:	B7A31FC31CC36017F1A72D18A882AA46602E4566AD943150480EF4C4C96E9D90
SHA-512:	C6379749A8FB332B48CD22F3CCA1CA59F372E7AFF4E256BF5A0FC49C3F936359CCA1F5394E9A57B10653ED955C13DBD4D339DF8288D2D45B6980A6A6DE8F2D1
Malicious:	false
Preview:	0\r..m.....c...-9.Y...._keyhttps://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1 .https://live.com/.U./J'/.....v.....(....-...5.....K.y....x.\<..A..Eo.....M.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f3329f3f8204488_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.672868064284606
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f3329f3f8204488_0	
SSDEEP:	6:mYw9YcRTRKGKcXZygZ8FNdP7+AOXDZiwGRZwS4flthK6t:FMkcXZQNdT+JXgwD
MD5:	E67B0C246B908FDA5734F7FA938B07A4
SHA1:	8E081BCBF13B7E21F9A40104B29070F8D4490113
SHA-256:	E1E21EAF9DCB80616A4E6EA1AB96AD8EB1A890D9A641EB9850E39E2D5DDE0EA0
SHA-512:	B817C46B5584E1CD8360C8F97E0149331F222DE3EB0D6673429B52D06444702BC6A3B7C06323CC6A139A8A347EB543D4E214DE0C2E48923E7B761BF6C8B3EFA
Malicious:	false
Preview:	0\r..m....._.....)....._keyhttps://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1 .https://live.com/.../J'/.....:V^C..e.a.2u.N^){ .3.k..t0..A ..Eo.....\.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\59f8bbf14d4853fd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.677728870662404
Encrypted:	false
SSDEEP:	6:mYoLnYcRT/REXA5Rhj5l1Z3Nd516cH6JRGhBK6t:FokAPhFl15Nd7T
MD5:	FC6F5925E2F08885689F7594B49CE213
SHA1:	5B74180FBC9B179568593B0D5F48ACA968E6771E
SHA-256:	53D0B0F64DDB6E0B38A428334CE887C209C259977D1FA2CA21F35D190DEC8855
SHA-512:	51622643649779886C22A908C9BCBFDA031BDAE3B4C07789C02DEAD286A7604D9F9CA2DD291F57927AFED48D98ED04F9B64D6B856B97181089857A445EE170F
Malicious:	false
Preview:	0\r..m....._....._keyhttps://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js .https://live.com/."./J'/.....B..%<.....,.%..).H.8.>.Y....Y.A. .Eo.....$.`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7291a5a014c1cea6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.509712867968589
Encrypted:	false
SSDEEP:	6:mIVYSHT8NWQAJ6S4xf09tyJvHDYK45sK6t:rz8NWQKvEfOqvjf
MD5:	35AD38F86E747FBBA9B90C096D6AA051
SHA1:	01C4407797471408E7D39EC05A2F089C00145816
SHA-256:	923CADBE909A0DC0FDCACDF25B5F3E1BBC909986620ED1EFCF93C502185CAB10
SHA-512:	462F8C8B555563645B3325D5F5F540A4791CFA8ED16512A0470B5D23A2263DAEF689DF6EA218DCE78E4C6EF2BDA5A193D30079C7754F2267CF79C2E9A88B8B3
Malicious:	false
Preview:	0\r..m.....^...$....._keyhttps://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js .https://appdomain.cloud/.../J'/.....>m....r....h..P)u7..%.:..hj.-F.A..Eo.....(T! 2.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7e4cea594f77c74d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.662734483239306
Encrypted:	false
SSDEEP:	6:mOEYcRTdFAwhTT5NdkAxIyKL2lBy45bK6t:KFAwhTT5NdZQ0N
MD5:	0BD68A4FF2288056AD9589129948F261
SHA1:	D6E09D6CC0DF183E469F34D94E0C5715165DDE73
SHA-256:	FF4AB2E185FB6DFA9C0CA3DF58D93D769D6C58A1D531CDF9EA3A826AAEDB51A2
SHA-512:	3F88E9B63430FE9F567B01E01613BD8CB6C4C4B4E2E09628E6078D0949CD7D4A4DCA0892D708060398B16A5D14C7C52A326BA139897F5E5D2878457F5FBC87FI
Malicious:	false
Preview:	0\r..m.....V...$.DV...._keyhttps://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1 .https://live.com/(../J'/.....}OZ.\.,...mg.:Y...b..;.p.kg+.."S.A..Eo..... ....8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8fdad95f34dd1d59_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	5.653700748933298

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8fdad95f34dd1d59_0	
Encrypted:	false
SSDEEP:	6:m4ngMYcRTxTr4YqDNdNADIUdHA9k4rDK6t://34YqDNdNoRm+e
MD5:	206FE7AC21266DDC00679E33F0EDC0E5
SHA1:	E91A88B509CB5A373C987C744222B33497EB39D1
SHA-256:	2A83E1656035F6F5D212DD0F6D64B4E10B557C448593B50E43C5359EABBA451A
SHA-512:	DD828BB3C6BA76F13E90040AFD58B1D877C8441F0C796A80E96A0457B9B4E07D78D103BE0D6A0FB2AEDA815884BA7EBBA0B4371EBA624A95C85CCE859D2AD299
Malicious:	false
Preview:	0\r..m.....v....._keyhttps://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_Hu9XQvsxbdtI5Cn8ywiXCA2.js?v=1 .https://live.com/.../J'/.....O9..o....V\. ...~..S....o.u.v.wy.A..Eo....._.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7469dcb9561abcd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.720220295586349
Encrypted:	false
SSDEEP:	6:myi/VYcRTvyMCKMnUyNaENdnjWXydztr9g+40DK6t:LizMnUyNnNdKXYRr9hH
MD5:	E6E2E00BDCAB40292A985C58A3A8159D
SHA1:	E37303FBFB131D0E690A262776322CAFD0D962B3
SHA-256:	2BA99D4DE4B54386DC03D874B27C8D9A9467C64A64557FF636992E6A4185BC5D
SHA-512:	9BE25875F0E8943308870D2AEC1D3F3F5E12CC25A9C4E54E5CC1B2117B8F57CEBD178A604DA66ACE2A3F2ADA3D43B717CE8827475D8D9550C303B698F39EB9B
Malicious:	false
Preview:	0\r..m.....i....._keyhttps://acctcdn.msauth.net/lightweightsignuppackage_2AvLXlM9Do2tIgiv0FDCDg2.js?v=1 .https://live.com/.../J'/.....7H .V..q?..9S..9....[..fe..X..A..Eo.....J.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	312
Entropy (8bit):	4.931455435156363
Encrypted:	false
SSDEEP:	6:BFXAMqtzTNTTmCOTcC3yTSvHeRe6dMci3:BFQMqtzpTmfly2/egp
MD5:	9EC375D5C23F39801F62DB833951E9D4
SHA1:	897282EFC350434AF8A9B222D8084ED396C4D281
SHA-256:	492494BD3347EEE5BC3CBA92F3A04D6C0F90DA26C32DB7BA3BB0EC2BA749B217
SHA-512:	37AE06EC94D59F213BCEC8B370D6419D37DA8DB452E0B90F2A3D2929DF02C67CACF17BB67DA37EF67650E571BC729266B310921933B287F5061436D450FE9DA
Malicious:	false
Preview:	0...a..=oy retne.....M.wOY.L~...0J'/.....SHM..Y...0J'/.....a..F..../J'/.....Y..4_...../J'/.....D ..)3O.../J'/.....C43.xB.../J'/.....r.5./J'/.....^}.Np....-.../......./...3..-.../.....X.."T.L.+..../.....3.$[.<..+..../..... ,.0J'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	312
Entropy (8bit):	4.931455435156363
Encrypted:	false
SSDEEP:	6:BFXAMqtzTNTTmCOTcC3yTSvHeRe6dMci3:BFQMqtzpTmfly2/egp
MD5:	9EC375D5C23F39801F62DB833951E9D4
SHA1:	897282EFC350434AF8A9B222D8084ED396C4D281
SHA-256:	492494BD3347EEE5BC3CBA92F3A04D6C0F90DA26C32DB7BA3BB0EC2BA749B217
SHA-512:	37AE06EC94D59F213BCEC8B370D6419D37DA8DB452E0B90F2A3D2929DF02C67CACF17BB67DA37EF67650E571BC729266B310921933B287F5061436D450FE9DA
Malicious:	false
Preview:	0...a..=oy retne.....M.wOY.L~...0J'/.....SHM..Y...0J'/.....a..F..../J'/.....Y..4_...../J'/.....D ..)3O.../J'/.....C43.xB.../J'/.....r.5./J'/.....^}.Np....-.../......./...3..-.../.....X.."T.L.+..../.....3.$[.<..+..../..... ,.0J'/.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	1.9395073286163727
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7Uk82CSY44lKqNd9d8J1Lw7kTZLLOpEO5J/Kn7U7VLvMDswO9Z:dNwQ0bKq9ELNwFvIswWp0bKq9EE5cTp
MD5:	66BA57FCDC52F43BC517F1BC40CD5146
SHA1:	5C0CDBE5B215F5875D779746CDFAB0B770AD62A3
SHA-256:	DEBA09E59115378C43D1AA7E4B0BAD485F983FDAC174CB14EB238ABB4F711C84
SHA-512:	56EA977CFAD937740B4D0078D995303CFC27E16E224F6021901826711CEF1889C030074D0AB8AA5F4E97541EC43A37407BEB9005ADEE6B5B6C4FFDEBE232A99
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):	1.3386367700675768
Encrypted:	false
SSDEEP:	48:l2UYerq5LLOpEO5J/Kn7UGBw7kVpN82CSY44lKqNd9d8J14qekLLOpEO5J/Kn7UU:AUYOcNwyN0bKq9E4MNwQ
MD5:	6E29371C23D3C9A4D0DADEF3BB46C9BB
SHA1:	F8A141D0AEF631776442FA7F9BC018E66473AC3B
SHA-256:	36441078B598E66980D95F3BCF2E4B6C5917182E76ABA490F6C5D5FFBE4750B3
SHA-512:	2AFA38AC749900C222ED97F1E2602EF5A9ED58F9292C065AC262C99156C64DEE2BA5F0BF271D7D163552C90A3155E83BA17786D62C870240E033FF86AF764933
Malicious:	false
Preview:	.....u..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	28295
Entropy (8bit):	4.888947766380264
Encrypted:	false
SSDEEP:	768:kuELu5m/vAjj3vkmo5mGvAjj3vJmw5mIvAjj3vevAjj3mmV:kuELuTjTwUjTTijTPj/
MD5:	ED77075DD76B6EAD85488CEDC283FD0F
SHA1:	BB9891B2ACAF6656E44363B4F2230320EFFD5F3F
SHA-256:	13B8DF9A70785DA1F888C7D88409232468442BBC80F80AAF33F7F68143B5CEDF
SHA-512:	008CCF9C693C4100C7D5A9747A56D277B263011C1B4DBBD758A0E5CCAA3DD7BDB6FE2DC527FC0F30505F66B0A130A85E8B86CD18D7EECE9670461BDBF7E9F F0
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...8df84998_6d24_4672_9da9_2689f8aeebf5.....Ze..... .....5..0.....&...{C578CEAF-A17C-4AAB-9284-A5059F1242C7}.....K...file:///C:/Users/user/Desktop/Project%20Proposal%20and%2 0Analysis.html.....h.....`.....o.....o.....@.....X.....K...f.i.l.e.:././.C.:./.U.s.e.r.s./.f.r.o.n.t.d.e .s.k./.D.e.s.k.t.o.p./.P.r.o.j.e.c.t.%.2.0.P.r.o.p.o.s.a.l.%.2.0.a.n.d.%.2.0.A.n.a.l.y.s.i.s...h.t.m.l.....8.....0.....8..... .....K...file:///C:/Users/user/Desktop/Project%20Proposal%20and%20Analys

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
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):	328
Entropy (8bit):	5.212929757432308
Encrypted:	false
SSDEEP:	6:mdFlyq2PcNwi23iKKdK8aPrqIFUtpjur1ZmwPJRkwOcNwi23iKKdK8amLJ:AFlvLZ5KkL3FUtpjur1/Pv54Z5KkQJ
MD5:	FBBF0B4DBC9BC5DF06C118059C2FCB58
SHA1:	042FAB2C22F6F509E8E9241675261490E65BA64F
SHA-256:	FB39F7AC253EC22269A9FF243C87318805352AF3B2E4D42E0AE075E53D05B804
SHA-512:	1DFF70F347F9B81BC17BAC16D2648D0665D1544BE6C7330DE6911B824F3C8E93C463620FA3170551A65098299D6E843460E2D7754B5EC202DDC6F2E02061340D
Malicious:	false
Preview:	2021/08/03-21:04:38.539 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-21:04:38.542 1710 Recovering log #3.2021/08/03-21:04:38.543 1710 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 Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.212929757432308
Encrypted:	false
SSDEEP:	6:mdFlyq2PcNwi23iKKdK8aPrqIFUtpjur1ZmwPJRkwOcNwi23iKKdK8amLJ:AFlvLZ5KkL3FUtpjur1/Pv54Z5KkQJ
MD5:	FBBF0B4DBC9BC5DF06C118059C2FCB58
SHA1:	042FAB2C22F6F509E8E9241675261490E65BA64F
SHA-256:	FB39F7AC253EC22269A9FF243C87318805352AF3B2E4D42E0AE075E53D05B804
SHA-512:	1DFF70F347F9B81BC17BAC16D2648D0665D1544BE6C7330DE6911B824F3C8E93C463620FA3170551A65098299D6E843460E2D7754B5EC202DDC6F2E02061340D
Malicious:	false
Preview:	2021/08/03-21:04:38.539 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-21:04:38.542 1710 Recovering log #3.2021/08/03-21:04:38.543 1710 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
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):	325
Entropy (8bit):	5.216679099639963
Encrypted:	false
SSDEEP:	6:miQL+q2PcNwi23iKKdK8NIFUtpxG1ZmwP+MwQLVkwOcNwi23iKKdK8+eLJ:/VvLZ5KkpFUtpxG1/P+nI54Z5KkqJ
MD5:	D1F18F9F1314DBE6837782D44920552A
SHA1:	A6D850CD6D95366FBF41C7F90630F5A02719DB8F
SHA-256:	349A98C049DA73F88187B8E81C299277118DA3BC183847F236EBFC735514767A
SHA-512:	FC3CF9B06ACEC8B594CC0364D59BFE40AAF3AA26C6198D5642550B379C5D29B9EA5727559D23A452B0F65FCFB961F7364E713859668F13E9378CF7780F1B39D
Malicious:	false
Preview:	2021/08/03-21:04:40.866 478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-21 :04:40.868 478 Recovering log #3.2021/08/03-21:04:40.869 478 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\Extension State\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	325
Entropy (8bit):	5.216679099639963
Encrypted:	false
SSDEEP:	6:miQL+q2PcNwi23iKKdK8NIFUtpxG1ZmwP+MwQLVkwOcNwi23iKKdK8+eLJ:/VvLZ5KkpFUtpxG1/P+nI54Z5KkqJ
MD5:	D1F18F9F1314DBE6837782D44920552A
SHA1:	A6D850CD6D95366FBF41C7F90630F5A02719DB8F
SHA-256:	349A98C049DA73F88187B8E81C299277118DA3BC183847F236EBFC735514767A
SHA-512:	FC3CF9B06ACEC8B594CC0364D59BFE40AAF3AA26C6198D5642550B379C5D29B9EA5727559D23A452B0F65FCFB961F7364E713859668F13E9378CF7780F1B39D
Malicious:	false
Preview:	2021/08/03-21:04:40.866 478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-21 :04:40.868 478 Recovering log #3.2021/08/03-21:04:40.869 478 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+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):	51200
Entropy (8bit):	3.3002286878674307
Encrypted:	false
SSDEEP:	384:vOR5X/iObX/qyPm5O6mgmRmZVmdVm0VmiVmo:WR5viObvRPmY6mgmRmvmjmomOmo
MD5:	D3ABBFFA76398363FC6577FB9141A8A7
SHA1:	4A05F018EA0A92B9CA658BF65D1889997DC63B59
SHA-256:	E9F27024533B772CE05B502B98EBEC8AF7C17CFD9417B71D5D3BB797A08D158B
SHA-512:	D44DEA2EB6B806E2F587694E03289F19498D9B1CD55B25F1CD31491006B2CA54C1E0B8CA7B0CE7552A18572FEF534535024063754AEB22A1E60DFA8596586432
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):	33944
Entropy (8bit):	1.2509466551095587
Encrypted:	false
SSDEEP:	96:0CdBCX090V+NBCa6XHX15cRDucHX15cjD1vm:BLA4tbUXH+6cHexu
MD5:	0A95B1AFA317CCAEB6BEA4BC8478F29B
SHA1:	CDB9530A0D7D9C5CE9C645C2F8BFE4953A26DFDB
SHA-256:	4E5DD2655511948FF38E8CD3BDD8F5A403875067298B5BF312259F5FDBA6527C
SHA-512:	2E64362A5C87FB2620035979B547082C1428C63B3EEDB50DD2F05CD72334880F9E9550E6926D17B01C1A3FDA6B080B0182BB5C7FBF347B44CEF9E1C452ABE16
Malicious:	false
Preview:	.....8..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	380
Entropy (8bit):	5.204295524247049
Encrypted:	false
SSDEEP:	6:mHaaVq2PcNwi23iKKdK25+Xqx8chI+IFUtpAsgZmwPAjIkwOcNwi23iKKdK25+Xc:QaaVvLZ5KkTXfchI3FUtpAsg/PAjI54q
MD5:	454A8C2BBD4BF528580004F57BC80023
SHA1:	63D7E0547D3F34DB80BD5ADCC0347DF749F70DCB
SHA-256:	6007CF53EF4B345C5D57756EA8C1B5FBFFED94DE101C018BD8A802037A2BDD4B
SHA-512:	DD746743BA5C2B722A42AD4B2DF792969EC7FAD220E6C149920FB4F54B3817CECBFFB07F806D398F79C2201C849FA1B0C421312466E58FDE0608DFE7EAB075D 4
Malicious:	false
Preview:	2021/08/03-21:04:43.426 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/08/03-21:04:43.427 1200 Recovering log #3.2021/08/03-21:04:43.428 1200 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\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	380
Entropy (8bit):	5.204295524247049
Encrypted:	false
SSDEEP:	6:mHaaVq2PcNwi23iKKdK25+Xqx8chI+IFUtpAsgZmwPAjIkwOcNwi23iKKdK25+Xc:QaaVvLZ5KkTXfchI3FUtpAsg/PAjI54q
MD5:	454A8C2BBD4BF528580004F57BC80023
SHA1:	63D7E0547D3F34DB80BD5ADCC0347DF749F70DCB
SHA-256:	6007CF53EF4B345C5D57756EA8C1B5FBFFED94DE101C018BD8A802037A2BDD4B
SHA-512:	DD746743BA5C2B722A42AD4B2DF792969EC7FAD220E6C149920FB4F54B3817CECBFFB07F806D398F79C2201C849FA1B0C421312466E58FDE0608DFE7EAB075D 4
Malicious:	false
Preview:	2021/08/03-21:04:43.426 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/08/03-21:04:43.427 1200 Recovering log #3.2021/08/03-21:04:43.428 1200 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):	366
Entropy (8bit):	5.148875210306494
Encrypted:	false
SSDEEP:	6:mH67Vq2PcNwi23iKKdK25+XuoIFUtpAzgZmwPA87IkwOcNwi23iKKdK25+XuxWLJ:QGVvLZ5KkTXYFUtpAzg/PA87I54Z5Kkl
MD5:	3EC74380F1047437105D8774B59B718E
SHA1:	1015A9E8B977A4E1EC60A89EA474885454A78F6E
SHA-256:	A5D9FB00DBC2C65A389A9AFB6D605015F44FA5701D483001D1AA5F4DAD7A35F6
SHA-512:	08A5BFBC58EE58CDEA254613D69F794603853FFEC1A1F2FB6DF39B4E1A68953888B37DF28ED7F83C8E7C06A84346711898B2D3D06EA06C448DE061901B5271E
Malicious:	false
Preview:	2021/08/03-21:04:43.410 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST- 000001.2021/08/03-21:04:43.415 1200 Recovering log #3.2021/08/03-21:04:43.416 1200 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\Feature Engagement Tracker\EventDB\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old.. (copy)	
Size (bytes):	366
Entropy (8bit):	5.148875210306494
Encrypted:	false
SSDEEP:	6:mH67Vq2PcNwi23iKKdK25+XuoIFUtpAzgZmwPA87IkwOcNwi23iKKdK25+XuxWLJ:QGVvLZ5KkTXYFUtpAzg/PA87I54Z5Kkl
MD5:	3EC74380F1047437105D8774B59B718E
SHA1:	1015A9E8B977A4E1EC60A89EA474885454A78F6E
SHA-256:	A5D9FB00DBC2C65A389A9AFB6D605015F44FA5701D483001D1AA5F4DAD7A35F6
SHA-512:	08A5BFBC58EE58CDEA254613D69F794603853FFEC1A1F2FB6DF39B4E1A68953888B37DF28ED7F83C8E7C06A84346711898B2D3D06EA06C448DE061901B5271E
Malicious:	false
Preview:	2021/08/03-21:04:43.410 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-21:04:43.415 1200 Recovering log #3.2021/08/03-21:04:43.416 1200 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):	338
Entropy (8bit):	5.164513302944588
Encrypted:	false
SSDEEP:	6:mH/d4YVq2PcNwi23iKKdKWT5g1IdqIFUtpAQgZmwPAyIkwOcNwi23iKKdKWT5g1L:Q/d7VvLZ5Kkg5gSRFUtpAQg/PAyI54Zz
MD5:	C331275B4B640B5FB27516ED7178C79C
SHA1:	18F36F9487E4FB605CEEC963537648FED914A2EE
SHA-256:	7C2EF273BA11AECCB1AF6FA05FD9D960490CC1CE50DE38F5D321CF626BBA06CF
SHA-512:	0E09EE3AFD1CAFC0405C6F7A61CBCDF17358A392A2AC44C7FE5A4F383801FE7EF22D09F29ABDA5F2C95D8AAD8D5BD15AA79BC5A1B8B365368A25372EFB07E D02
Malicious:	false
Preview:	2021/08/03-21:04:43.398 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08 /03-21:04:43.401 1200 Recovering log #3.2021/08/03-21:04:43.403 1200 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.oldil (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.164513302944588
Encrypted:	false
SSDEEP:	6:mH/d4YVq2PcNwi23iKKdKWT5g1IdqIFUtpAQgZmwPAyIkwOcNwi23iKKdKWT5g1L:Q/d7VvLZ5Kkg5gSRFUtpAQg/PAyI54Zz
MD5:	C331275B4B640B5FB27516ED7178C79C
SHA1:	18F36F9487E4FB605CEEC963537648FED914A2EE
SHA-256:	7C2EF273BA11AECCB1AF6FA05FD9D960490CC1CE50DE38F5D321CF626BBA06CF
SHA-512:	0E09EE3AFD1CAFC0405C6F7A61CBCDF17358A392A2AC44C7FE5A4F383801FE7EF22D09F29ABDA5F2C95D8AAD8D5BD15AA79BC5A1B8B365368A25372EFB07E D02
Malicious:	false
Preview:	2021/08/03-21:04:43.398 1200 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08 /03-21:04:43.401 1200 Recovering log #3.2021/08/03-21:04:43.403 1200 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.4481240366544235
Encrypted:	false
SSDEEP:	3:8EflnJ/t:8cJ/t
MD5:	1D97F5DEF77F3A35DD6C755C7C8C77F1
SHA1:	E3EA69CFA07C946020D018814C5EC677E5422D44
SHA-256:	271EC6597FB7E9FA3C2A6739259027A74241D4F034B8B1D8FF7D5CB71E638B6D
SHA-512:	A1FE40200433E6560628A082E2D807374A04848F0BEF6578734CCAAF7B46CE593DF7DB84029DDCDAFD6CD4E9AF27BDA296E8D6A04D64CB0D7C04C36DDEE74 26
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Preview:	.'..(..... ....=Y.0J'/.....

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):	1.7857255701871597
Encrypted:	false
SSDEEP:	384:pfwzmX/+kDtrhX/8wmamLVmKmHvkVm3m6m:pfvpphv8wmam5mKmHwm3m6m
MD5:	8AD0EC8CAD6EFD4B86F1E9F0AD3D9815
SHA1:	B6730308BF36B90FDC0AB66ACD918B24955A22C8
SHA-256:	0461DCDF38C0A29EE682A6A96FC1B4352C946F46F401FFF11B8065A5755F4CDD
SHA-512:	010EC5272D45B9AB339B53754B3D8837F82B8A4B10B680C5D5ECDD65E112FB2AB8A8728ACD63A0F1AA0CFB2FE4D4E7D6D9E725283AE24D8D1379FB5A7B19E6AD
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):	652
Entropy (8bit):	5.276397005311081
Encrypted:	false
SSDEEP:	12:61o7W3wsRXaVVBiAenBOQjRCfoUkC6deO0ca+QP8d3lBk778B/xgskZBa9sd1OhA:eo7wlaLW8Q0MC6dcxATY78BJgskfa9iR
MD5:	733E921CFC77B20D46A89195758D4709
SHA1:	2F35A5B2892EA7368DA2F9A307DDED108150B5BB
SHA-256:	8E746BD9F4B7D8091E7FEF8680E55337C95853D9DABDD3DAEB17C3B2D5A23C67
SHA-512:	3493F94380060CACA9F320592CEE2C299F7987EB4DEDCF29E004DAA0B753541A467360F0DD1E632450A6CAEC05D60B96FB76BA98D004ADAFDB4F2D23D62A230
Malicious:	false
Preview:	....."N....analysis..and..c..desktop..file..user..html..project..proposal..users*v.....analysis.....and.....c.....desktop.....file.....user.....html.....project.....proposal.....users..2.....a.....c.....d.....e.....f.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....y...:\..... .....Bs...o..... .....*Kfile:///C:/Users/user/Desktop/Project%20Proposal%20and%20Analysis.html2.:.....J.....#+48A

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):	75432
Entropy (8bit):	0.30479669921969677
Encrypted:	false
SSDEEP:	48:SqJvY3NqLXHX15lHqRDuYPHX15lHqvD4mVF3fBO:ScvwgXHX15cRDuYPHX15cvDfVm
MD5:	D8351A2D9EE1D99FDC00304681763031
SHA1:	4C64157B7BEEB7D85B2E9A503087BE2012692649
SHA-256:	CD04F1ED04E8A96DE52671690D00C14DF9D860B2032BA530B24D7056C67275D8
SHA-512:	70EB95768B25FE77EE69C7D86EEB64593A0964546CBDE660F254013467A8CD617A607C795FC6073EDD3F1A3A4239D115203D15CFB8268D22433DE25D8B94C6B
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	28295
Entropy (8bit):	4.888947766380264
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session (copy)	
SSDEEP:	768:kuELu5m/vAjj3vkmo5mGvAjj3vJmw5mIvAjj3vevAjj3mmV:kuELuTjTwUjTTijTPj/
MD5:	ED77075DD76B6EAD85488CEDC283FD0F
SHA1:	BB9891B2ACAF6656E44363B4F2230320EFFD5F3F
SHA-256:	13B8DF9A70785DA1F888C7D88409232468442BBC80F80AAF33F7F68143B5CEDF
SHA-512:	008CCF9C693C4100C7D5A9747A56D277B263011C1B4DBBD758A0E5CCAA3DD7BDB6FE2DC527FC0F30505F66B0A130A85E8B86CD18D7EECE9670461BDBF7E9F F0
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...8df84998_6d24_4672_9da9_2689f8aeebf5.....Ze..... .....5..0.....&...{C578CEAF-A17C-4AAB-9284-A5059F1242C7}.....K...file:///C:/Users/user/Desktop/Project%20Proposal%20and%2 0Analysis.html.....h.....`.....o.....o.....@.....X.....K...f.i.l.e.:././.C.:./.U.s.e.r.s./.f.r.o.n.t.d.e .s.k./.D.e.s.k.t.o.p./.P.r.o.j.e.c.t.%.2.0.P.r.o.p.o.s.a.l.%.2.0.a.n.d.%.2.0.A.n.a.l.y.s.i.s...h.t.m.l.....8.....0.....8..... .....K...file:///C:/Users/user/Desktop/Project%20Proposal%20and%20Analys

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabs (copy)	
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\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.472738585621826
Encrypted:	false
SSDEEP:	48:Rv6GF7ta7jMK8dbBy5eA3bQSefgGlNrS0U9RdiN9e4:Rla7jMJdbBy5eA3bQ5fgGXrS0f
MD5:	BC5B75F24361E34507D7C13DBAFCA04D
SHA1:	56E7C09E2204972C22EC608784F7F43585343990
SHA-256:	C70FC19D723C62BEA839DF775977BD9F6C6E4734162BF4DA21626E663B76478D
SHA-512:	90BC6E2BAF65D229E196A00F36D7651D3FCBDD8E9489A417CAB810A05E4B813134566EE101C50DCA3C5F9FD29E2A747FA0A033DCB8EB6CD62F63E0E73979A9 5C
Malicious:	false
Preview:	.....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutS inkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast. RequestIdGenerator..746720000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 21:04:47.28][INFO][mr.Init] MR instance ID: 336523e9-17be-4ae6-b4a9-d5eada8025d5\n","[2021-08-03 21:04:47.28][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 21:04:47.28][INFO][m r.Init] Native Mirroring Service is enabled.\n","[2021-08-03 21:04:47.28][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 21:04 :47.28][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 21:04:47.28][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 21:04:47.28][INFO][mr.CloudProvider]

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):	340
Entropy (8bit):	5.149193287982256
Encrypted:	false
SSDEEP:	6:mdsyq2PcNwi23iKKdK8a2jMGIFUtpiivz1ZmwPiElRkwOcNwi23iKKdK8a2jMmLJ:SBvLZ5Kk8EFUtpiir1/PiA54Z5Kk8bJ
MD5:	7923D5559DDE66ED35F8C8EE06C544CA
SHA1:	AC47E8DD782EBF137D8E74380C1FA046068DB2B3
SHA-256:	41177B798D530E24A905B70975F90BB2AFACDA4AAF5A7F839D89AE0EE9D791F2
SHA-512:	82E8340ED96B02AE712F6486B6516D28FF22B03E32E77CC6A97DB2BAAEC279458EBDE767FF839C55454E531640C8A7D89C874ABBBFEA806EB17B746C17A85DI 5
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Preview:	2021/08/03-21:04:38.202 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-21:04:38.204 1710 Recovering log #3.2021/08/03-21:04:38.206 1710 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\Local Storage\leveldb\LOG.old01 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.149193287982256
Encrypted:	false
SSDEEP:	6:mdsyq2PcNwi23iKKdK8a2jMGIFUtpiivz1ZmwPiElRkwOcNwi23iKKdK8a2jMmLJ:SBvLZ5Kk8EFUtpiir1/PiA54Z5Kk8bJ
MD5:	7923D5559DDE66ED35F8C8EE06C544CA
SHA1:	AC47E8DD782EBF137D8E74380C1FA046068DB2B3
SHA-256:	41177B798D530E24A905B70975F90BB2AFACDA4AAF5A7F839D89AE0EE9D791F2
SHA-512:	82E8340ED96B02AE712F6486B6516D28FF22B03E32E77CC6A97DB2BAAEC279458EBDE767FF839C55454E531640C8A7D89C874ABBBFEA806EB17B746C17A85D5
Malicious:	false
Preview:	2021/08/03-21:04:38.202 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-21:04:38.204 1710 Recovering log #3.2021/08/03-21:04:38.206 1710 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):	49152
Entropy (8bit):	1.2625341618328965
Encrypted:	false
SSDEEP:	96:vOqAuhjspnWOFOqAuhjspnWOY5+nUVOqAuhjspnWOvmVXvOqAuhjspnWOY+uIkb9:H8n+nUZ04L+u1NL
MD5:	32F3BEEEDCF2B3EDB59DEE345B285368
SHA1:	B253D5E0EA431DE17818E8D2B7B6A8E1CC61FE37
SHA-256:	824DED3565FBF74827E4A098A1CD956AC3BD8421174BBD79613736D9E6AFADA3
SHA-512:	3864D06CF7DD7301477688EF6F71E7F269947D2E317D0F6DD133DF12C4912BBFEBBE7E85D35AD1D867DAD0C65C2810BA64855EEEAD92535518EFA31B6B7B355
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):	51344
Entropy (8bit):	1.0795736284326338
Encrypted:	false
SSDEEP:	96:KEUOqAuhjspnWOlhkOqAuhjspnWOqtKW0OqAuhjspnWOpmVXyEOqAuhjspnWOT:ByGihSClCU
MD5:	ED89F40D204B837B4A8DF87E6E7C79CB
SHA1:	765D28CE3BEAAC6E2113999D24E5D15FD8E8635A
SHA-256:	1266964FABA6BD3FBF566485A4A3C4D49C1613141D9BDE548723B80E35CED66C
SHA-512:	654440BB01B3D773C455E3686522F8E0D3933636527FFF62446CBD6F1ED17B1384CF19AD1EE2F1EBC2083EC0F4170AE4A824820FCAAD175F551138FDE251A3C
Malicious:	false
Preview:	.....F..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
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):	2776
Entropy (8bit):	4.876565559930106

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
Encrypted:	false
SSDEEP:	48:Y2nCDHXT6qtwz5sQDsYTsrRLsnATSPspyKsG7t8zso3qoPACksxMHbgYhbyD8:JnCDHXTxOz7d+DTBp5CaoPACNGFhj
MD5:	88E8F8C858A0E524DFCD7193C134666F
SHA1:	9F1C396811DDD241B050DD90CD94E57CDAEB2888
SHA-256:	CBEF70A474FED91889263F4F870D10ECCF4F69D5ED1270D152A414283BD779FB
SHA-512:	34B31694D51B81D712E69A9A7EF7986CD6C56B97DBEE8D08175B888DADB64C68839D98FD13C9F019DE82A8823F495468901A299DA975EEC5862CAEFE2C05FE 9
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com", "supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"i solation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https: //ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expirati on":"13275115483758874","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertise d_versions":[50],"expiration":"13275115483769355","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","

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):	342
Entropy (8bit):	5.274499331989101
Encrypted:	false
SSDEEP:	6:mdq2PcNwi23iKKdKgXz4rRIFUtp2ZmwPyRFkwOcNwi23iKKdKgXz4q8LJ:MvLZ5KkgXiuFUtp2/PyRF54Z5KkgX2J
MD5:	3A0A23994863ECEBF705DE52BD581B77
SHA1:	5D5787F34891A8B30994BFB316676DED48019B8B
SHA-256:	11399D3B1D31D70DB4DA224359DC35DF6E43DB35F10899C365A02CCC8B267EB1
SHA-512:	C32CC8C5F9F2AF34AA41BA8E216E4D89106AC0629A18A793F4B9143E63C158D33D1C62985AEF8449BAFE80424A0838264ABEDE013D171C01E0CCF05A8FE05A D
Malicious:	false
Preview:	2021/08/03-21:04:38.575 1694 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/ 08/03-21:04:38.578 1694 Recovering log #3.2021/08/03-21:04:38.581 1694 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	342
Entropy (8bit):	5.274499331989101
Encrypted:	false
SSDEEP:	6:mdq2PcNwi23iKKdKgXz4rRIFUtp2ZmwPyRFkwOcNwi23iKKdKgXz4q8LJ:MvLZ5KkgXiuFUtp2/PyRF54Z5KkgX2J
MD5:	3A0A23994863ECEBF705DE52BD581B77
SHA1:	5D5787F34891A8B30994BFB316676DED48019B8B
SHA-256:	11399D3B1D31D70DB4DA224359DC35DF6E43DB35F10899C365A02CCC8B267EB1
SHA-512:	C32CC8C5F9F2AF34AA41BA8E216E4D89106AC0629A18A793F4B9143E63C158D33D1C62985AEF8449BAFE80424A0838264ABEDE013D171C01E0CCF05A8FE05A D
Malicious:	false
Preview:	2021/08/03-21:04:38.575 1694 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/ 08/03-21:04:38.578 1694 Recovering log #3.2021/08/03-21:04:38.581 1694 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\Preferences (copy)	
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):	5777
Entropy (8bit):	5.190513999327844
Encrypted:	false
SSDEEP:	96:na3hEyKU495mJD9YKI4ik0JCKL8vkshKbOTQVuwn:nOhmz95mrYKk4KOksy
MD5:	3AE1EC4A2202C3B6F604F5BB8F697571
SHA1:	0923C261C9B5C5BBBA3873948E0FCF187BDB0F62
SHA-256:	2BFBE42D958E3C311019D88366C98A8615E15EFD2567EC28923E7A5FF214A491
SHA-512:	9D30B14613375F255268877F9B64219BCA433B460CBF0DBC840A4CDC20051E0C4AF3ABDB9966F424DBE92A48655BC3EDD2DC3330104F251ACC1287F96088E41
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_ser
vice_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser
_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl
acement":{"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}},"co
untryid_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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences0 (copy)

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):	5489
Entropy (8bit):	5.1768257890539715
Encrypted:	false
SSDEEP:	96:na3hrfKU495mJD9YKI4ik0JCKL81bOTQVuwn:nOh+z95mrYKk4Ku
MD5:	BCAC91E04515774E8B7970C46A655ABE
SHA1:	995FF951EF933F569ACA35328AD2CCFEAFB2A103
SHA-256:	90BC2F509504FC28F6475746D4EC59D9998207D91F8BE735F9F926B2E3606C58
SHA-512:	D516061001C59945FA2864F5C76A0F49917E108EE84F4999058E556EE2050CD51F1C554AA0EEC30D9481B03247A39140D5CF71BDB98DFF0300516E50DFB05C86
Malicious:	false

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_ser
vice_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser
_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl
acement":{"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}},"co
untryid_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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences0) (copy)

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):	5489
Entropy (8bit):	5.177049184241513
Encrypted:	false
SSDEEP:	96:na3hEMKU495mJD9YKI4ik0JCKL81bOTQVuwn:nOhgz95mrYKk4Ku
MD5:	04EBAEA150A62187116E8D2A23D30868
SHA1:	0240E755AD1A935D6C7C7F521C70FBDC40A48F25
SHA-256:	C065BF6370E1631A74B2CF12872318C5F0FEF8F00896E3BA5519A901DE96EE10
SHA-512:	48D4C02BA665691D24B01F03F66347978EC55915CF896336139E2033531F94ECD6C2DB01FAFF9249F588CF791520446A7EEBB98A9B479D6BBB14D73B89ABBF6F
Malicious:	false

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_ser
vice_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser
_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl
acement":{"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}},"co
untryid_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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesE (copy)

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):	5777
Entropy (8bit):	5.190513999327844
Encrypted:	false
SSDEEP:	96:na3hEyKU495mJD9YKI4ik0JCKL8vkshKbOTQVuwn:nOhmz95mrYKk4KOksy
MD5:	3AE1EC4A2202C3B6F604F5BB8F697571
SHA1:	0923C261C9B5C5BBBA3873948E0FCF187BDB0F62
SHA-256:	2BFBE42D958E3C311019D88366C98A8615E15EFD2567EC28923E7A5FF214A491
SHA-512:	9D30B14613375F255268877F9B64219BCA433B460CBF0DBC840A4CDC20051E0C4AF3ABDB9966F424DBE92A48655BC3EDD2DC3330104F251ACC1287F96088E41
Malicious:	false

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_ser
vice_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser
_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl
acement":{"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}},"co
untryid_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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesP (copy)	
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):	5777
Entropy (8bit):	5.190513999327844
Encrypted:	false
SSDEEP:	96:na3hEyKU495mJD9YKI4ik0JCKL8vkshKbOTQVuwn:nOhmz95mrYKk4KOksy
MD5:	3AE1EC4A2202C3B6F604F5BB8F697571
SHA1:	0923C261C9B5C5BBBA3873948E0FCF187BDB0F62
SHA-256:	2BFBE42D958E3C311019D88366C98A8615E15EFD2567EC28923E7A5FF214A491
SHA-512:	9D30B14613375F255268877F9B64219BCA433B460CBF0DBC840A4CDC20051E0C4AF3ABDB9966F424DBE92A48655BC3EDD2DC3330104F251ACC1287F96088E41
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferencesb (copy)	
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):	5777
Entropy (8bit):	5.190513999327844
Encrypted:	false
SSDEEP:	96:na3hEyKU495mJD9YKI4ik0JCKL8vkshKbOTQVuwn:nOhmz95mrYKk4KOksy
MD5:	3AE1EC4A2202C3B6F604F5BB8F697571
SHA1:	0923C261C9B5C5BBBA3873948E0FCF187BDB0F62
SHA-256:	2BFBE42D958E3C311019D88366C98A8615E15EFD2567EC28923E7A5FF214A491
SHA-512:	9D30B14613375F255268877F9B64219BCA433B460CBF0DBC840A4CDC20051E0C4AF3ABDB9966F424DBE92A48655BC3EDD2DC3330104F251ACC1287F96088E41
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523478498781","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

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):	20480
Entropy (8bit):	1.0031952989869743
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGURTi:wIElwQF8mpcSdW
MD5:	F3B7E6A695B662873DD33001CAAEF3F0
SHA1:	3761A69FF00553EB99DB7543A6DBDA7D088FFC50
SHA-256:	A2DCBB97ED59C6AADF601FE8BE80FE8A16A0B5D3719A5CD52B5D0FBF6212B6BA
SHA-512:	AFAFE67467EE3DF25C36A0CADBEC4FE8E49ECEE1C4004874A0D4CC7DC981CE9BE0C56247080B3FC559583D3AFC6469073BC42DC68F58D7D818ECF1472615E EE
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):	21044
Entropy (8bit):	0.8262633485012618
Encrypted:	false
SSDEEP:	48:jEqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUC6:jEhIElwQF8mpcSb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
MD5:	C9E47AFE73EBCE0F7D23090AC64FD045
SHA1:	6515AFAE4A91F51564EE2C52CA202CD35BFFC786
SHA-256:	06C714B083F79273678092BD3858A3C6B45C82A4300C5DB217A0EFDD2268BCEA
SHA-512:	7CE3299E7E801C2E99C739F2BA564758EB0CB189B9B232A9DDEDA62A6DB9107B4CCFD02D4A47700F71E06C47BFEC328FB90CFF10F10CEC3FD43577391952CE 7E
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences'. (copy)	
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):	5.536221021665821
Encrypted:	false
SSDEEP:	384:MaJKtQLlS/XS1kXqKf/pUZNCgVLH2HfDzrUlHGQnTjSw45:7LlMS1kXqKf/pUZNCgVLH2HfvrU5GQny
MD5:	9EF9321CC8031D0D4F14C61CD5046CF7
SHA1:	39B9B91DA6EEDBB49175E62DD3704D62A1A4D197
SHA-256:	02A54A1AFC5A7EE07086155D7E5F3091E1221EC6004543F34778FB7DD3D8B588
SHA-512:	B1407FEFCBFF52165E49AAB85DB3A2EA605DE5634797DA9F3CB06F2D6129F5C13A2851636BFF7B7280AE4592EEAD49867A49630ECD1473C51517A609ACC495C 4
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272523478212116","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535934187938461
Encrypted:	false
SSDEEP:	384:MaJKtpLlS/XS1kXqKf/pUZNCgVLH2HfDzrUlHGbnTuZ+8w4r:ALlMS1kXqKf/pUZNCgVLH2HfvrU5GbnW
MD5:	5D64BC594C1C1442C3EA4810DA33E6DB
SHA1:	B9535A4CEDD3C3EC8FBD3D2BFE8A498F30A72AD7
SHA-256:	56EFF1757BCCAB9B2D4E3A4A8ACD2DC13635E6B639604D2ECB23FB2BA5B0162A
SHA-512:	F15C4DA71AA10B36174549561C61163FF1D309C9923F34A558875987D1FA201BCDA3B4B17A04417EA4C8B3EC7FF224C6898C8EE52F4F3EDF25ABA6BC5D76479
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272523478212116","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946 B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.1797838000215535
Encrypted:	false
SSDEEP:	6:mbOI+q2PcNwi23iKKdKrQMxIFUtpkV5ZmwPkVtVkwOcNwi23iKKdKrQMFLJ:3dvLZ5KkCFUtpu/PC54Z5KktJ
MD5:	281AE5B2833F1B61AD50E8F9F14AC32C
SHA1:	A1F4D84CD647AD16CA7F926DDA8C11265924F0C4
SHA-256:	98C18687EB53B4C96FE724B9B5344B4A64B4E1F36584B7884880B8CA0AE4C784
SHA-512:	B204BB87B66F684C0669DA39EE07323EBAD81E46E8439A8A3585E01C0EB8D9A2C5D54C0C109D927048D379E0CF0E3D32D2385EAF08AE55B9AFD874FA1166E1 0
Malicious:	false
Preview:	2021/08/03-21:04:38.486 1698 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-2 1:04:38.488 1698 Recovering log #3.2021/08/03-21:04:38.488 1698 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.oldTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.1797838000215535
Encrypted:	false
SSDEEP:	6:mbOI+q2PcNwi23iKKdKrQMxIFUtpkV5ZmwPkVtVkwOcNwi23iKKdKrQMFLJ:3dvLZ5KkCFUtpu/PC54Z5KktJ
MD5:	281AE5B2833F1B61AD50E8F9F14AC32C
SHA1:	A1F4D84CD647AD16CA7F926DDA8C11265924F0C4
SHA-256:	98C18687EB53B4C96FE724B9B5344B4A64B4E1F36584B7884880B8CA0AE4C784
SHA-512:	B204BB87B66F684C0669DA39EE07323EBAD81E46E8439A8A3585E01C0EB8D9A2C5D54C0C109D927048D379E0CF0E3D32D2385EAF08AE55B9AFD874FA1166E1 0
Malicious:	false
Preview:	2021/08/03-21:04:38.486 1698 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-2 1:04:38.488 1698 Recovering log #3.2021/08/03-21:04:38.488 1698 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.14182438071701
Encrypted:	false
SSDEEP:	6:m8vlyq2PcNwi23iKKdK7Uh2ghZIFUtpYr1ZmwPY9RkwOcNwi23iKKdK7Uh2gnLJ:DAvLZ5KkIhHh2FUtpYr1/PY754Z5KkIT
MD5:	0722CB646107DAFD2ABF5A59BD4841C3
SHA1:	79F66AC223CE985BB3C14B415B9936F404BE2992
SHA-256:	6FF331107EB4D75FEB1D80413E9F7FB29E53E110A94DE07357D4185FD502B232
SHA-512:	11B400786C264E15863A9DC20EB4ECB7A3C98339AF7E596B546ED6514684B9D42A8BD34BCF4034737D68A4D6F132325DE2B7ADA1A5E3E85ECCC297F3AA546A F
Malicious:	false
Preview:	2021/08/03-21:04:38.176 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-21:04:38.180 1710 Recovering log #3.2021/08/03-21:04:38.180 1710 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old.E (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.14182438071701
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old.E (copy)	
SSDEEP:	6:m8vlyq2PcNwi23iKKdK7Uh2ghZIFUtpYr1ZmwPY9RkwOcNwi23iKKdK7Uh2gnLJ:DAvLZ5KklhHh2FUtpYr1/PY754Z5KkIT
MD5:	0722CB646107DAFD2ABF5A59BD4841C3
SHA1:	79F66AC223CE985BB3C14B415B9936F404BE2992
SHA-256:	6FF331107EB4D75FEB1D80413E9F7FB29E53E110A94DE07357D4185FD502B232
SHA-512:	11B400786C264E15863A9DC20EB4ECB7A3C98339AF7E596B546ED6514684B9D42A8BD34BCF4034737D68A4D6F132325DE2B7ADA1A5E3E85ECCC297F3AA546AF
Malicious:	false
Preview:	2021/08/03-21:04:38.176 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-21:04:38.180 1710 Recovering log #3.2021/08/03-21:04:38.180 1710 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):	438
Entropy (8bit):	5.252024602037692
Encrypted:	false
SSDEEP:	6:mzjF34q2PcNwi23iKKdKusNpV/2jMGIFUtpHJZmwPSDkwOcNwi23iKKdKusNpV/s:GOvLZ5KkFFUtpp/PM54Z5KkOJ
MD5:	14609C37AB2CBA4D20CEC35E251C0D82
SHA1:	0AA4FB831A4474533CA26BD98B6FCDFEEAF942A5
SHA-256:	21CCDCFF2786EA4ACE7B38D3AF0F6C3DBEC27DC68BD5943563A5FD2F922F7A7B
SHA-512:	CDFAEC08F775C9DE1D6D667760C027515AA24D5E300D0EF8534625CA84F1B26FC0417674B40F072E96CCF70F6B6FA95AEF7FE7DF4244E5C8E3082D229CEF75DC
Malicious:	false
Preview:	2021/08/03-21:04:38.516 15d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-21:04:38.517 15d0 Recovering log #3.2021/08/03-21:04:38.518 15d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.252024602037692
Encrypted:	false
SSDEEP:	6:mzjF34q2PcNwi23iKKdKusNpV/2jMGIFUtpHJZmwPSDkwOcNwi23iKKdKusNpV/s:GOvLZ5KkFFUtpp/PM54Z5KkOJ
MD5:	14609C37AB2CBA4D20CEC35E251C0D82
SHA1:	0AA4FB831A4474533CA26BD98B6FCDFEEAF942A5
SHA-256:	21CCDCFF2786EA4ACE7B38D3AF0F6C3DBEC27DC68BD5943563A5FD2F922F7A7B
SHA-512:	CDFAEC08F775C9DE1D6D667760C027515AA24D5E300D0EF8534625CA84F1B26FC0417674B40F072E96CCF70F6B6FA95AEF7FE7DF4244E5C8E3082D229CEF75DC
Malicious:	false
Preview:	2021/08/03-21:04:38.516 15d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-21:04:38.517 15d0 Recovering log #3.2021/08/03-21:04:38.518 15d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent Statemp (copy)	
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):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	437
Entropy (8bit):	5.297257656318444
Encrypted:	false
SSDEEP:	12:wVvLZ5KkmiuFUtpbdNAG1/PzdI54Z5Kkm2J:6l5KkSgtdNjZQo5Kkr
MD5:	34795C184F7FA172F55AC5E8F70CDA4B
SHA1:	C9FB8810FC149385771D2E5C6DAD68885449B457
SHA-256:	5D06667D344DE67AF8424474EC83C19D1626A3927325A31C5AEE2F9612BD05F0
SHA-512:	57AB135741DD2D393040C497C82A10D1113E3F71D640E6ABEACC1FFA17B9B2C0E2B7D4A705367185844E377683A9E0A8016CF461E9920956FEF03E6B2004C0C8
Malicious:	false
Preview:	2021/08/03-21:04:38.581 478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/08/03-21:04:38.585 478 Recovering log #3.2021/08/03-21:04:38.586 478 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	437
Entropy (8bit):	5.297257656318444
Encrypted:	false
SSDEEP:	12:wVvLZ5KkmiuFUtpbdNAG1/PzdI54Z5Kkm2J:6l5KkSgtdNjZQo5Kkr
MD5:	34795C184F7FA172F55AC5E8F70CDA4B
SHA1:	C9FB8810FC149385771D2E5C6DAD68885449B457
SHA-256:	5D06667D344DE67AF8424474EC83C19D1626A3927325A31C5AEE2F9612BD05F0
SHA-512:	57AB135741DD2D393040C497C82A10D1113E3F71D640E6ABEACC1FFA17B9B2C0E2B7D4A705367185844E377683A9E0A8016CF461E9920956FEF03E6B2004C0C8
Malicious:	false
Preview:	2021/08/03-21:04:38.581 478 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/08/03-21:04:38.585 478 Recovering log #3.2021/08/03-21:04:38.586 478 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
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):	423
Entropy (8bit):	5.261283026245541
Encrypted:	false
SSDEEP:	12:xk9+vLZ5KkMFUtpBboX/PBpk9V54Z5KkTJ:xkKl5KkUgrb+Co5Kkl
MD5:	F372FB0CC5F2D9EEA49895C5EE4BF02F
SHA1:	18B0D223FB4CC2839DF3331E0F1E69F2123F13D5
SHA-256:	E97DC65E8BE47EC22360F8D5A8FB52042B1398326D39D98A3BD82903A2B5E3E8
SHA-512:	DC08271CB3D76D5A6D1871F142B306FFF71BC3DE4A39D7EE2C471463B55945EBDEF7266E8EE888A9F2B5BCBF6863C8F013387CCFB5F8455D572BAFB1BCB973 40
Malicious:	false
Preview:	2021/08/03-21:04:55.202 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Session Storage/MANIFEST-000001.2021/08/03-21:04:55.239 57c Recovering log #3.2021/08/03-21:04:55.240 57c Reusing old log C:\Users\user\AppData\Lo cal\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\Session Storage\LOG.old` (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	423
Entropy (8bit):	5.261283026245541
Encrypted:	false
SSDEEP:	12:xk9+vLZ5KkMFUtpBboX/PBpk9V54Z5KkTJ:xkKl5KkUgrb+Co5Kkl
MD5:	F372FB0CC5F2D9EEA49895C5EE4BF02F
SHA1:	18B0D223FB4CC2839DF3331E0F1E69F2123F13D5
SHA-256:	E97DC65E8BE47EC22360F8D5A8FB52042B1398326D39D98A3BD82903A2B5E3E8
SHA-512:	DC08271CB3D76D5A6D1871F142B306FFF71BC3DE4A39D7EE2C471463B55945EBDEF7266E8EE888A9F2B5BCBF6863C8F013387CCFB5F8455D572BAFB1BCB973 40
Malicious:	false
Preview:	2021/08/03-21:04:55.202 57c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Session Storage/MANIFEST-000001.2021/08/03-21:04:55.239 57c Recovering log #3.2021/08/03-21:04:55.240 57c Reusing old log C:\Users\user\AppData\Lo cal\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\cec7fb21-548b-40af-8254-ab21f60c91a2.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):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","port":443,"protocol_str":"quic"}],"isol ation":[],"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\13d4f0f9-f60f-49b4-b615-33b9561f3c56.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):	4.96345415074364
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5Z0WlyhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd/0WCsBdLJlyH7E4f3K33y

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\13d4f0f9-f60f-49b4-b615-33b9561f3c56.tmp	
MD5:	1FE877DDE8B96DED122AC08BB07A83C5
SHA1:	5BEA5FFAF686474CE8ACA1D95500C29D65007745
SHA-256:	3AD373EB6FF8EA394964EDA2A9E53ADD8DBA11DC9716ED3CA672F10DF369BA4D
SHA-512:	1854F005CD691674FCF27376150ABD6F036A79C42BB4FFECDCCA14A74CB21D8ADF2552CACE631E6E9C92C58E7EF27279CA30CE5648C8EB90B06F2247A462003
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544342473569","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:	.'..(..... .....

Static File Info

General

File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	5.137162505922457
TrID:	
File name:	Project Proposal and Analysis.html
File size:	267
MD5:	acb86ccd1bb408c4aab64eb285118261
SHA1:	f2db12da0432d9371abd4986878fe57e183c5ed3
SHA256:	b452a456c1db4aeb269b51985302bb81576a775123c3b41a070f74973595c723
SHA512:	6b731b91a341a2abe00cbd4b1438e01cd537029085d3b579c3c2b76a01d120c129844c06ceb8c0311e16a9fd09c68b9588e4910d74e085e860334974bf586005
SSDEEP:	6:/OI6wQWR0NNEXW0YXlpz/8vpq2XRPx4fY2WPFrIsARNbBADQygFn:WI6wYf1mq2X9xESr9ATbIQygF
File Content Preview:	<HEAD>.. <meta http-equiv="Content-type" content="text/html; charset=ISO-8859-1" /> .. .. <META HTTP-EQUIV="Refresh" CONTENT="1;https://mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud/hebetate/index.html" >..... ....

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 21:04:43.612086058 CEST	192.168.2.7	8.8.8.8	0xc76f	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:43.615712881 CEST	192.168.2.7	8.8.8.8	0xee41	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:43.620676041 CEST	192.168.2.7	8.8.8.8	0x5090	Standard query (0)	mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:44.667143106 CEST	192.168.2.7	8.8.8.8	0xf541	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:46.312679052 CEST	192.168.2.7	8.8.8.8	0x9bf8	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:48.601341009 CEST	192.168.2.7	8.8.8.8	0xdcfb	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:49.439557076 CEST	192.168.2.7	8.8.8.8	0xe4f8	Standard query (0)	signup.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:50.666053057 CEST	192.168.2.7	8.8.8.8	0xc674	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:50.742177963 CEST	192.168.2.7	8.8.8.8	0xb049	Standard query (0)	acctcdn.msftauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:54.935806990 CEST	192.168.2.7	8.8.8.8	0x53b8	Standard query (0)	fpt.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:56.004988909 CEST	192.168.2.7	8.8.8.8	0x5b1a	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 21:04:43.649554968 CEST	8.8.8.8	192.168.2.7	0xc76f	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:43.651288033 CEST	8.8.8.8	192.168.2.7	0xee41	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:43.651288033 CEST	8.8.8.8	192.168.2.7	0xee41	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:43.662904978 CEST	8.8.8.8	192.168.2.7	0x5090	No error (0)	mailbuk50.s3.jp-osa.cloud-object-storage.appdomain.cloud	s3.jp-osa.cloud-object-storage.appdomain.cloud		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:43.662904978 CEST	8.8.8.8	192.168.2.7	0x5090	No error (0)	s3.jp-osa.cloud-object-storage.appdomain.cloud		163.68.118.49	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:44.700284958 CEST	8.8.8.8	192.168.2.7	0xf541	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:44.700284958 CEST	8.8.8.8	192.168.2.7	0xf541	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:46.349457979 CEST	8.8.8.8	192.168.2.7	0x7e67	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:46.360804081 CEST	8.8.8.8	192.168.2.7	0x9bf8	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:48.634197950 CEST	8.8.8.8	192.168.2.7	0xdcfb	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:49.477159977 CEST	8.8.8.8	192.168.2.7	0xe4f8	No error (0)	signup.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 21:04:49.477159977 CEST	8.8.8.8	192.168.2.7	0xe4f8	No error (0)	account.msa.msidentity.com	account.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:50.707616091 CEST	8.8.8.8	192.168.2.7	0xc674	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:50.707616091 CEST	8.8.8.8	192.168.2.7	0xc674	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:50.707616091 CEST	8.8.8.8	192.168.2.7	0xc674	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:50.768505096 CEST	8.8.8.8	192.168.2.7	0x53df	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:50.768505096 CEST	8.8.8.8	192.168.2.7	0x53df	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:50.793756008 CEST	8.8.8.8	192.168.2.7	0xb049	No error (0)	acctcdn.msftauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:50.793756008 CEST	8.8.8.8	192.168.2.7	0xb049	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:50.793756008 CEST	8.8.8.8	192.168.2.7	0xb049	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Aug 3, 2021 21:04:54.988718033 CEST	8.8.8.8	192.168.2.7	0x53b8	No error (0)	fpt.live.com	fpt.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:56.042627096 CEST	8.8.8.8	192.168.2.7	0x5b1a	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:56.042627096 CEST	8.8.8.8	192.168.2.7	0x5b1a	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:04:56.042627096 CEST	8.8.8.8	192.168.2.7	0x5b1a	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 21:04:56.117079973 CEST	152.199.21.175	443	192.168.2.7	49767	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jun 06 01:52:36 CEST 2021 Wed Jul 29 14:30:00 CEST 2020	Wed Jun 01 01:52:36 CEST 2022 Fri Jun 28 01:59:59 CEST 2024	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=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		
Aug 3, 2021 21:04:56.460557938 CEST	152.199.21.175	443	192.168.2.7	49769	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jun 06 01:52:36 CEST 2021 Wed Jul 29 14:30:00 CEST 2020	Wed Jun 01 01:52:36 CEST 2022 Fri Jun 28 01:59:59 CEST 2024	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=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 21:04:56.831404924 CEST	152.199.21.175	443	192.168.2.7	49770	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jun 06 01:52:36 CEST 2021 Wed Jul 29 14:30:00 CEST 2020	Wed Jun 01 01:52:36 CEST 2022 Fri Jun 28 01:59:59 CEST 2024	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=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5996 Parent PID: 4856

General

Start time:	21:04:37
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\Project Proposal and Analysis.html'
Imagebase:	0x7ff76d1c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 5424 Parent PID: 5996

General

Start time:	21:04:38

Start date:	03/08/2021
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=1552,17296826692838302678,18007796765270658976,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1664 /prefetch:8
Imagebase:	0x7ff76d1c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Disassembly