



ID: 452350
Sample Name:
Westernunionreceipt711
___vaw.html
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 07:59:17
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Westernunionreceipt711 ___vaw.html 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Initial Sample 3
Sigma Overview 3
Jbx Signature Overview 3
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 5
Domains 5
URLs 6
Domains and IPs 6
Contacted Domains 6
Contacted URLs 6
URLs from Memory and Binaries 6
Contacted IPs 6
Public 6
Private 7
General Information 7
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 7
IPs 7
Domains 8
ASN 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 37
General 37
Network Behavior 37
Network Port Distribution 37
TCP Packets 37
UDP Packets 37
DNS Queries 37
DNS Answers 38
Code Manipulations 38
Statistics 38
Behavior 38
System Behavior 38
Analysis Process: chrome.exe PID: 5028 Parent PID: 968 38
General 38
File Activities 39
Registry Activities 39
Analysis Process: chrome.exe PID: 5624 Parent PID: 5028 39
General 39
File Activities 39
Registry Activities 39
Disassembly 39

Copyright Joe Security LLC 2021

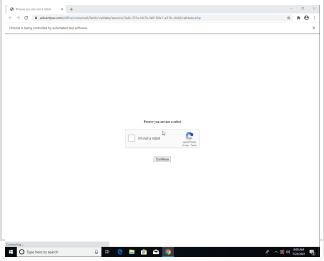
Windows Analysis Report Westernunionreceipt711 ___v...

Overview

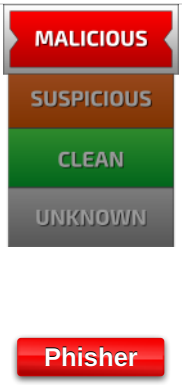
General Information

Sample Name:	Westernunionreceipt711 ___vaw.html
Analysis ID:	452350
MD5:	e43b99fcb58eef1..
SHA1:	3038d1bb1f1f23d..
SHA256:	ed68eb96911f17d.
Infos:	

Most interesting Screenshot:



Detection



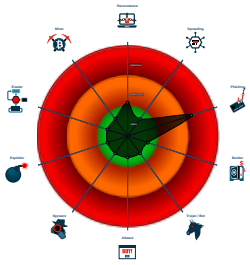
Phisher

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

Signatures

- Yara detected Phisher
- IP address seen in connection with o...

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5028 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\Westernunionreceipt711 ___vaw.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5624 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1540,9784536074538328282,17911257635406631719,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1716 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Westernunionreceipt711 ___vaw.html	JoeSecurity_Phisher_2	Yara detected Phisher	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Copyright Joe Security LLC 2021

Click to jump to signature section

Phishing:

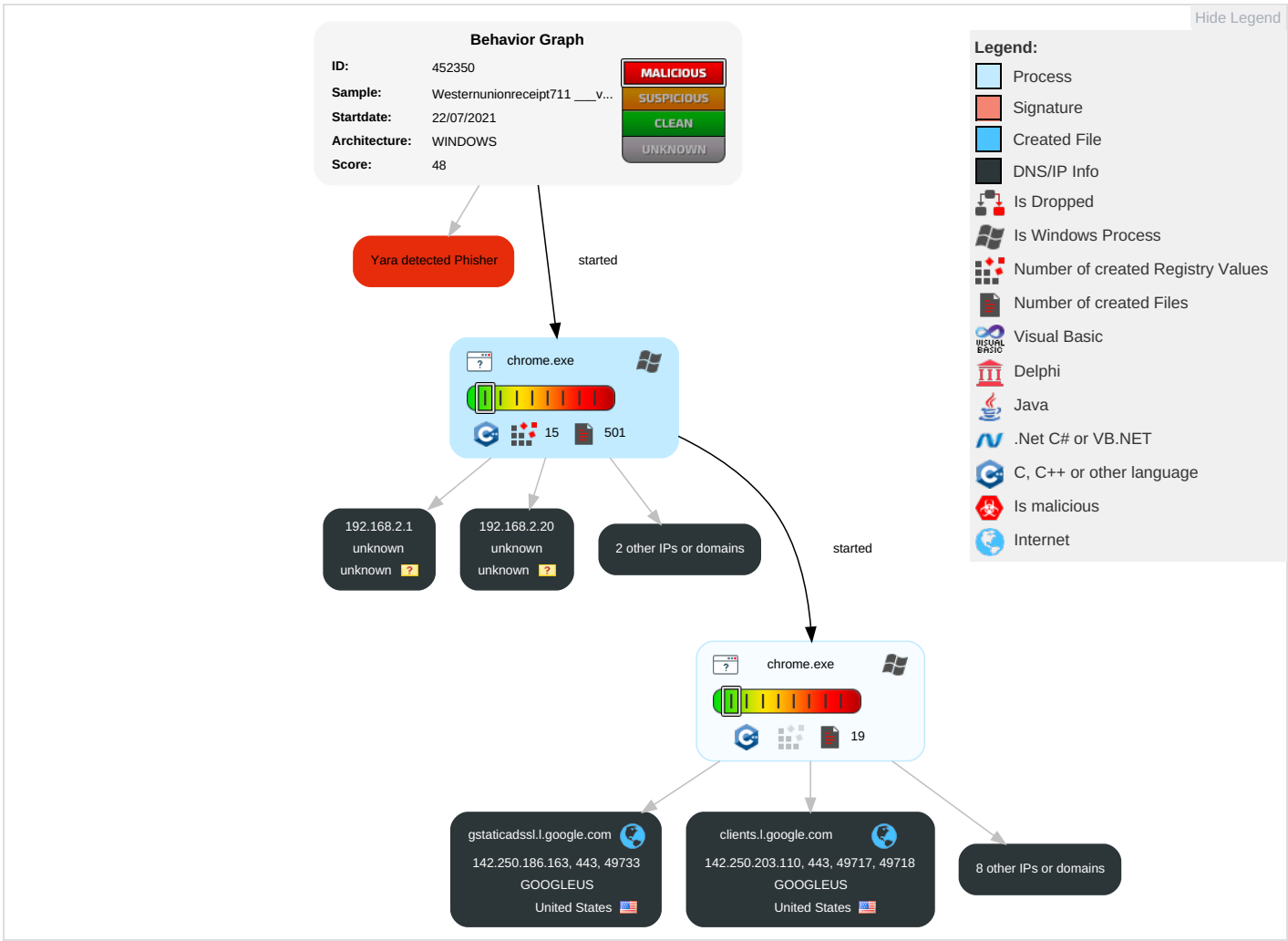


Yara detected Phisher

Mitre Att&ck Matrix

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

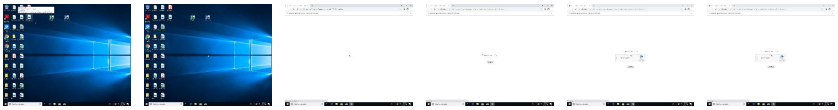
Behavior Graph

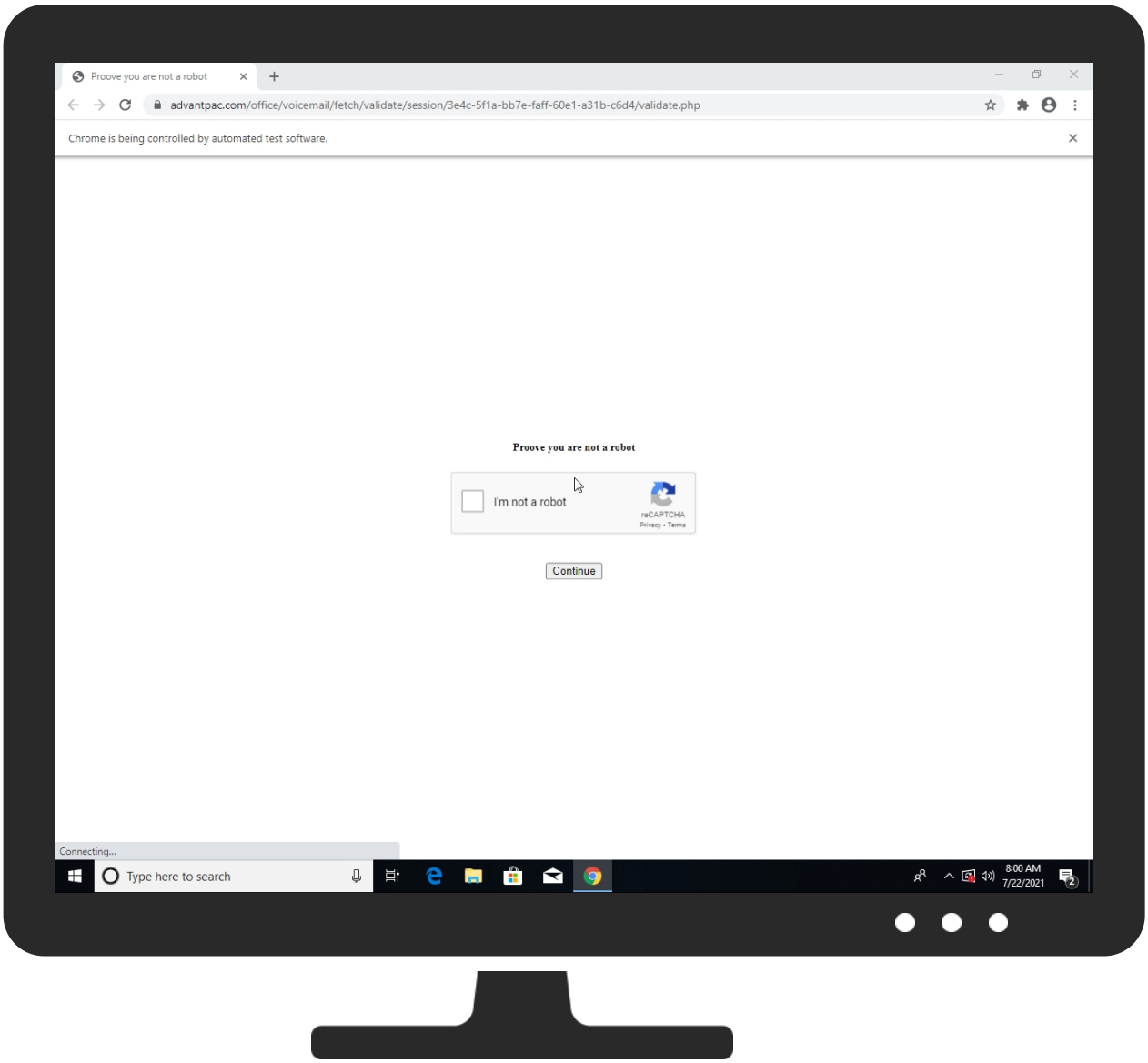


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://advantpac.com/office/voicemail/fetch/validate/session/3e4c-5f1a-bb7e-faff-60e1-a31b-c6d4/?em	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://advantpac.comh	0%	Avira URL Cloud	safe	
http://https://advantpac.com/	0%	Avira URL Cloud	safe	
http://https://www.google.comh	0%	Avira URL Cloud	safe	
http://https://advantpac.com/office/voicemail/fetch/validate/session/3e4c-5f1a-bb7e-faff-60e1-a31b-c6d4/val	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	Avira URL Cloud	safe	
http://https://advantpac.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
advantpac.com	104.21.40.98	true	false		unknown
gstaticadssl.l.google.com	142.250.186.163	true	false		high
a.nel.cloudflare.com	35.190.80.1	true	false		high
accounts.google.com	172.217.168.45	true	false		high
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldy1KEbAAAAAD62_S30p43Ix4MCrtTeHW9p7edM&co=aHR0cHM6Ly9hZHZhbnRwYWMuY29tOjQ0Mw..&hl=en&v=vzAt61JclNZYHl6fEWIBqLbe&size=normal&cb=imfahrxzyhdg	false		high
http://https://advantpac.com/office/voicemail/fetch/validate/session/3e4c-5f1a-bb7e-faff-60e1-a31b-c6d4/validate.php	true		unknown
http://https://www.google.com/recaptcha/api2/bframe?hl=en&v=vzAt61JclNZYHl6fEWIBqLbe&k=6Ldy1KEbAAAAAD62_S30p43Ix4MCrtTeHW9p7edM&cb=s2uulxcjojk	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.163	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
104.21.40.98	advantpac.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false

Copyright Joe Security LLC 2021

Private

IP
192.168.2.1
192.168.2.20
192.168.2.22
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452350
Start date:	22.07.2021
Start time:	07:59:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Westernunionreceipt711 ___vaw.html
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.winHTML@44/243@6/12
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html
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	Remittance.html	Get hash	malicious	Browse	
	DHL Documents.html	Get hash	malicious	Browse	
	2DAAD8278E0DDD4D247303ACED4B1D41C75CE94BE3A9E.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Convert HEX uit phishing mail.htm	Get hash	malicious	Browse	
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	
	Unisys.com_Fax-Message.htm	Get hash	malicious	Browse	
	192-3216-Us.gt.com.html	Get hash	malicious	Browse	
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	
	banload.msi	Get hash	malicious	Browse	
	Enclosed Business Proposals From 4 Square Services.html	Get hash	malicious	Browse	
	Invoice-Message-500.htm	Get hash	malicious	Browse	
	IPVrDRKfYj.exe	Get hash	malicious	Browse	
	_VM_1064855583.HtM	Get hash	malicious	Browse	
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	
	Pbogart.htm	Get hash	malicious	Browse	
	ATT93916.HTM	Get hash	malicious	Browse	
	Pbeesley-PAID-ACH-SJOJFB-30488393-Comtact.htm	Get hash	malicious	Browse	
	Cx9ER7vYGi.exe	Get hash	malicious	Browse	
	Emilemercier ProtectedCall.htm	Get hash	malicious	Browse	
	INV #95000987.html	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	MPU702734-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	XuQRPW44hi	Get hash	malicious	Browse	• 104.21.58.112
	Remittance.html	Get hash	malicious	Browse	• 104.16.18.94
	jRPSjUSf.exe	Get hash	malicious	Browse	• 104.23.98.190
	989E2813477A4245E0357E0F8E49AFAE384AF828C95EE.exe	Get hash	malicious	Browse	• 104.21.71.170
	P58w6OezJY.exe	Get hash	malicious	Browse	• 104.25.234.53
	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 172.67.130.27
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 162.159.134.233
	rxfttQnoO5	Get hash	malicious	Browse	• 1.13.147.24
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.21.72.95
	Cotizaci#U00f3n.pdf.exe	Get hash	malicious	Browse	• 104.21.36.131
	aviso de pago.pdf.exe	Get hash	malicious	Browse	• 104.21.39.75
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 172.67.130.27
	kRGc0HgN5b.exe	Get hash	malicious	Browse	• 172.67.188.154
	0n4xyK1WyMB3UE2.exe	Get hash	malicious	Browse	• 172.67.217.147
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28334.exe	Get hash	malicious	Browse	• 172.67.188.154
	Yaharasoftware.com_Fax-Message.htm	Get hash	malicious	Browse	• 104.16.19.94
	rrnIEffG4c.exe	Get hash	malicious	Browse	• 104.21.19.200
	Unisys.com_Fax-Message.htm	Get hash	malicious	Browse	• 104.16.18.94
	192-3216-Us.gt.com.html	Get hash	malicious	Browse	• 104.16.19.94

JA3 Fingerprints

No context

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

Copyright Joe Security LLC 2021

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\0e64314e-20f6-4266-ad6a-fca5dc5c22d8.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):	166488
Entropy (8bit):	6.050849630904747
Encrypted:	false
SSDEEP:	3072:WkZExZKKJEuwA4x37SiHnDcWYKWF8FcbXafIB0u1GOJmA3iuRY:VExzgRx37iWYFMaqfIlUOoSiuRY
MD5:	12D725F212C7275EAF7A44FE6CE0D0EA
SHA1:	8FD528BEFC05A408C6CC1D757AB432B5A1FA3427
SHA-256:	BDCBBB0EA692CA823DA9378B0F61A46CB2586178A155822DEFB1CF49085303A4
SHA-512:	9CA6379F9B633BBFDEF7C456488E1FD1B0E75B53850B8088875EBE3EDC1DBB868139BA05753F73744827489F785EE152F78EFFD9A353E1B2CC77384577B0C599
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":1.626966010115265e+12,"network":1.626933612e+12,"ticks":6186119719.0,"uncertainty":4946474.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1

C:\Users\user\AppData\Local\Google\Chrome\User Data\164da6ad-6634-4430-bc08-1dd997da7e52.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):	166067
Entropy (8bit):	6.049740424590365
Encrypted:	false
SSDEEP:	3072:6kZExZKKJEuwA4x37SiHnDcWYKWF8FcbXafIB0u1GOJmA3iuRY:hExzgRx37iWYFMaqfIlUOoSiuRY
MD5:	76CF34F2C470E7EDD4CA618F255EC564
SHA1:	5D1B3853E7112F54C337AB81E21AF195CFA221EC
SHA-256:	0348DD9F4B9F90A406DA7B4EE3D9FF63E12442B845CF69B65032AD263BAB1510
SHA-512:	250FB84D9235B8FFB59C8C7B1AF47704F58DC77DCCB49E394C40987BE1F47DCF0CAC4E83FD7F6D12648D1138ABAF5C6695C0BBB7AC5CB3129886D65DA5C9B31
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":1.626966010115265e+12,"network":1.626933612e+12,"ticks":6186119719.0,"uncertainty":4946474.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016952416"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\29064128-aceb-42fc-b4f9-d6c69f07389c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\29064128-aceb-42fc-b4f9-d6c69f07389c.tmp	
Category:	dropped
Size (bytes):	166153
Entropy (8bit):	6.049902372714611
Encrypted:	false
SSDEEP:	3072:LkZExZKKJEuwA4x37SiHnDcWYKWF8FcbXafIB0u1GOJmA3iuRY:qExzgRx37iWYFMaqfIlUOoSiuRY
MD5:	22E3268F8F745B6D609337E11594457E
SHA1:	65BA61C51165E5B97D9D945299727E9423B33EBC
SHA-256:	203EE4882010CA8651F093F883A8D1D47EDFA6C0F4EB12D4D07F3563CD53D17B
SHA-512:	B6F2B0EBC58872F66CC9C3D4B802E54B4D9558A4238C8F50A6AB2002E77D1827369DBEABA959A91632A8693F38E21ADFF90526D686D00D12C69702B910150A7
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":1.626966010115265e+12,"network":1.626933612e+12,"ticks":6186119719.0,"uncertainty":4946474.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016952416"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\777c35a9-578d-4f2b-a730-744262322fb1.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):	174421
Entropy (8bit):	6.0792197298394095
Encrypted:	false
SSDEEP:	3072:BVakZExZKKJEuwA4x37SiHnDcWYKWF8FcbXafIB0u1GOJmA3iuRY:HBExzgRx37iWYFMaqfIlUOoSiuRY
MD5:	47119C4A1E7B39F64FBB7B1CE8591C5D
SHA1:	010BD67DD18AF7F4BF11B2D099468AC6FD60CB57
SHA-256:	4FCD133A474814795712F2B1BF3140DC9155F8C1FA703A95250C82CE761A5B05
SHA-512:	2061A7EB7C1BA7C9F4B47C28DB3AB02E8397531ABA3CB48ED4B2F528CBA3BE033B1E16227C0D29F67C569E06725AEB3B6B812F172B5054D1122D490DAEF82A44
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":1.626966010115265e+12,"network":1.626933612e+12,"ticks":6186119719.0,"uncertainty":4946474.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016952416"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\780d3fde-b508-48a2-a2bb-981cb031d55f.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):	165963
Entropy (8bit):	6.04942978542699
Encrypted:	false
SSDEEP:	3072:SkZExZKKJEuwA4x37SiHnDcWYKWF8FcbXafIB0u1GOJmA3iuRY:5ExzgRx37iWYFMaqfIlUOoSiuRY
MD5:	7A570F1491AF0451F30C9EA34A6160F7
SHA1:	C07F08C44AEAB2C45582E7D140E68DDBA582F408
SHA-256:	EEBBAB9B254D2375C647C10EA089E29DA2E5B798591504D3B596A7C042145FB5
SHA-512:	59F047B7081744874E87F4B7D325F0958BECD76274DE174E665E83A2E3DCD4AF31175811C7730CC52C8281E217328A28B81E3AC883F29A69A041B14A03B3D4EE
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":1.626966010115265e+12,"network":1.626933612e+12,"ticks":6186119719.0,"uncertainty":4946474.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016952416"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\8622c107-8ea5-41f6-85d8-7ba4681d3664.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified

C:\Users\user\AppData\Local\Google\Chrome\User Data\8622c107-8ea5-41f6-85d8-7ba4681d3664.tmp

Size (bytes):	166571
Entropy (8bit):	6.051002953575357
Encrypted:	false
SSDEEP:	3072:hkZExZKKJEuwA4x37SiHnDcWYKWF8FcbXafIB0u1GOJmA3iuRY:oExzgRx37iWYFMaqfIlUOoSiuRY
MD5:	2455696D4E7113A66BAF3364D7DE9761
SHA1:	CD7C806799657A82FDF2C80AF75CDEE9A9236625
SHA-256:	797279809AD69A3ECD8D7662375DEF7C23A6B0B03B14F0F57527C753FEE8AF10
SHA-512:	6D02B4093D5DD0068534D135A129B912C9F5CF6A5592CC25B0B63EC978038CF43D00B45745F36EB65CBCBF5F2531A502C8375C408D878628282F07F0A0D22F33
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":1.626966010115265e+12,"network":1.626933612e+12,"ticks":6186119719.0,"uncertainty":4946474.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAA AAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRh NbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyX OajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"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:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D0212294256372C916B8155AC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1e6acc8c-cdf8-4207-980c-ccbe9841a06b.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\42eefd77-adfa-4811-9108-7008de8eed83.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):	4869
Entropy (8bit):	4.959518206570019
Encrypted:	false
SSDEEP:	48:Yc0UklSLklwHjUcrqA8dqTlYqlQKHoTw0RH3CH3G/s8C1Nfct/9BhUJo3KhmeSnz:n2CTGXMpcKIJok0JCKL8VbOTQVuwn
MD5:	D6599AC46A9F6738FE5074E0ED11F541

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\42eefd77-adfa-4811-9108-7008de8eed83.tmp	
SHA1:	0616D9555354ECE9390BE6C434E202DA36DEE5F5
SHA-256:	89BD748CAFF3B4B8443EB95B535D1508BF60BF619C0576A7F466B08C47850E24
SHA-512:	D370FEA5A3BA6D9D9C28CF931F478C930C3511551EF50FF9F5D813DF3F6F9A96D77D1E03A9128F157E8982E83FA6A052EB55F70EA295ADC74B3D5AF5AB05938
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271439607306792","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\86059bc0-7144-457e-8b33-4714e03f3808.tmp	
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.183948680010528
Encrypted:	false
SSDEEP:	6:mpVb+q2PWXp+N23iKKdK9RXXTZIFUtpQUZmwPQVVkwOWXp+N23iKKdK9RXX5LJ:gJ+va5Kk7XT2FUtpQU/PQVV5f5Kk7XVJ
MD5:	10F8EAC6785D92B2AD1AFE4D8A213F07
SHA1:	67FA66F5EE7F089BA36ACFC6DAF0DA04CAC47D4E
SHA-256:	F0BC23EE39077F8808A3BB1E93C0BD1A1E190E878BD0A8030F3B15CF0E83B66F
SHA-512:	A8016A652F4E64BF55E249F6168FD719C3FBECF851955D3AC3E6DF9D8576ECE6D31A2C21B50DDF97FAF4223CB92D0626D57DCC675818F497D363E2AC48FEF73
Malicious:	false
Preview:	2021/07/22-08:00:17.867 1adc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/22-08:00:17.921 1adc Recovering log #3.2021/07/22-08:00:17.922 1adc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.180331250125292
Encrypted:	false
SSDEEP:	6:mpZ+q2PWXp+N23iKKdKyDZIFUtpQHZmwPQ0VkwOWXp+N23iKKdKyJLJ:gZ+va5Kk02FUtpQH/PQ0V5f5KkWJ
MD5:	637B6F367CDD920B5050B4D1041D273B
SHA1:	5E3365404558BDB37E9699D8BBA6E7D5619038C3
SHA-256:	08F81AFE68A9BBE4B8BE9497A96F86AE6CED41E889064A0C86D6EFB0FDB3FF4A
SHA-512:	D72692765264DBE467ADCDAD636A0832559B5CDE55F19FA6B7D3A401122C0B8D159F8FA0EC9AE55100999C07176164541D98CB3035C91E9691F877AAAAFDE18
Malicious:	false
Preview:	2021/07/22-08:00:17.852 1adc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/22-08:00:17.854 1adc Recovering log #3.2021/07/22-08:00:17.855 1adc 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\Code Cache\js\1c36e4712c078b87_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	454120
Entropy (8bit):	6.135177784460166
Encrypted:	false
SSDEEP:	6144:o9UddlJiPe1OgwsOsQhul5tULbdDdivp0/cDo78+YEslx7QqMuc2:o9+dlGgw62bHN/78PZVQ6x
MD5:	583787586E0B54DAAD7F56CECC82D6A0
SHA1:	FA43102DE4AAEBAD22EFF097A40BC011C16DF477
SHA-256:	0342B4FA39EFB38ADF7FDB9CE0037250D72A3C8BF5B49F0CA90D42D45C05BC0D
SHA-512:	2825D1755BFDA964E44E31495862910F01A20972BD3108D869F4B1CC8E3D38541AD92C8B31B18DE37EDA514EEDD6A28B1A3803E16A0F06DF32C2C0F03DDBF92
Malicious:	false
Preview:	0\r..m.....@.....X....FF13900C1787683A7693232282F87CDF1C8CDC4015FE4A0E20AB5C7043BF81F2.....'.KU....O~... ...0.?".....4.....`...,.....p.....`.....d.....$.....D.....$.....H...\.....\.....t...X.....T...X.....@.....@.....X.....4...$.....8.....<...$.....(S.<..`2....L`.....(S.....`.N.....L`.....5.Rc.....QbVh.....Z.....Qb.....w.....Qb.BWQ....e.....Qb.m.....c.....QbR.....E.....Qb...V....Ja....Qb..;.....sI....Qb&L.e....kw....Qbj.90....rP....Qb.....XB....Qb.^.v....tp....Qb.....ei....Qb...]....iO....Qb&.e.....bd....Qb..Y....pz....Qb~.*.....HG....Qb2.....EI....Qb.....hp.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6e7e5900b9b0660b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.624965901352539
Encrypted:	false
SSDEEP:	6:maYnYGLKdXNQKH1AXtKGRK0PiHgFJqEot9/PbK6t:G6hNQKHidKGRv7JqEonHN

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6e7e5900b9b0660b_0	
MD5:	A2C284C4728B38B44B074312078DD2AD
SHA1:	67860874009568FBAFCCEC8ED664496D0E6BAD24
SHA-256:	D1AF84FD1886B8381948184BE240444CEABAFE8EA7D7793B03F43B3378B15D7B
SHA-512:	ECB66531F62B2D4551B1CBD4BD585BE3F3F1A0B6EA4424E5F85F7821F104A39A845AB3F00494CB094F24C8E8B1478C3995A8CE5B7D4655E893F4F5F945C3414(
Malicious:	false
Preview:	0\r..m.....p...M.K....._keyhttps://www.gstatic.com/recaptcha/releases/vzAt61JclNZYHl6fEWIBqLbe/recaptcha__en.js .https://advantpac.com/....M&/..... .....Y."..] ...P.SC.1....QO....or.}HZP.A..Eo.....6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8e2e4561ce876411_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	373
Entropy (8bit):	6.024825406665716
Encrypted:	false
SSDEEP:	6:m5EYGLKdXNQKH1AXtRuK70PiHg6KiSr/n4B/ZK6tiw8mCduuJN7VbPmmdzziSr/n:ShhNQKHid8KwjxUBrwmCPJVV7H3x
MD5:	ABD9E61623CA65B02EB63F1F47807070
SHA1:	49133687DFF151145F4EE1A7E21930E8DAF1ECF1
SHA-256:	006E30A9C2C626CB4508E525680B2C5D32608B00C741DC99C9BBB0AFD06CEFBF
SHA-512:	0EBE1429F4E10102EABCABE5462F9D317C15060619C7DCEFD031EAC96DFC3C18AE31221895AC5339D27D94B412106EB61EC833A6487533C8762796D182C0CD 1
Malicious:	false
Preview:	0\r..m.....m.....U....._keyhttps://www.gstatic.com/recaptcha/releases/vzAt61JclNZYHl6fEWIBqLbe/recaptcha__en.js .https://google.com/....M&/.....2..}2.N.ry ...w.!..P.g.A..Eo.....R}>.....A..Eo.....M&/.@...FF13900C1787683A7693232282F87CDF1C8CDC4015FE4A0E20AB5C7043BF81F2.....2..}2.N.ry...w.! ..P.g.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	312
Entropy (8bit):	4.911119325823777
Encrypted:	false
SSDEEP:	6:BD0QMTG4+Binj+SJMazQ3zbn3pHkQ+IRwHd:BD0TG4+WiOzyz7V4hd
MD5:	69696B678A50257638C1AC8C3C3D5F06
SHA1:	BD61A2DD098D78CB96B22DD7E862ECDE670ACB09
SHA-256:	B35F6AAD5AB263EDCA10FAF9A1D2B98859A830A3D2F79EEE850055ADC3DA1FF4
SHA-512:	C8EF9EBE098FC0412D065E72CF5E910F77F01C27C659B76A5237EBA29BB05D03BB060ED40ECBC5D7C3AE078E1681962E3461BAC2D9BB92E15427DC0FB01F13 41
Malicious:	false
Preview:	0.....4.oy retne.....,q.6.....M&/.....d..aE.....M&/.....f...Y~n@y..M&/.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<. .\.O$.KPu../.....p..(....KPu../.....q....._.KPu../.....+<P|...X.KPu../....._..M&/.

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):	0.8388358561387396
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwOXEqyoI2:TekLLOpEO5J/Kn7ULUqyr2
MD5:	3DFDB62B2A167C6DDCA94C38C853528B
SHA1:	702D127CA4098A8E916AA61BA310D682993A1584
SHA-256:	CAEB2D490F5D32759A73DFB59C14277A3C6BC9E11A30AB52F08977E46048F9EC
SHA-512:	3006ADD93A89B31F26D4A9632A3A750252B6639233B5B1626DD25687D41A218DE7F801DF722F9B85053138C8DA1B400CD574549B5EBD824D1AE3362321CCEBD
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9689668925502314
Encrypted:	false
SSDEEP:	24:LrcLgAZOZD/ZqLbJLbXaFpEO5bNmISHn06UwxH8:Lr8NOZZq5LLOpEO5J/Kn7UK8
MD5:	C5F93F955286ABF2642A5C61B62448EB
SHA1:	80411B87C0BC373570EA081F51AD205094BAAFD5
SHA-256:	C28A23B2345F85FDD788B00C2E0876BE33AA952876E81A58DAA690FFDF7C3C13
SHA-512:	D61378C6FCDCF1D4B25D2FBF831FA60FBF8CAE004E0AB4F5CC44CA2FD963C7F34D7D2E6325E9EC9F098B2754F5F2B8CAABFB5AD3B4D1471A6FD6C55D5515 E8B
Malicious:	false
Preview:	.....{..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5967
Entropy (8bit):	3.3284321443803173
Encrypted:	false
SSDEEP:	96:34TQlVFWbs1Ps1yn5yN52+X1bs16Ybn+ybs19:3/zfayns52N6wnq9
MD5:	BBED0EBF148E87432758244A7888B3FA
SHA1:	E5800572CED27EA5A015AEEDDC05F95DA6B2DAB8
SHA-256:	E446BA2B95B602B46C75332993EFEBA0DAF942D06705F7B4C9552BB127B79EFE
SHA-512:	DE83A10C7E7481D8BD28D812C6015C682EF5F87192D759938FEB59A7CBBA2E15F40219298881BFDDA20495D14F6BE95F1BD9D357D4682CC7E5E143C4BFA756 5
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...0e0c2df8_aae2_4efa_b021_77ff37ea7df6.....?..p..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....C...file:///C:/Users/user/Desktop/Westernunionreceipt711%20___vaw.html .....h.....`.....0.....H.....C...f.i.l.e.:././.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p ./.W.e.s.t.e.r.n.u.n.i.o.n.r.e.c.e.i.p.t.7.1.1.%.2.0._.-._.v.a.w...h.t.m.l.....8.....0.....8..... ....C...file:///C:/Users/user/Desktop/Westernunionreceipt711%20___vaw.html.....pp..M&/.....

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):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.190963889777618
Encrypted:	false
SSDEEP:	6:mp6X733+q2PWXp+N23iKKdK8aPrqIFUtpQ6uXZmwPQ6RR39VkwOWXp+N23iKKdKc:g673+va5KkL3FUtpQ6uX/PQ6RLV5f5KV
MD5:	E8D17DB68754ADE033FB16F5756B1DFB
SHA1:	50686DCCE38C3C6483352D128486694B63C01BC8
SHA-256:	B198B4C50DEDF5FCFE98857C9AD6C29B33835F5BEDFB75AE93F2AAD14291AE3C
SHA-512:	AA0F6FFC4342176031CA14AFF73B7BC60B1ACC79BB339887E8D9E36780FB0D72B0DCE2B915DE5BAB0CD0C6723E5F9F3DB547DE34CC82600D4EB5AA577A34108
Malicious:	false
Preview:	2021/07/22-08:00:07.312 d9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/22-08:00:07.313 d9c Recovering log #3.2021/07/22-08:00:07.314 d9c 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):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4C
Malicious:	false
Preview:	.f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

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\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_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):	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:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.218179156161132
Encrypted:	false
SSDEEP:	6:mppFUoi+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpQnFqZmwPQ73VkwOWXp+N23iKG:gAoi+va5KkTXfchI3FUtpQnFq/PQ7V5M
MD5:	3054C8845081C6BEA4A80FD75B43A9E2
SHA1:	32322B19EEEE612DDE2975B8ABA3E768A23D1A41
SHA-256:	90975C6DE0B3EDA88FFB9276FB315E63934EA0AE90B08D86EDA7A3D9AA5A296C
SHA-512:	0CFABEC4681A50F52C762A0738603B5A0EECE64AB79CC47AE6D3685CD55D172C73D2650C5F7C15C0E0382B6600863C64756AA728815D73529BC26E1795BD457
Malicious:	false
Preview:	2021/07/22-08:00:17.826 1adc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/22-08:00:17.828 1adc Recovering log #3.2021/07/22-08:00:17.829 1adc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.165638168827337
Encrypted:	false
SSDEEP:	6:mpsG+q2PWXp+N23iKKdK25+XuoIFUtpQeqZmwPQeGVkwOWXp+N23iKKdK25+Xuxo:gsG+va5KkTXYFUtpQf/PQfV5f5KkTXHJ
MD5:	7127A583CC1D048D036BDA30C34E5C99
SHA1:	408CCB2E1ED7734D42C62D92682A64EDF1CD2319
SHA-256:	911E15284B1806D5CE95DA859F3F4C8B3969005CE6D2166A868AF4ED95D06CBC
SHA-512:	98A74601A85C82F2D786DE4E640C5AE64A6A814179BB38FF993390A5590E84BD0C8381D7B016740D0089A39C09AAB8AC9EA9A990632F30B4CD25F99BF9B568A(
Malicious:	false
Preview:	2021/07/22-08:00:17.816 1adc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/22-08:00:17.818 1adc Recovering log #3.2021/07/22-08:00:17.818 1adc 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\File System\Origins\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	102
Entropy (8bit):	4.707425199545215
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\000003.log	
SSDEEP:	3:w1tsm1ilLeNlA1jPqciKPnSc+VVn:w1tsmRLVP1/Sc+VV
MD5:	7E6074135B54581D9C9A50EC25141C6A
SHA1:	362BE82BA04A240771813665F436B0EF9D24C35F
SHA-256:	8A14329F2C4F6E9CD07FDABA314C1F29FDE90C936695F0E95118778B2E0CD7A2
SHA-512:	D715BD9AE5A94DC6F30D6B8A475DFD69DE15C3915987D6A2D9E6F761237055AB1409B24431F9F6497FE0CDF664449F13F3D52FB0C49E4221CE3145862D9048F8
Malicious:	false
Preview:	mP.....LAST_PATH.-1.X7.>.....LAST_PATH.000..ORIGIN:https_www.google.com_0.000

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	143
Entropy (8bit):	5.280442407739586
Encrypted:	false
SSDEEP:	3:tUKIHedSQLLKqFkPWXp5cViE2J5iKKKc64E/+MOMcWIDMGk4cWIV//Uv:mpedjL+q2PWXp+N23iKKdK29MRgPRIF2
MD5:	FD352E639B970234B3CD6AF275075E14
SHA1:	D63C295A277C863444616F0D798A85920230A959
SHA-256:	5ABF54F678B4A5C939B2D1F74AF875CBCA0DC2F2399436811DF53EEFEF0DF57B
SHA-512:	02A789D4F609CFC989B54D50627373A87E89A13A14E34149AFA36E40FFF00C7041433C20E8731E596481578A32299E9CE5561D5D037878C6E0EAE7A6A58A0603
Malicious:	false
Preview:	2021/07/22-08:00:14.573 1558 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins/MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAIxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C235B
Malicious:	false
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.198913293072796
Encrypted:	false
SSDEEP:	6:mpZUoi+q2PWXp+N23iKKdKWT5g1IdqIFUtpQf1ZmwPQfZVkwOWXp+N23iKKdKWTk:gqoi+va5Kkg5gSRFUtpQf1/PQfZV5f5N
MD5:	E6ED75C1DECED10033F18E873A285549
SHA1:	38ABD81EF20A9D65124F2F72E02D213147180F08
SHA-256:	25B7B708B3CA8764025475014D625A49045DE1A1476180120536389A64C35057
SHA-512:	62CA8921252726A60AD210191F1B993AEA63E31A9B9640AA5B4FDF3272B917E11389ADD7F6D2C6E87E0BDEBDF6C4DF753D3227054AA44CC2A996089DE8FED61
Malicious:	false
Preview:	2021/07/22-08:00:17.789 1adc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/22-08:00:17.791 1adc Recovering log #3.2021/07/22-08:00:17.791 1adc 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):	0.45488079341118026

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Encrypted:	false
SSDEEP:	3:8EflNewPl/:84Pl
MD5:	76A02C9BA3E683DD60B6CB2B40E46B1E
SHA1:	4DF26DDE9C8F8164E8B0F21757AB467D4A529A4B
SHA-256:	D72B9AEE00933D6254254539AEE26940497B16842DCD4CB0E2FD619E5E53AB50
SHA-512:	E8D5E5418B9989104E8B3F99B9930663B8F80B681106769C7B88DD929F387EC545C7A9EDD5740D49A95CADFBEFF9175F46751440C849768ED811BED868A11CF
Malicious:	false
Preview:	.'..(.....;.M& /.....

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):	0.37604018857518
Encrypted:	false
SSDEEP:	12:TL+A/8T8B324O6nW6Lrlx6fwGRoQHtmSyEl8LB6fwGRoQHtmSzL0Q7PModQQl27i:TLxs85vxW6LrYqLBKL06UQpZf85vx0
MD5:	3C4BB0D239EEB7D47441B6B1A00404C7
SHA1:	D8B8FAB61736B7EE102745CFDD58FDF9E2F9F199
SHA-256:	EE90BA8C6874AE3B3522D3BB3D642F39E8763025296298E3A945FE8902A65890
SHA-512:	3A659CB393718642FECC16B90BC0B5485986E3268650A509DE4C2F655C4CDD772A94823B68C0A6DBD36888334B82CF694EBDAA9AED6DDB2E2BFBB83D11A34 FA
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):	2003
Entropy (8bit):	5.816369547290444
Encrypted:	false
SSDEEP:	48:Eoj164mWDRTwBftvit0dV1X3X7DnhnrDf8/5/:3ICyhtviw7H79nrD8V
MD5:	05B4CB0E2D6D06701929437FE65F2E68
SHA1:	8F3C5CE9BCEE4391FD6F84E44675ABD6EB42D7C2
SHA-256:	4720673AFFFA03BCC6EB29E5CF87D1A64232EE9DA3204BCCF2764978F2C0A259
SHA-512:	D81B8D6974CCBA011302E0CA70B4423147C19D61971A0D83CA14F51D035F9B518C9280539767A342740CCB98019232AEDDB73F287AB795F345554F492B65A0B5
Malicious:	false
Preview:	....."..."..3e4c..5f1a..60e1..a..a31b..advantpac..are..bb7e..c6d4..com..email..faff..fetch..https..huang..not..office..proove..robot..session..validate..voicemail..waley..w esternunion..you..php..c..desktop..file..user..html..users..vaw..westernunionreceipt711*..."....3e4c.....5f1a.....60e1.....a.....a31b.....advantpac.....are.....bb7e.....c.. ....c6d4.....com.....desktop.....email.....faff.....fetch.....file.....user.....html.....https.....huang.....not.....office.....php.....proove.....robot.....session.....users.....val idate.....vaw. ....voicemail.....waley.....westernunion.....westernunionreceipt711.!....you..2.....0.....1....!....3.....4.....5.....6.....7...!....a..... .....b.....c .....!.....d.....e.....!.....f.....g.....h.....i.....!.....k.....l.....m.....n.....!.....o.....!.....p.....!.....r.....!.....s.....!.....t.....

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):	0.11644717834977913
Encrypted:	false
SSDEEP:	6:499oug9bNFlWCj/lZl3lGS4/fMt76Y4QZVRtRex99pG/gqR4EZY4QZv8fO/S:49euqLBj/x3lX4nMWQA9LsBQZ8fOa
MD5:	9B2C5D01F96A1CDD9986E6CD9AA65841
SHA1:	FE212A525E03FD79EFE062DAE099D5A7044A988E
SHA-256:	F433FB882B49333357FE2B68440BF83689A1BB6C2124442650754A29B71C79BE
SHA-512:	3749A5870CDF6734F0A15BEC4AFAEA1F26A5F27173F3C454247D3D0E6E02546C2F1EF91D9C513298F4B2F18CE8840F3F733ED44012FA294DC184DE2CC5597D5
Malicious:	false
Preview:	.....D..D..... ....

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):	3069
Entropy (8bit):	5.552052077873499
Encrypted:	false
SSDEEP:	48:lb6aXSmGQVTa7sMv8dbC4IHbQSefgGn8NrS0U9RdiN9L3:BX1da7sMkdbC4IHbQ5fgGncrS053
MD5:	8D7B7586831194AF3A7E6A51C2824F0F
SHA1:	723D3B23FF51525FAB807FE3B0C20B6939D17227
SHA-256:	30850A98CCC299D072DAE2B1604FD4A43FC2FA2959A77093B3F83887F436B826
SHA-512:	498CDAA34612ED2E6904479DD1724F2A6954E57B9F7C78123B0D1A14178B54E9CEBC1BFCC967C5D588A5F0FF6870341C90C445A16934DBFDD6200110AF0EB98
Malicious:	false
Preview:	a..>k..*.....META:https://www.google.com....._https://www.google.com..rc::a..cjJxcGN6MTNtdzE5YQ==B.....,.....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..404755000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-22 08:00:19.72][INFO][mr.Init] MR instance ID: 879c5856-6686-4033-b782-6fd4802f929c\n","[2021-07-22 08:00:19.72][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-22 08:00:19.72][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-07-22 08:00:19.72][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-22 08:00:19.72][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.155793619933916
Encrypted:	false
SSDEEP:	6:mpAL+q2PWXp+N23iKKdK8a2jMGIFUtpQi1ZmwPQtsLVkwOWXp+N23iKKdK8a2jM4:glva5Kk8EFUtpQi1/PQe5f5Kk8bJ
MD5:	8E42F27F9FE03B838A0C32433CF485D6
SHA1:	D65ABE1E9F2C643CBB529EC0851277D86BE15D09
SHA-256:	D70BF036596D86C3A3968E08973B381DBE0E8A7445582FC8F4241FB95A4B7E27
SHA-512:	32E66C53F8BD449C599B846AC909E28FAF021BFD7DACC45DD0573F06FF6CBF9E7D3E5DBE2383EF8646EE0C701094787793409136FFFB3E88643593165CF7123
Malicious:	false
Preview:	2021/07/22-08:00:07.034 1558 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/22-08:00:07.038 1558 Recovering log #3.2021/07/22-08:00:07.043 1558 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2168894338059175
Encrypted:	false
SSDEEP:	6:mpoCFlL+q2PWXp+N23iKKdKgXz4rRIFUtpQcU11ZmwPQ+VQlLVkwOWXp+N23iKK2:govva5KkgXiuFUtpQcU11/PQ+VQz5f5j
MD5:	4E4278E89C3E125A5BB7C942C11AF4B3
SHA1:	13F9FAFFD391F29F83CE8E572A9547B119D4E6A7
SHA-256:	51B4AE614FF348FD99C08797527F5DE35BE5C8A4600B7EDFB03FE0C11211ECF2
SHA-512:	6D1711211D0AB72D1B65D75A9A5E2345004DE97BBD82CD4BF7B6AF58ECAD86D386C5C5D592795BC31E6DED84EE9E2021ACF2C7377506AB3409219AC746EC873
Malicious:	false
Preview:	2021/07/22-08:00:07.345 1558 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/22-08:00:07.349 1558 Recovering log #3.2021/07/22-08:00:07.350 1558 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\QuotaManager	
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):	77824
Entropy (8bit):	0.47942612120793326
Encrypted:	false
SSDEEP:	96:vCIG+6bDdsDaBJvtHIm50I4sX/CIG+6bDdsDaBJvtHIm50I4d0rh:a96EJTv4sXK96EJTv4d0rh
MD5:	0CA3F137DC9397DDCB874816009AFF8D
SHA1:	92946B04717FAF9BB13CB777B3E78FEEF1C35E9A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager	
SHA-256:	924A936E03D57CF92FCE4879E1D76A0CF600525251234AB1BC367262761AA2A3
SHA-512:	E6A5BF0D9B4C80F6C4ED3EEA459371CE0B342735AE2888D0F4E3A557E3E4316F133B8351AD9E60DDF5BD6253006575B09F1C322E87BACA10FA7D21F3460D186A
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g....*.W.L.[.....".....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	0.654937120768139
Encrypted:	false
SSDEEP:	48:3M3wqzLbCIG+6bDdsDaKgJgKtHIm50l9a+UaM5:3OwsCIG+6bDdsDaBJvtHIm50l4Z
MD5:	A27E3AE7AE0257FF205E3638754632CF
SHA1:	ED996574F6B281FD9A73A87EF979C89FC116B7CA
SHA-256:	2197B0F90030BF2DCC1A5DC6BDBED15430E8CDEB199B0F9C3914BA005623AD2F
SHA-512:	A205E533FE7CBB4A931DA24725DAAF91110A439B5170816558BB8D2FC5F5D4086480E4460E0B2F24A9B90ACDB9B97130D5C4FE610DBDFFA9234B682D32A22B03
Malicious:	false
Preview:	.....gk..... .....c.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.9887466392698049
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUmUIxfUAvpfUZB:wIElwQF8mpcSSUIxdvp8Z/
MD5:	08B739CCF0DDEA2B0D3E5368DE90AE26
SHA1:	C8253F31FF2C2221A994833278E412DA877B403D
SHA-256:	FE5B053862857238B039E11A1F80ED779E844E6067285083983CC90D954FD8BD
SHA-512:	D4E5023F39437BA41B3A1D9C29A5BCF48DCF15043C98C9D66055FC4B96F950E9ECBD3E9776175E66BFD7E63165903B546DF4E307F3F81AE7761331BE4A872E9
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):	0.6276050878835665
Encrypted:	false
SSDEEP:	48:ZIqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUX+4:ZIhIElwQF8mpcSd
MD5:	D84ADD51DEB60D118D9389AB25E8B1F0
SHA1:	3264C2E487F317C985135570327DF35B0C0763E6
SHA-256:	6EADB4D678E4DC20F53FE5906CA40FED3E4CF4B03C16235B6BC308DC82F1BA7C
SHA-512:	9ADD5C2E99DAD71F8080C563829F4E4C04172B03F97F05A27C3D8E27FBBC0255FADB3D7F1389DFAB060084C9B8828C3A31601F3986289F80A014B13E9A14A835
Malicious:	false
Preview:	.....8.:t.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	930
Entropy (8bit):	4.315643252307666
Encrypted:	false
SSDEEP:	12:5lxnNlCg7i0ls5C7bSUnGYEsUlJlkTSlkTSlkTSlkTXUi0lo5C7benfDpXUC:7xnlqCEvJ99991S22Nd7
MD5:	3F15365B0E011E585EBD20B3FA52662E
SHA1:	6DE74B0B2C4FD22DD51D741BC5EA5C28674403BA
SHA-256:	BDF78904EA0866BF28849D2F6D0E7D02CED986D44564717320 93E3D67F328D86
SHA-512:	D3B81FD051B205A66DC98153F6E7A2532780955170B5097E3B13392D59DA6DACB482D7EE6B80D8C8B3948DE2EB0C71680231E91BB69733B39688DFF8A62337F4
Malicious:	false
Preview:	..&f.....pe.....next-map-id.1.Fnamespace-0e0c2df8_aae2_4efa_b021_77ff37ea7df6-https://www.google.com/.0.9.....map-0-rc::c..B.H.K.B.S.T.l.G.v.m.l .J.Z.6.d.j.P.C.o.g.v.a.E.1.u.6.W.h.j.S.n.e.K.V.a.J.g.6.Q.O.Z.Z.0.J.C.q.4.5.N.Q.e.7.x.5.i.K.3.P.A.l.S.R.N.N.0.V.D.F.z.i.0.-.Q.T.e.Y.e.n.0.4.z.Z.L.6.J.U.1.H.8.1.O.8.u.u.B.p .8.2B.l.....2B.l.....2B.l.....2B.l.....2B.l.....|8).....map-0-rc::c..B.H.K.B.S.T.l.G.v.m.l.J.Z.6.d.j.P.C.o.g.v.a.E.1.u.6.W.h.j.S.n.e.K.V. a.J.g.6.Q.O.Z.Z.0.V.C.p.I.d.w.Q.d.T.X.4.S.S.e.O.E.R.a.R.P.5.3.f.W.8.H.w.W.G.c.Y.O.Y.3.-.0.V.4.X.t.m.r.U.k.3.l.3.O.U.u.m.h.J.-.X.E.H.Y.P.Q.h.....map-0-rc::c ..B.H.K.B.S.T.l.G.v.m.l.J.Z.6.d.j.P.C.o.g.v.a.E.1.u.6.W.h.j.S.n.e.K.V.a.J.g.6.Q.O.Z.Z.0.Z.C.p.a.p.4.Q.u.7.X.4.i.S.e.O.E.R.a.R.P.5.3.f.W.8.H.w.W.G.c.Y.O.Y.3.-.0.V.4.X.t.m. r.U.k.3.l.3.O.U.u.m.h.J.-.X.E.H.Y.P.Q.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.1380376346236645
Encrypted:	false
SSDEEP:	6:mpuN+q2PWXp+N23iKKdKrQMxIFUtpQInZZmwPQM3VkwOWXp+N23iKKdKrQMFLJ:guN+va5KkCFUtpQw/PQoV5f5KktJ
MD5:	ECD1D4B1DE1BED06662CBBD29DB01E73
SHA1:	3241CA5343B4EF72502166B1B8A4D2ECA05D2266
SHA-256:	379F018378C4E1A35D9426F453E7260C8AED38286D0EC31694F8A59E6E8DAE6C
SHA-512:	D49F81C828824A1D8ADE0A54168D54649E913E571E790230E8EC5310CBE32CF759013079ADD4A03F4021D7CAE61725D815F86E10EF66C11FC01954F88EE11EAE
Malicious:	false
Preview:	2021/07/22-08:00:07.260 d9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/22-08 :00:07.262 d9c Recovering log #3.2021/07/22-08:00:07.257 d9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.161105727543621
Encrypted:	false
SSDEEP:	6:mpORaIq2PWXp+N23iKKdK7Uh2ghZIFUtpQO7ZZmwPQORkwOWXp+N23iKKdK7Uh2w:gORaIva5KklhHh2FUtpQO1/PQOR5f5KF
MD5:	D2EA01563EC84E7946D7B6E2F3862053
SHA1:	B0BBB8824550B2212F08ED51DBA304540A3C0929
SHA-256:	F8DF5FECF5D925AE7B1101EB3DE2A34936E59A244568EEA59CDE597F947B891D
SHA-512:	6B42F253EEA6A959AB986E950509AE24136C3EACAC2A0704D342F027EB144B6E5D4AE6668D1DF93490115D7CC8BE9A82F8B2DAB55EE65F20639575255C653B2
Malicious:	false
Preview:	2021/07/22-08:00:06.949 4b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/07/22-08:00:06.971 4b0 Recovering log #3.2021/07/22-08:00:06.973 4b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Char acteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\75ff1d10-9ace-40ff-8d36-0f7a88d fa848.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\75ff1d10-9ace-40ff-8d36-0f7a88dfa848.tmp	
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.257864676769057
Encrypted:	false
SSDEEP:	6:mpxFL+q2PWXp+N23iKKdKusNpV/2jMGIFUtpQj1ZmwPQsLVkwOWXp+N23iKKdKux:gCva5KkFFUtpQj1/PQ85f5KkOJ
MD5:	4C6D468AE3587664BADF337F0BBAE905
SHA1:	38CFE3801F34AF38E5A48F9395650817D7CA4B56
SHA-256:	310AF9C3DDC55AD16D93ED356F32E4BD1D41B728646ED6D318EAEBA550DDCC50
SHA-512:	F91865699F8827F5118C070A6C77654FEB87C1796ED666BD0E2EC68E11C3650D0DB1E2A20315213D59AAA2368423E7E35DBA719CF25DD28B768CF09EAB26E76
Malicious:	false
Preview:	2021/07/22-08:00:07.291 1558 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-08:00:07.293 1558 Recovering log #3.2021/07/22-08:00:07.294 1558 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.250371082158088
Encrypted:	false
SSDEEP:	6:mpaRIq2PWXp+N23iKKdKusNpqz4rRIFUtpQO7ZmwPQcRzkwOWXp+N23iKKdKusN9:goIva5KkmiuFUtpQo/PQcR5f5Kkm2J
MD5:	BC6A55E62C0DBFA7628B1EFFFF641120
SHA1:	5BE858F6E6606A923B7C525B1052BD66E55EE213
SHA-256:	D7EF042883C475044795695CF6F61B4BF44C45699DFAE6C54D293654481613CB
SHA-512:	ED4979FA969415DD8DE9D3CED329F04F5246C81CF328F229DDBA693B1947A3506E32661DB29A63FD5DFEE885C96AE1C8ACE14110B5BD40932D916A33F79B89A
Malicious:	false
Preview:	2021/07/22-08:00:07.343 600 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/07/22-08:00:07.347 600 Recovering log #3.2021/07/22-08:00:07.349 600 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.2659963881936935
Encrypted:	false
SSDEEP:	6:mpJbMq2PWXp+N23iKKdKusNpZQMxIFUtpQJXZmwPQJwBkwOWXp+N23iKKdKusNpB:gJgva5KkMFUtpQJX/PQJwB5f5KkTJ
MD5:	EB8E4A353152904CFD8DE3DDD1950B08
SHA1:	BE19B6126D4C8468CA123C9C3E76D82FFA494416
SHA-256:	7B866848392F9ED812F885E7895E299CDBE096C6C1BCD482CD4548DADA23059A
SHA-512:	6C0E724F65A768890F6176982EED36045A65EF643A20C828013601C6FF9E6194D05F8344BBA1B014780600B48B86EB580CB42D2DFCBE2742CD1B8E8F80B38052
Malicious:	false
Preview:	2021/07/22-08:00:23.540 464 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/07/22-08:00:23.542 464 Recovering log #3.2021/07/22-08:00:23.543 464 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\36551c3b-7e77-4e7d-8f10-70a0969c19f6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.1950732222939155
Encrypted:	false
SSDEEP:	12:gg+va5KkkGHArBFUtpQ9/PQ2V5f5KkkGHAryJ:gpa5KkkGgPgGewf5KkkGga
MD5:	0459A74574E619F66D8DC8F94319F3E3
SHA1:	65071113CC9442288A6CC2BADB33628FB77CBC33
SHA-256:	C3B21ECF39DA213BED640DBE98E5BD00B9253CD609BD744D0B4AF9F5AC40312D
SHA-512:	08A76829F330DEB57DEE15FD9C375141D8C6884B4B2342DAFFA1452E3AF8097EE882B351BC4A836760D1739EC535F8A5839CC04C06D014481CB391A0B2E609B
Malicious:	false
Preview:	2021/07/22-08:00:18.334 d9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-08:00:18.335 d9c Recovering log #3.2021/07/22-08:00:18.336 d9c 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.200913096247907
Encrypted:	false
SSDEEP:	12:gBoOva5KkkGHArqiuFUtpQ0/PQQr5f5KkkGHArq2J:g3a5KkkGgCgGd0f5KkkGg7
MD5:	89E05011C3F0D3574A6C5D8336002084
SHA1:	9FC8F25C479D88A1BAE57A6EE755DDAEB18227CC
SHA-256:	175804270CC91A6DAEF43C776C7CDF0158B418FEE7C7FF242CAE2E8FFA652462
SHA-512:	6F219CF4E59E8E02AEBD4406A5F5FC0E56DC4FDEBD84B68C684207739119F3EF045A4A464EDDFDD75032DD5B9CBF66079FD8FE1DC59ADB7730F45DF3B8083 2B
Malicious:	false
Preview:	2021/07/22-08:00:18.348 1420 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/07/22-08:00:18.351 1420 Recovering log #3.2021/07/22-08:00:18.353 1420 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):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Preview:	..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.213838703991671
Encrypted:	false
SSDEEP:	12:glqva5KkkGHArAFUtpQlA/PQlrT5f5KkkGHArfJ:gKa5KkkGgkgGblFf5KkkGgV
MD5:	ADF789F3A4BE1099BF08C4813E352BCA
SHA1:	D5F8D5E3C2387DBED697856AFFCBA01301F68903
SHA-256:	E231E6F5C999B29C65E1329009BFF533D140453B272A4805BFEB56C286BDC62A
SHA-512:	1D2AC09E91B335C690AF5A08BA5C9F0B757ABC5D68D16D11A1F5974D60EECB0DCAC65AD39A21420C0E42FD5B865D3D3E022416C5AC56DBD8738294E725F4B 65
Malicious:	false
Preview:	2021/07/22-08:00:33.651 464 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/07/22-08:00:33.652 464 Recovering log #3.2021/07/22-08:00:33.653 464 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.258393820529447
Encrypted:	false
SSDEEP:	6:mpOTRlL+q2PWXp+N23iKKdKpIFUtpQO61ZmwPQOifQFLVkwOWXp+N23iKKdKa/Wd:gOGva5KkmFUtpQO61/PQOsE5f5KkaUJ
MD5:	F1B2747F4E02DAA3481A80B3E7FDDB2D
SHA1:	76077DAC4E46F99C7CB91292DD40652515FB2F0F
SHA-256:	F316F8D5CF2786EA2023D7FEE6D0E965E3B882A719A07A920E3EAB1C574F5732
SHA-512:	75A3BF4828E4AEEF672B3AC22A9541EDBF5449F8B86B5C736521DA452DC930A3E6D95A020736B633B3E10B209BA53CCA325631C391ED3CFF426806E50862A40
Malicious:	false
Preview:	2021/07/22-08:00:06.967 1558 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/22-08:00:06.971 1558 Recovering log #3.2021/07/22-08:00:06.974 1558 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.355874962105005
Encrypted:	false
SSDEEP:	12:gRva5KkkOrsFUtpQyZ/PQyz5f5KkkOrzJ:gda5Kk+gGyqylf5Kkn
MD5:	A45BFB6E95711234EE7010FCFCDABCE3
SHA1:	B6087A4A76203E142DDFE7B07C7DB762759374AB
SHA-256:	FB881326A3A5994D43FC8762B0A6329CBED14AB6B0538DE43AB853C8E0ECF9D7
SHA-512:	C06AA2CB7A030F24D101B125DEB28F393A344521268DC54300F535A221EA04A698DC31E26D54480467BB0E0622BDD6B1BA85291C3812D9186001641BCB97375D
Malicious:	false
Preview:	2021/07/22-08:00:19.687 464 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/22-08:00:19.689 464 Recovering log #3.2021/07/22-08:00:19.689 464 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\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	36
Entropy (8bit):	4.377443751081732
Encrypted:	false
SSDEEP:	3:WRKUgtNS7Bkul/XW1ZV:WKckq/G1r
MD5:	39404601C7EA5889F9098D9B6A1266A7
SHA1:	7FC4AC512AAAA55001913337FBC6D152681B21F5
SHA-256:	43CAFFD0EE8027C95B3A0073F287C2DC5446F72EB653D0409FB65D6BDACAB3BE
SHA-512:	BBBD5FF7EC4C4690E0376ACA205F0C7AE42A6F385EF8B2FA60994F1A63CDAEBB357A3DF97079D1CAE989CB31229CCE0E1DC47D0F7D9D0D7CD4F140924BC7 AFF
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Preview:	....24/1.v.....Y.7^.....t;..|0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\05f45425-066d-45e8-bcfd-961c899efd3b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E.....I...k}....{.m.t.CP.....E...\.....=H..,A..,J..;P.....nn p}nnp}.....~~~.....!...!---2---2.. .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P.. .Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e..... ....nnnzXXXa.....RRR\.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	4.0
Encrypted:	false
SSDEEP:	3:SeFcn:Sec
MD5:	61B979ECA159ECAC9C7F8F1D6FD43E9D
SHA1:	0373696351FC2172E811DA8393DEC84036FA34A0
SHA-256:	AB05E0A6FF7E8FFF89F924B279D93AFC72ACCE817C4D250C60BB8059CC534303
SHA-512:	C95825DA33CBDDFA627D9FF9A5B8371BC5F4E643A09573B6E1E839A83B619F53D878C344030B9701DCBC24D4CECCC016CF4D298D10EE8C37D1B5FEC1A5168B6
Malicious:	false
Preview:	F.....r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a4c7b28f-062a-47cb-8bf3-049f70c324ce.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):	2849
Entropy (8bit):	4.888429769717674
Encrypted:	false
SSDEEP:	48:Y2twXGDHz5scARLs6Ts8G+4spkzsnCr1s0yKsxy3zslPMHPsqMHP7syMH5rYhbD:JOXGDHz8Bg+pVCr7dwG7GP3G5shH
MD5:	57002D8FB1CDF45E7BB17A10AA41EF19
SHA1:	F296659DDA65EDF5F6B4533D65AA00F5D9680BF7
SHA-256:	A000DB8AD198131D214799C406A6B398A96E2C0D3F145AB82275DA4A4783ABC0
SHA-512:	701B267E9F8212BF9C671255BF76539CCDE1E9D78293977194CBB01744326FF5C88B189A45733AECCBB3288DE6218EF6564D7809F650478E8F9038D906958D73
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274031611955936","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274031612015441","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274031612277156","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13274031612277160","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b2fbcb0a-75bd-4d7d-b3b8-85cbab9d35b7.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):	1039
Entropy (8bit):	5.56825671473239

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b2fbcb0a-75bd-4d7d-b3b8-85cbab9d35b7.tmp	
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXv27wUSRUenHQ:YI6UUhVseKUewqPeUer2UefIwUyUenw
MD5:	6114B058226731ED53C07C454C002C9B
SHA1:	D82628E7AABD7671D1AAE1DCE1B7A6ACA9840CBA
SHA-256:	DB851346F89BC01D210AA049EF8849C65D27DEFB20090ACB4407ADB863F17A0A
SHA-512:	0EFA36507CB7F9DF2F355A598B469C2154E332E9D02A0F7C85694DF0E11225782D2A976BD9925E8E8AD3E8244C3E79A8383B13D62C4E3CA9E80A66F0761DA38
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1658502011.955994,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626966011.955998},{"expiry":1633014077.462534,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b4b4ed0c-e249-4c38-8e54-fdbae9b9d2af.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):	5491
Entropy (8bit):	5.173524413624703
Encrypted:	false
SSDEEP:	48:Yc0UklSLklwHjUcgMxqAZ1dqI3g51cV54lYqlQKHoTw0RH3CH3G/s8C1Nfct/9BY:n2CT6I1M4RMcKIJok0JCKL8+bOTQVuwn
MD5:	9056237C073070DBD77F796BE354D167
SHA1:	C6CA314A40257D0318181F1ACEA4F3D2A6537697
SHA-256:	025ED0DADF1BAD0B437C71FA8C8EBE3B9CF247145F40A921E6F49216F4F6A610
SHA-512:	30F3E6E3C6BABBCB0F4C4CBC2BAAD75DD8A37F5AD0CA2CB6817F5C68AE9122659B812FBC68D53F27EF41B52A65C9C241EEE51E9BDD367725A908B5D246F2A719
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271439607306792","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d2f31c47-e661-46f6-9289-42ecf1b85673.tmp	
SHA-256:	5751F88A6A9AF7A62C65C12D5300876C3893E071B310B060F28DFB748AE70846
SHA-512:	1148B9CF8EFAE9EE82A4A89406864206E4DFAE6D24F83FBC3A46F274C6C4F0882D774F6E027153ABF64A8E41339ADFF1F7788CF65B96567E3FE457BA8EC6C13D
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13271439606957434","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.544231271231136
Encrypted:	false
SSDEEP:	3:tUKIH1RFdBG11Zmwv32HpFdwFWSV8s2HqMkSWGv:mp1ZcZmwPQpLwkSVvQMStv
MD5:	21D7C3A8FD7ACB1589132802B2CE4045
SHA1:	C459B31E2943D8A4534A630F56339D564E013B94
SHA-256:	58C6D4100A1103E455906F6BAAA91283E6BD8EA67B362E8A3F2B1ABCE6550085
SHA-512:	8DE63D4523D91C99C0C2CC2AFB996DDDDDD3A079D1213332F88FBAF0F07478EC3FDC88F65175E0B35B5C36004E414E15F5F9AF3282D01E6C09D4475DF796B53
Malicious:	false
Preview:	2021/07/22-08:00:17.554 1adc Recovering log #3.2021/07/22-08:00:17.611 1adc Delete type=0 #3.2021/07/22-08:00:17.612 1adc Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dfbfbe9a-9457-476a-99c4-c6cc36b12e5d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dfbfbe9a-9457-476a-99c4-c6cc36b12e5d.tmp	
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.5774831947778925
Encrypted:	false
SSDEEP:	384:/iEtGLlKBX01kXqKf/pUZNCgVLH2HfDPrUmQi4m:cLlu01kXqKf/pUZNCgVLH2HfDrUBiR
MD5:	6B07B841398A78CE74D55BFF8E58FB42
SHA1:	D0AF9148BE288EDB13F3627BEC9EDE54EADDC0C8
SHA-256:	3B259B5E1140001F9204F3BD59B37F52A2DDA1A81CBC9CFE4E985C139A8866B3
SHA-512:	AD185CFE9BCC49439474D28E4365970F9A47AEBE16A58B173404BD06550D420442CF2FEB718DCF51ADF823492CC90E084A9B913629E3510F704EB00C309F091E
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13271439606957434","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.182860838498332
Encrypted:	false
SSDEEP:	6:mpX9+q2PWXp+N23iKKdKfrzAdIFUtpQnNJZmwPQnN9VkwOWXp+N23iKKdKfrzILJ:gX4va5Kk9FUtpQNJ/PQND5f5Kk2J
MD5:	6DB90C4AFF13F8CA73B0F6B9B827E70F
SHA1:	8B77540887C83B494342C472A1D7D16306C78BA8
SHA-256:	0A6FE8ED399DBFC6CA1F5EDB2A803956F2C49BB35E34474D53F053657390DE7D
SHA-512:	8FDAEDF1C102EAF8FF5B960CE56106466D5FEAE38F4A4DCD44E93F9B9AD7A92414CB8FEA0C0C1D33BF42585BEC381D275E0F9CA8B2557AC109CE352B7686DEE7
Malicious:	false
Preview:	2021/07/22-08:00:17.940 1428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/07/22-08:00:17.942 1428 Recovering log #3.2021/07/22-08:00:17.942 1428 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8EflZq:8
MD5:	F38CDBE1C86767A8E43CA2AD015A83EE
SHA1:	A551DF27C06AD007EB8C10BB434C9FFA7203500F
SHA-256:	DFC6CB1AAAA9B9CE08C1A4D704965EB3515140419928179879980A2A49DC28459
SHA-512:	7792426F37D22DEBCD97757C6693E24B3BA2CE05CD825DBF664CF2A710C75AC3AB8EE1DC2E74B78CEDBCE78EDAE3B82EEB237FD5E8EE83DE8F206AE65CF780DC
Malicious:	false
Preview:	.'..(.....6.M&/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.28.0\Indexing in Progress	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir5028_324214516\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	186784
Entropy (8bit):	4.915957886381836
Encrypted:	false
SSDEEP:	3072:bl35PHEWQyoghJbTloZq6L45c7wbMn5nezpiKmneSxCgWCCkHjuhjMQBJXS:R3NKghJbTl96BXTChW
MD5:	E4ED6CE0DB78ED18701755E5FF177B82
SHA1:	7D660E76CE91C05FC52FE1AD54C28EAD7E4A04B6
SHA-256:	BBA545E82F5720A1AD3BCB3743EB27BB1F015CB2E1222615CB880DA40CE42C20
SHA-512:	F49A4487C245DE86158EE6BD675BF70C74D8FE7164A5AA5D71469AFA94071FD4C06BB09E88E06B1CCDE9ADE6C124C957E45179C25891E12BD7C9FD419B7EBF72
Malicious:	false
Preview:	.....$...(.....\.....p.....P.....,.....geips..... /.....lgoog.....6.....ozama.....onwod.....Hi..(.....g.bat..... <q..@.....uotpo.....w..X.....ennab.....S..p.....nozam.....E..h....^.....t.....L.....$.....x.....|...l...h...d...`...\...X...H ...P...L...H... ...@.....4...0...,..(...$... .....h.....(.....\|.....t...p...l...h...h...`...H...X...T...$. ..L...H...D...@.....8.....,..(...$... .....p.....4.....|...x...t...p...l...h...d...`...\...X...T...P...L.. .H...

C:\Users\user\AppData\Local\Google\Chrome\User Data\a841512c-9373-4cae-b1d7-25fcfc262efb.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):	166404
Entropy (8bit):	6.050697141222643
Encrypted:	false
SSDEEP:	3072:ukZExZKKJEuwA4x37SiHnDcWYKWF8FcbXafIB0u1GOJmA3iuRY:NExzgRx37iWYFMaqfIlUOoSiuRY
MD5:	C21F76570ACB0B7C18494CAEA8A21A65
SHA1:	B1E284C8A67F8C414568EBBDFF5C5CACF1F2A6AE

C:\Users\user\AppData\Local\Google\Chrome\User Data\a841512c-9373-4cae-b1d7-25fcfc262efb.tmp	
SHA-256:	7F718E130742BCB2CD53A10498FB428D42ACF913F8DE9C473F2DF4E746CF886E
SHA-512:	486A44C4ABE5A6FFE3DFE61BF024BAF06E8D81160B428ECADFE966015CEA6F7D62C3AB2610FB3AA68D35800A4EFDB192220855781274A49DF3C89707C5F7BF/0
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":1.626966010115265e+12,"network":1.626933612e+12,"ticks":6186119719.0,"uncertainty":4946474.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAA AAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRh NbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyX OajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1

C:\Users\user\AppData\Local\Google\Chrome\User Data\a9830303-7a35-4348-bc4b-8662085c1b23.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.743019451231429
Encrypted:	false
SSDEEP:	384:33ReWoLRA0jqNNGrDvai3py8BHMpGdErf8agxRMQEzrLamHMPMuuSNOUAuNP1ena:7mxpy8dVgeXsGYofX2SKkCOhJ
MD5:	9152D483D9AE990A4B81018679FCF2E0
SHA1:	76B3168A72CCF4CF271F0AE6F135AA88D86A2B68
SHA-256:	D51574C27C3330261873494C12E2BFB9543CBF980A83211B68896A4287E7E605
SHA-512:	18B0BE276C43CE271E795F47F13D2291F218E2D40CB6C908E5429822861AE8866E6C7487CA307DF7A4E57B355E3CCB9B8D66EA0B8F85B05A7A1C2790A001A8D
Malicious:	false
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...o@8.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\b0f211eb-9450-4a98-a484-ed895fa5cfbc.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):	174421
Entropy (8bit):	6.079219909818137
Encrypted:	false
SSDEEP:	3072:PhBkZExZKKJEuwA4x37SiHnDcWYKWF8FcbXafIB0u1GOJmA3iuRY:JIExzgRx37iWYFMaqfIlUOoSiuRY
MD5:	603772DCE474200D66817DF84C3877B1
SHA1:	289BB950E97CE2C60FFA0016CE489F00C82E5826
SHA-256:	92D208BAD060D39FFD2F37909E6EC80207A9926B34BB6D79A029BC0900A3DA43
SHA-512:	6B7CC56DABB16282174049FE16FE59A4E861A07A8A228BEC2C3DBF28DFD3220D6FEAF9BCF4DF8B6662AFB36A224F91F805D2793C2ABB02C4C38B8DBEDCCC4E91
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":1.626966010115265e+12,"network":1.626933612e+12,"ticks":6186119719.0,"uncertainty":4946474.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\ccdb9b69-5c7f-43a4-adde-7c005c6843af.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7435340900911176
Encrypted:	false
SSDEEP:	384:h3ReWoLRc70KVDlqNNGrDvai3py8BHMpGdErf8agxRMQEzrLamHzxPMuuSNOUAuE:Jemxpy88VgeXsGYofX2SKkCOhS
MD5:	895CE2F947875991C50F576016AF0A0B
SHA1:	9B6B45A5B208671923E0BD54737D56E0BB557605
SHA-256:	460BB3869A39DA86E3F5633C94D0CAE08BD2CD0273F0B8EA2078C91717B8C623
SHA-512:	5742393DF2C20C5D258654E3009866EFEE9C5DFEA83970D6CFC12F54960C741A24EA7F2320FBB5978B484A118C67878EA44BC4E0295E660D31452CFE6F2A1125
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\ccdb9b69-5c7f-43a4-adde-7c005c6843af.tmp	
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...o@8.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\eaf7b720-6d04-4dbc-9886-3467fcd7c0c4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7434171232364073
Encrypted:	false
SSDEEP:	384:x3ReWoLRc70KVDlqNNGrDvai3py8BHMpGdErf8agxRMQEzrLamHMPMuuSNOUAuNj:5emxpy8dVgeXsGYofX2SKkCOhH
MD5:	0EA45A0262018D1EE4EACD8B14F3C7C3
SHA1:	7BD31E15325235A1B10E7CA64298505742B54ECE
SHA-256:	AD39D510C9AF7565EE436EEB25DEE948B7AACB8D8E4D089F94EDD817B0877970
SHA-512:	F1C408F28EA7BA407F1B11AE18AE4439EB6C4FF0A9BC66774AD0DC59F72DC70EFF9B974C741A5E9985D1C0A71CE06EA1FE4F4979CDBD817CD94D195ED21AA 3CD
Malicious:	false
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...o@8.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\ed6bc138-5966-4a05-8380-b2d0d5b8e105.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):	166247
Entropy (8bit):	6.0501717851867065
Encrypted:	false
SSDEEP:	3072:3kZExZKKJEuwA4x37SiHnDcWYKWF8FcbXafIB0u1GOJmA3iuRY:+ExzgRx37iWYFMaqfIlUOoSiuRY
MD5:	625BF3D93712230CE67859CA47369A3E
SHA1:	9809B9D3AC7400EFC220ED82E3ACF6566C48A657
SHA-256:	03A823967D9BEC752AFCC47B02AAFEC61D1684A6ACE57E1DFEC7E89AA82AC143
SHA-512:	20024466E8543CEAB6641A250D73575590EFEF7B3F9FCAD54323B50B1DB8A020B34D4827AEAB900AA870AF920E8A4DA3FA99DA57716C18DD7A846B9235F53DD 5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.626966010115265e+12,"network":1.626933612e+12,"ticks":6186119719.0,"uncertainty":4946474.0}},"os_crypt":{"encrypted_key":"R FBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_ma nager":{"os_password_blank":true,"os_password_last_changed":"13245951016952416"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\f8a7aa67-58f1-4f38-9883-580ed163aec2.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):	174421
Entropy (8bit):	6.0792196794537885
Encrypted:	false
SSDEEP:	3072:PcmkZExZKKJEuwA4x37SiHnDcWYKWF8FcbXafIB0u1GOJmA3iuRY:0FExzgRx37iWYFMaqfIlUOoSiuRY
MD5:	747FEF5C2B7706122D825387364629E1
SHA1:	F0B53D2B6D01C699F02779FBBC0E2DABB55BB19E
SHA-256:	6AA8C31B1470F848FADB7C33DB87334D3B4AC7BBC7DD19A6172640C13E65ED73
SHA-512:	8DA57955C7C092250B5389614182B23DEEED905D856963B936170C38D685C5C7E9EE96740B37B0D7E88702E5DB80E9C56E2F8A4B31C9BCAB5110B0340EB30EB
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\f8a7aa67-58f1-4f38-9883-580ed163aec2.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626966010115265e+12,"network":1.626933612e+12,"ticks":6186119719.0,"uncertainty":4946474.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Temp\0150fb22-30bd-4262-bc51-ee86ac4729a1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\09aedfaa-844a-4b09-b7f2-67bd54886fdc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...'].....+A.....u....k...e..&..I.6r[yU...%..f.....N..V.....<+.....I..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\30348599-f928-43f7-9724-30f649f91eca.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\32094c79-ff7e-493b-85bd-793d1e78fb1e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531

C:\Users\user\AppData\Local\Temp\32094c79-ff7e-493b-85bd-793d1e78fb1e.tmp	
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LlP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\5028_1643468988\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9570514164363635
Encrypted:	false
SSDEEP:	3:SVCBGERJd9WaHpYx4eiXoA:SVCwERJdVMiXd
MD5:	C6ABF42CB5AF869629971C2E42A87FD5
SHA1:	6EB0FAE28D9466E76FA12E31FE6CDADD3ACCE4D1
SHA-256:	D281AFDA759075F4CB7D7CEEC4A3CB2AF135213B4D691F27090E13F238486AD1
SHA-512:	EDDF7E4883E82718743C589E8F2E48BEAD948428E730231FEFADAD380853343332BC56C9DC61C963B3F537CD4865B06FF330CEF012B152CEA35F8A0AA2C7B56D
Malicious:	false
Preview:	1.fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace

C:\Users\user\AppData\Local\Temp\5028_1657145117\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9301659996057974
Encrypted:	false
SSDEEP:	3:SXlpS0VHAgzlURX/PVdAwtL:Si0G5X
MD5:	FF0CBA325E01ED1EAE9021FBC02D3362
SHA1:	ADD06DA6B8FF5D8234EE155166C7498A5CFF8977
SHA-256:	CBD1231298B252479D8A63155A8FC0CFBC94AC5E8F74D93C683BC182CA3EA245
SHA-512:	7420B818C45FE804ABA451687DADCFD18A80FCF43F5D783D0BCEFC77191C716374B5F4F7989469FF0BEAC422DA75FC534E71ECD8BFC38EF51ABAD42913C3A956
Malicious:	false
Preview:	1.2731bdeddb1470bf2f7ae9c585e7315be52a8ce98b8af698ece8e500426e378a

C:\Users\user\AppData\Local\Temp\5028_2025115243\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9029938937928734
Encrypted:	false
SSDEEP:	3:ST1HTRWzccXBpy1CcYgy:SxHoIfXy
MD5:	47D76975618B8F3256F4CD7FA94C37AB
SHA1:	4496F70B0A44B33C15B1AECEAEAF7D8E8F4EE197
SHA-256:	FAD49B3586ABA84BD8239D25EF5ED27C7BF552A56AFF2B9438B3D9D551A228AE
SHA-512:	7EF8A13685078E5D08EFB5C8C265ED732053750D006D62F0E700898681AF607C02D0A4F91B88F574DFD0EAE0D5DAA75647307EDBC062DD3A5DB864BD541B93CD
Malicious:	false
Preview:	1.694636bbb2f68d5629d1e4a499aabd2d82f93c95c49c20e270b301d94cae333a

C:\Users\user\AppData\Local\Temp\5028_26295858\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

Static File Info

General

File type:	HTML document, ASCII text, with no line terminators
Entropy (8bit):	4.911149580990165
TrID:	• HyperText Markup Language (31031/1) 100.00%
File name:	Westernunionreceipt711 ___vaw.html
File size:	197
MD5:	e43b99fcb58eef1969c8ab9b2ede9404
SHA1:	3038d1bb1f1f23d2e047fe33780815cf7e62ce18
SHA256:	ed68eb96911f17d8750e57133b7016efa2f4a9d2a368c47ae9ae77003af1f861
SHA512:	89afd5e1aa477679f38e125a501aa745fb807f1d21ad985d6b5a7fc32e1b0eeae3ec92f4ec4bb717f9d69747df5467d45414913f48376b6bd6a587dffe69a3cb
SSDEEP:	6:7AqJm7+mkdGRoQXXtTREmgizIXXfEIMl2gb:EqJm7+BGRoQHtmSZb
File Content Preview:	<script type="text/javascript">window.location.href ="https://advantpac.com/office/voicemail/fetch/validate/session/3e4c-5f1a-bb7e-faff-60e1-a31b-c6d4/?email=waley.huang@westernunion.com";</script>

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 08:00:11.614839077 CEST	192.168.2.3	8.8.8.8	0xf237	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:11.617360115 CEST	192.168.2.3	8.8.8.8	0xa0dd	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:11.621053934 CEST	192.168.2.3	8.8.8.8	0x512e	Standard query (0)	advantpac.com	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:13.085411072 CEST	192.168.2.3	8.8.8.8	0x5dc6	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:15.312527895 CEST	192.168.2.3	8.8.8.8	0x3ca6	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 08:00:17.914249897 CEST	192.168.2.3	8.8.8.8	0x5cca	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 08:00:11.677246094 CEST	8.8.8.8	192.168.2.3	0xa0dd	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:11.681721926 CEST	8.8.8.8	192.168.2.3	0x512e	No error (0)	advantpac.com		104.21.40.98	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:11.681721926 CEST	8.8.8.8	192.168.2.3	0x512e	No error (0)	advantpac.com		172.67.183.212	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:11.693965912 CEST	8.8.8.8	192.168.2.3	0xf237	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 08:00:11.693965912 CEST	8.8.8.8	192.168.2.3	0xf237	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:13.136163950 CEST	8.8.8.8	192.168.2.3	0x5dc6	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:14.560502052 CEST	8.8.8.8	192.168.2.3	0x17a1	No error (0)	gstaticadssl.l.google.com		142.250.186.163	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:15.376076937 CEST	8.8.8.8	192.168.2.3	0x3ca6	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)
Jul 22, 2021 08:00:17.974056005 CEST	8.8.8.8	192.168.2.3	0x5cca	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 08:00:17.974056005 CEST	8.8.8.8	192.168.2.3	0x5cca	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5028 Parent PID: 968

General

Start time:	08:00:06
Start date:	22/07/2021
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\Westernunionreceipt711 ___vaw.html'
Imagebase:	0x7ff77b960000

File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: chrome.exe PID: 5624 Parent PID: 5028

General

Start time:	08:00:07
Start date:	22/07/2021
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=1540,9784536074538328282,17911257635406631719,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1716 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

Copyright Joe Security LLC

Copyright Joe Security LLC 2021