



ID: 452312
Sample Name: Remittance.html
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 05:22:39
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Remittance.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 6
URLs 6
Domains and IPs 6
Contacted Domains 6
Contacted URLs 6
URLs from Memory and Binaries 6
Contacted IPs 6
Public 6
Private 6
General Information 6
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 7
IPs 7
Domains 9
ASN 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 39
General 39
Network Behavior 39
Network Port Distribution 39
TCP Packets 40
UDP Packets 40
DNS Queries 40
DNS Answers 40
HTTPS Packets 41
Code Manipulations 41
Statistics 41
Behavior 41
System Behavior 41
Analysis Process: chrome.exe PID: 4168 Parent PID: 2592 42
General 42
File Activities 42
Registry Activities 42
Analysis Process: chrome.exe PID: 672 Parent PID: 4168 42
General 42
File Activities 42
Disassembly 42

Copyright Joe Security LLC 2021

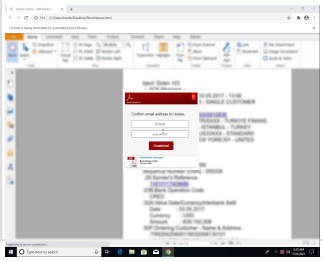
Windows Analysis Report Remittance.html

Overview

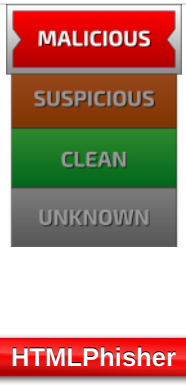
General Information

Sample Name:	Remittance.html
Analysis ID:	452312
MD5:	1dd3d108e04a63..
SHA1:	f4efed64ae98943..
SHA256:	bbde5d42af6fd69..
Infos:	

Most interesting Screenshot:



Detection



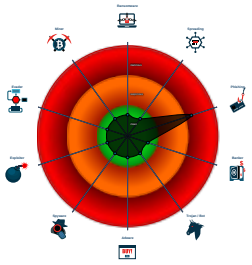
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish10
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4168 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\Remittance.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 672 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,10324375867687729821,3875551371938988928,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Remittance.html	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Phishing:

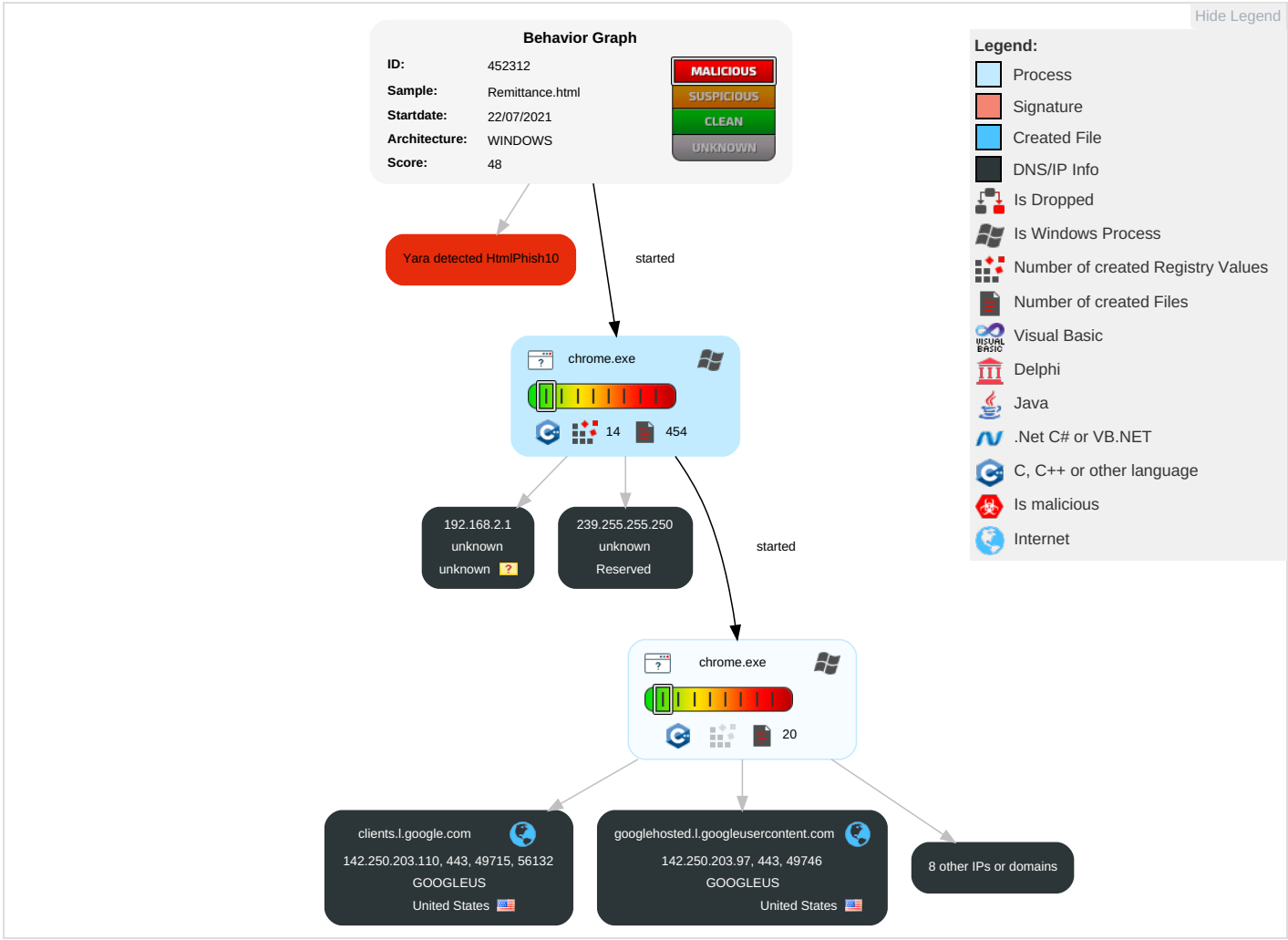


Yara detected HtmlPhish10

Mitre Att&ck Matrix

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

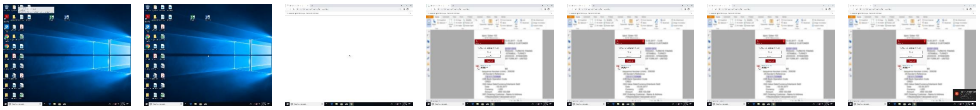
Behavior Graph

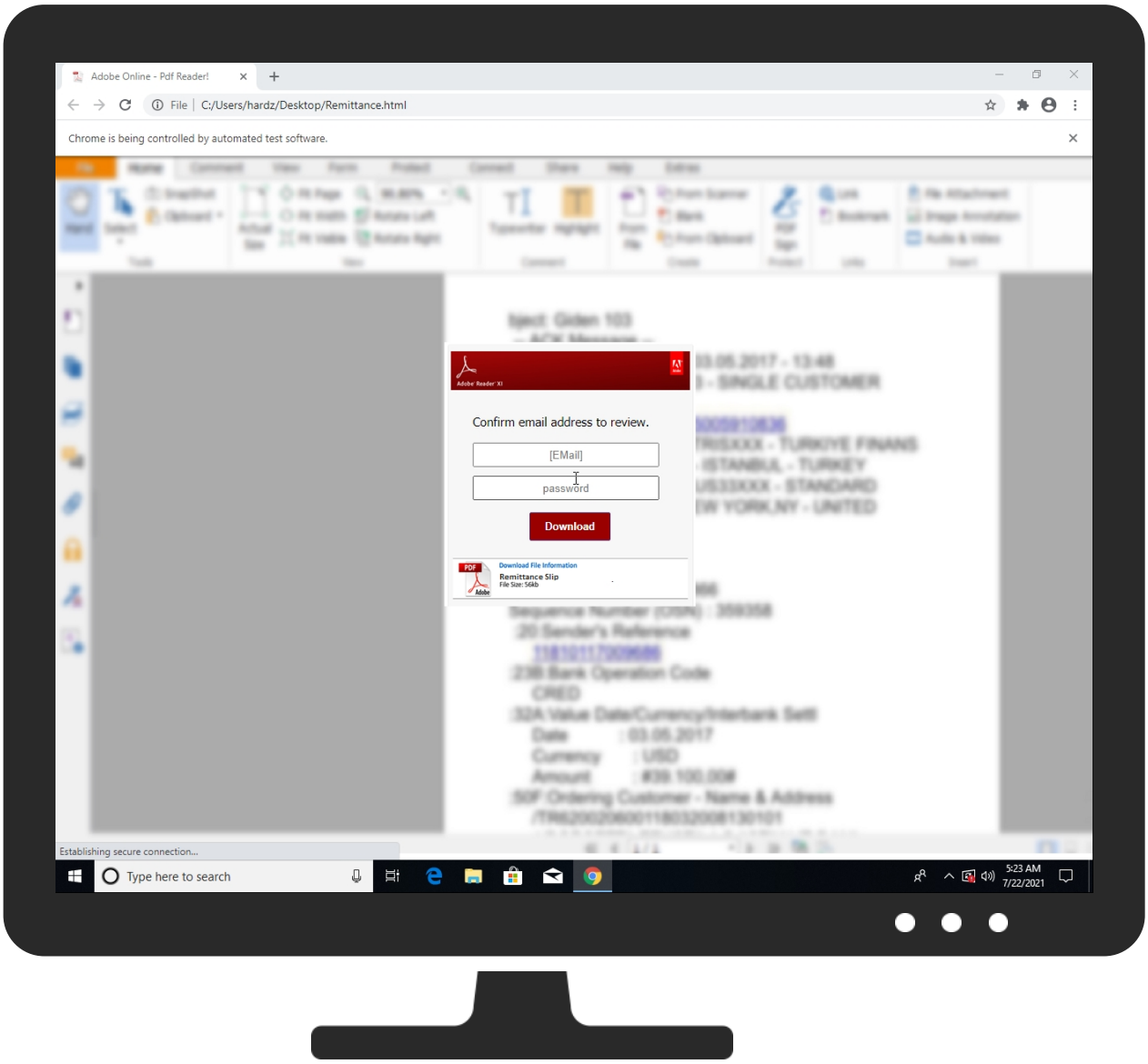


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Remittance.html	4%	ReversingLabs	Document-HTML.Phishing.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Copyright Joe Security LLC 2021

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://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	50.16.239.65	true	false		high
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.16.18.94	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
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/Remittance.html	true		low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.16.239.65	elb097307-934924932.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
142.250.203.110	clients.l.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
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452312
Start date:	22.07.2021
Start time:	05:22:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Remittance.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:	29
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@35/184@5/8
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
05:23:31	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
239.255.255.250	DHL Documents.html	Get hash	malicious	Browse	
	2DAAD8278E0DDD4D247303ACED4B1D41C75CE94BE3A9E.exe	Get hash	malicious	Browse	
	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	

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Cx9ER7vYGi.exe	Get hash	malicious	Browse	
	Emilemercier ProtectedCall.htm	Get hash	malicious	Browse	
	INV #95000987.html	Get hash	malicious	Browse	
	Joelle#310712.html.txt.html	Get hash	malicious	Browse	
104.16.18.94	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://rva.fonotecanacional.gob.mx/preview-assets/css/smoothness/reports/chron_import.php?spent=1s0xppx5zxx96n&science=sun&round=hand	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2XaOiGR	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bitly.com/2Xaw8VA	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://j.mp/3rJBANn	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://www.rekmall.net/.well-known/acme-challenge/act_contactar2/admin_cat/mgc_chatbox/information-12/pspbrwse.php?sit=ervw1yb1atp20npd0&remember=quiet&feel=sleep	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://rassrochka.rusfishcom.ru/wp-snapshots/mailpage/information-66.php?sit=11kdh2bsq0r0z&bright=afraid&produce=sets	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bitly.com/3nmYKXc	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://j.mp/2URXSx8	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/33I4Nht	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2Gwx0iC	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/3jDHDOo	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://Kardanan.com	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/datamaps/0.5.8/datamaps.all.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	0706_1643278086845.doc	Get hash	malicious	Browse	• 54.225.78.40
	123.dll	Get hash	malicious	Browse	• 50.19.92.227
	DDA9.dll	Get hash	malicious	Browse	• 23.21.168.151
	4fZX8fJwHn.dll	Get hash	malicious	Browse	• 54.235.190.106
	Drawing for New Purchase Order.exe	Get hash	malicious	Browse	• 23.21.224.49
	triage_dropped_file.dll	Get hash	malicious	Browse	• 54.243.175.83
	265.exe	Get hash	malicious	Browse	• 54.243.175.83
	7QC4uSmZCg.exe	Get hash	malicious	Browse	• 54.225.78.40
	ter.dll	Get hash	malicious	Browse	• 23.21.224.49
	WSn11SBJ55.dll	Get hash	malicious	Browse	• 50.16.216.118
	aIY9sQv1qW.exe	Get hash	malicious	Browse	• 23.21.224.49
	ier.dll	Get hash	malicious	Browse	• 23.21.173.155
	0714_2313552213.doc	Get hash	malicious	Browse	• 54.225.165.85
	0714_1242782601.doc	Get hash	malicious	Browse	• 54.225.165.85
	T20009002.exe	Get hash	malicious	Browse	• 54.225.78.40
	VvwylSyPeD.dll	Get hash	malicious	Browse	• 23.21.224.49
	6kZeSToEoa.dll	Get hash	malicious	Browse	• 50.16.220.248
	QJLwL56Pag.exe	Get hash	malicious	Browse	• 54.225.245.108
	120.exe	Get hash	malicious	Browse	• 50.16.226.23
	ter.dll	Get hash	malicious	Browse	• 23.21.224.49
cdnjs.cloudflare.com	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.16.18.94
	Yaharasoftware.com_Fax-Message.htm	Get hash	malicious	Browse	• 104.16.19.94
	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
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.16.18.94
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.16.19.94
	Pointids.ca_Fax-Message.htm	Get hash	malicious	Browse	• 104.16.18.94
	Globalfoundries.com_scanned_file.htm	Get hash	malicious	Browse	• 104.16.19.94
	Seic__-Do__cu__me__n__t(s)__.HTM	Get hash	malicious	Browse	• 104.16.18.94
	RemittanceAdvice617492.html	Get hash	malicious	Browse	• 104.16.18.94
	Dir.texas.gov_scanned_file.htm	Get hash	malicious	Browse	• 104.16.18.94
	#Ud83d#Udd0ajs_msg_ 3pm.html	Get hash	malicious	Browse	• 104.16.18.94
	Kay Supply, Inc. REQ 009046.html	Get hash	malicious	Browse	• 104.16.19.94
	Globalfoundries.htm	Get hash	malicious	Browse	• 104.16.19.94
	James.sowinski.html	Get hash	malicious	Browse	• 104.16.19.94
	INV_289553.html	Get hash	malicious	Browse	• 104.16.19.94
	htmlattachment.htm	Get hash	malicious	Browse	• 104.16.18.94
	htmlattachment111.htm	Get hash	malicious	Browse	• 104.16.19.94
	#Ud83d#Udd0aMsg_ 3pm.html	Get hash	malicious	Browse	• 104.16.18.94
	(5) Domesticandgeneral MPYV-DTG.html	Get hash	malicious	Browse	• 104.16.19.94

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	ZlvFNj.dll	Get hash	malicious	Browse	• 3.223.192.20
	bPAMfuy9oa	Get hash	malicious	Browse	• 107.23.89.187
	U4r9W64doy	Get hash	malicious	Browse	• 54.61.104.90
	C4PozjQdGE	Get hash	malicious	Browse	• 54.131.116.216
	kb5IbEJU8c	Get hash	malicious	Browse	• 54.2.185.151
	CefN2XNyFi	Get hash	malicious	Browse	• 54.54.164.140
	MD5OxTSc6i	Get hash	malicious	Browse	• 54.14.140.106
	jy7J855bNO.exe	Get hash	malicious	Browse	• 3.211.138.232
	SUpODCSauS	Get hash	malicious	Browse	• 44.207.177.58
	iUmNR6tkEd	Get hash	malicious	Browse	• 54.55.106.195
	LDWhPg4vRM	Get hash	malicious	Browse	• 44.200.82.226
	0706_1643278086845.doc	Get hash	malicious	Browse	• 54.225.78.40
	123.dll	Get hash	malicious	Browse	• 50.19.92.227
	triage_dropped_file.dll	Get hash	malicious	Browse	• 23.22.217.86
	AUFFFNSdKy	Get hash	malicious	Browse	• 34.202.219.235
	kw7HGENm1D.exe	Get hash	malicious	Browse	• 3.92.185.198
	TFG18FA4eD	Get hash	malicious	Browse	• 44.214.154.33

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	StyBaUxNYq	Get hash	malicious	Browse	• 52.73.216.92
	qgQgEjI283	Get hash	malicious	Browse	• 100.24.228.158
	jhUxzb7jPW	Get hash	malicious	Browse	• 34.205.150.10
CLOUDFLARENETUS	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
	ORDER SKYMET 847759 REVISED PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	Cotizaci#U00f3n.pdf.exe	Get hash	malicious	Browse	• 104.21.6.222
	Specifications_Details_20330_FLQ.exe	Get hash	malicious	Browse	• 172.67.188.154

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	Convert HEX uit phishing mail.htm	Get hash	malicious	Browse	• 50.16.239.65
	IPVrDRKfYj.exe	Get hash	malicious	Browse	• 50.16.239.65
	_VM_1064855583.HtM	Get hash	malicious	Browse	• 50.16.239.65
	INV #95000987.html	Get hash	malicious	Browse	• 50.16.239.65
	ATT74992.HTM	Get hash	malicious	Browse	• 50.16.239.65
	5cksYFGC2g.exe	Get hash	malicious	Browse	• 50.16.239.65
	ATT59696.HTM	Get hash	malicious	Browse	• 50.16.239.65
	ATT59696.HTM	Get hash	malicious	Browse	• 50.16.239.65
	jYzWBKTsxE.exe	Get hash	malicious	Browse	• 50.16.239.65
	ATT25402.HTM	Get hash	malicious	Browse	• 50.16.239.65
	ATT62725.HTM	Get hash	malicious	Browse	• 50.16.239.65
	WAdStf9Llw.exe	Get hash	malicious	Browse	• 50.16.239.65
	RemittanceAdvice617492.html	Get hash	malicious	Browse	• 50.16.239.65
	qET1iJuly 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 50.16.239.65
	July 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 50.16.239.65
	Statement & Remittance advice 07.13.21 - Copy.htm	Get hash	malicious	Browse	• 50.16.239.65
	07xufnlKWd.exe	Get hash	malicious	Browse	• 50.16.239.65
	Machine Service.xlsx	Get hash	malicious	Browse	• 50.16.239.65
	Machine Service.xlsx	Get hash	malicious	Browse	• 50.16.239.65
	#Ud83d#Udd0ajs_msg_ 3pm.html	Get hash	malicious	Browse	• 50.16.239.65

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331

Copyright Joe Security LLC 2021

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.l.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$...._Y..Y`&..s.1.....s.{.,,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...l.....D0.....Ba...Z.0.o..l.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1392054451166236
Encrypted:	false
SSDEEP:	6:kKn15qdoW+N+SkQlPlEGYRMY9z+4KlDA3RUelID1Ut:f1I5kPlE99SNxAhUe0et
MD5:	F93381399BD9AB19E0884D11E2F93BAB
SHA1:	56615A608F590090CB49FAF50AE849368879B5AD
SHA-256:	F87751CF42F06B4E4C5E4105E54D3967D9BBA19637E4D90E40907EA47E3A3BBF
SHA-512:	174BEDF02CC7C171093F921D3E449133889C29743A60C0B03153A29046A868C7B7077A45898859946CFF50203C350B57FED3E375F1261FFAD54D0C2F6758DB74
Malicious:	false
Reputation:	low
Preview:	p..... .....b.~..(..... ..... T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.::.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\160fe46c-79d7-4b2f-838e-2d2e23a89a8b.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):	166056
Entropy (8bit):	6.049735030563403
Encrypted:	false
SSDEEP:	3072:9FkZExZKKJEuwA4x37SiHnDcWYKWFRFcbXafIB0u1GOJmA3iuRA:9UExzgRx37iWYFhaqfIlUOoSiuRA
MD5:	E788EBC1353EFD510B231B7CE637D3E1
SHA1:	58F770F938A9039893653770A3F368638276DD17

C:\Users\user\AppData\Local\Google\Chrome\User Data\160fe46c-79d7-4b2f-838e-2d2e23a89a8b.tmp	
SHA-256:	B823D37211B7687EDE0992B021AAAF7BDD43B00EAEBD26E2A6D3A39B121AC218
SHA-512:	972C80344E7B5C0542B23F67F9B9A6C53268FA37FA3368547A24874EB0B06D7ED583EFEB1A842ABD0A2CBC7549F6B7C50FFF124833F3B7D919DD0D2985D9FF2
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":1.626956608543805e+12,"network":1.626924211e+12,"ticks":5491858375.0,"uncertainty":5181276.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016170022"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\2e276980-3526-4afe-9036-aaa2ebad6b68.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):	174420
Entropy (8bit):	6.0792099919773905
Encrypted:	false
SSDEEP:	3072:7+EkZExZKKJEuwA4x37SiHnDcWYKWFRFcbXafIB0u1GOJmA3iuRA:CLExzgRx37iWYFhaqfIlUOoSiuRA
MD5:	BA737CDBFEB55A318D0753E313FCEFB1
SHA1:	A693942A7DC266B54E8FD917B9397C0306E56E75
SHA-256:	B198830769059E6F9A06B83CC988A07B32F2BC9A7173E7AF9D35E4070434E099
SHA-512:	891154036BFE98EE70F26AA0CCE59BBEFE200816DD5EADE31DF3C89CBF88689FE57E6241CCB5F1C01E32E23F89C749A1C6948B6C161C170E34EAD1BF60523B4B
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":1.626956608543805e+12,"network":1.626924211e+12,"ticks":5491858375.0,"uncertainty":5181276.0}},"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\Google\Chrome\User Data\2e932043-0a5d-4e3a-b858-f1f78a86f7a3.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):	166246
Entropy (8bit):	6.050198137765541
Encrypted:	false
SSDEEP:	3072:DQkZExZKKJEuwA4x37SiHnDcWYKWFRFcbXafIB0u1GOJmA3iuRA:D/ExzgRx37iWYFhaqfIlUOoSiuRA
MD5:	BC020D76FDADB28577E1E8CAEA6324B9
SHA1:	5E161858924E3C687C2F13D26E7C28BC120F4BDC
SHA-256:	0EAB0C447CCDD5416DEDDDAA6F70E57151BC385216F9EB0FA7C0FB789467B609
SHA-512:	8D26D275CD314AFECF33B0FBF9DBA5467559F5C7B0760EBFF641F0CA4718D7151F2AB087A1154BEF7F6F0830ECF272BAF6DAD4E01EC14A21440875B84308520A
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":1.626956608543805e+12,"network":1.626924211e+12,"ticks":5491858375.0,"uncertainty":5181276.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016170022"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\3785b700-a36f-40a8-b091-37691a01001c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.74574090881733
Encrypted:	false
SSDEEP:	384:FbkLzxOcJi9BVawXeN3rUvjp3MbVsHFIG4XridbjxU1xZArq3my1ep3TvcO9t7Nl:RCa9tSpU8Meb/xdcPL+RKvpzpF
MD5:	D1DA870B77BDC5FEEBCF34716A77CA3D
SHA1:	926084B1AFBD92A38A6FF09736F3937DD92704F2

C:\Users\user\AppData\Local\Google\Chrome\User Data\3785b700-a36f-40a8-b091-37691a01001c.tmp	
SHA-256:	BCDC701B717B8E53FC04EAD36C285C6644BF405D912720F04FD592B5F700B6D1
SHA-512:	778AC8D4103E9AE85361E422C4D381AA664A42A407B6C94040DCBF8138BC7382CB11A279F69D214525D4FFA9BB11F0667ECDF487FE4B9C4BC57C9255B4D1AFD
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...l@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\4049c86f-6edd-42e1-80e3-26d18c0f2297.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):	174420
Entropy (8bit):	6.07920845999673
Encrypted:	false
SSDEEP:	3072:2+EkZExZKKJEuwA4x37SiHnDcWYKWFRFcbXafIB0u1GOJmA3iuRA:fLExzgRx37iWYFhaqfIlUOoSiuRA
MD5:	07D3CE0C8324477792153CF3546F466A
SHA1:	4D7E34CAC2CE75786CC7144D771AF6D7BD218EC0
SHA-256:	414B920D753B628316F24112497FAC17F3E93EF96F33FB39D3A7FE4F26D59BC1
SHA-512:	CFFBEFAD878DB09F8B4D7C824E4E858AE0A4DB1FE7E8AF79FE07ABBDDDF9BCB22CF525564C591D450CAACDC3E041427165A7368B9BCAB245E95A283E4990I 7FF
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":1.626956608543805e+12,"network":1.626924211e+12,"ticks":5491858375.0,"uncertainty":5181276.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016170022"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\581c149b-c2e9-41a0-9c4d-5a6f6a726f13.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	165962
Entropy (8bit):	6.049456388242606
Encrypted:	false
SSDEEP:	3072:9dkZExZKKJEuwA4x37SiHnDcWYKWFRFcbXafIB0u1GOJmA3iuRA:9MExzgRx37iWYFhaqfIlUOoSiuRA
MD5:	039779E5B26C66305B07357D348E5B65
SHA1:	DEA5C50210681FA1520064D04EA6BDAE55CC23E5
SHA-256:	7DFCA8B9583A4491C33CD962C9A905D56C78A3CEB24D5ED68D644E931CEE9781
SHA-512:	68793DB6A4BDE33D0E168D002B36A37EB1AB326F353175A6348EE9168592A9167F5B0D8AAD99FA703B06595AF7D187A33EEEB00B48D3A656F068CD4C9DBFDA3 2
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":1.626956608543805e+12,"network":1.626924211e+12,"ticks":5491858375.0,"uncertainty":5181276.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016170022"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\62c27e2d-edd5-41fe-811e-514e5555a469.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):	174420
Entropy (8bit):	6.079210324457543
Encrypted:	false
SSDEEP:	3072:7/NkZExZKKJEuwA4x37SiHnDcWYKWFRFcbXafIB0u1GOJmA3iuRA:TcExzgRx37iWYFhaqfIlUOoSiuRA
MD5:	72D8057E8A2AF0D8A27CE5027FDBFDE3
SHA1:	B90F986F96F084781F394C871013EB3465A4726B
SHA-256:	A6A5A46020EF5E6DEA3416437D7468C6E15B975526FDE712331AA28011FA0A8F

C:\Users\user\AppData\Local\Google\Chrome\User Data\62c27e2d-edd5-41fe-811e-514e5555a469.tmp	
SHA-512:	307B05B57DA838B21338AA529384EA64A88CA4ECDB2E73311512F7C8348016BC614263F2CD01A4A07C43F1D86E6D917AFC00EAA376D64CCD1FBB74E22B6EBDA1
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":1.626956608543805e+12,"network":1.626924211e+12,"ticks":5491858375.0,"uncertainty":5181276.0}},"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\89fa2550-ff36-44b2-aae7-98589a647dd5.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):	166056
Entropy (8bit):	6.049735030563403
Encrypted:	false
SSDEEP:	3072:9FkZExZKKJEuwA4x37SiHnDcWYKWFRFcbXafIB0u1GOJmA3iuRA:9UExzgRx37iWYFhaqfIlUOoSiuRA
MD5:	E788EBC1353EFD510B231B7CE637D3E1
SHA1:	58F770F938A9039893653770A3F368638276DD17
SHA-256:	B823D37211B7687EDE0992B021AAAF7BDD43B00EAEBD26E2A6D3A39B121AC218
SHA-512:	972C80344E7B5C0542B23F67F9B9A6C53268FA37FA3368547A24874EB0B06D7ED583EFEB1A842ABD0A2CBC7549F6B7C50FFF124833F3B7D919DD0D2985D9FF2
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":1.626956608543805e+12,"network":1.626924211e+12,"ticks":5491858375.0,"uncertainty":5181276.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016170022"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\9aab83c5-b1cb-4e85-9d62-97ba646a05c3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7451809994044667
Encrypted:	false
SSDEEP:	384:zbkLzxOcF9CXeN3rUvjp3MbVsHFIG4XridbjxU1xZArq3my1ep3TvcO9t7NC1vW3:Ma9tSpU8Meb/xdcPL+RKvpzph
MD5:	BAB6DAEEA131CC50528BC94CFB849D14
SHA1:	8BA380B6603BB1FFDBE032259BFD41BD03C5D354
SHA-256:	23BD473F560B67D8C84AB69B795B79296FF0FF577D2300179552CEA5242E2A9D
SHA-512:	3A5F7E34AA9E0AB66F88EBFE3EDBF479BB6A01C25067C17892FF98651EF6B47683B14736E7DFAD465392D54638F91D7001A6E368B77AFDA8FC5CC870CBB0F9FA
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...l@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\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\48df04dc-ff9b-4ec4-a84f-97918f468f8a.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):	2120
Entropy (8bit):	4.886766316003863
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHzM6MsstTsqRLsdxdATseDshyKs53gYhbD:JTnOCXGDHzM6It/ebADkgxhH
MD5:	D5D47F8C59C84C9ABA2E171D7C48B2CA
SHA1:	FC8293A90230195EBE99B33741F2E1B7E468FE4F
SHA-256:	909D7FAF6D212A1369AF8604A82EF44879C91A74EC5E56B07B692FED4D09CD12
SHA-512:	622CC21DC79C95A36BD7E520474A87ED5FF658ABD6F725CADC82DA211E5DBC1F591FAB73C1F93C00E40E655BAFC5F2F7FF3F52DB5EC26361B1053B691009894
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274022210502253","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274022210503959","port":443,"proto

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4afd69e8-f247-4022-92bc-c403c19bd8dc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\50f8a42d-830e-4ac8-8f88-ee44c3e78ed0.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):	2151
Entropy (8bit):	4.889964008280612
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHzM6MsstTsqRLsdxdATshyKs53zseMHNYhbD:JTnOCXGDHzM6It/ebAUgzGqhH
MD5:	E33244C419F5CD9FCF7E9F3977A9BEA4
SHA1:	518AAABC6F6D069B35EE727EA6E0E137A3DBD9B0
SHA-256:	57D19E66964B5E1A0A4269922CBF7160F86D6FDC09F198D8B3B8696D0A1811ED
SHA-512:	B3AF6B7A7E4BCA018F3BD2E4551C720F1CFE55278C2209E8B15754E2A8F48EC1D20ACCB81DA9A4B7A884FBA378E32B87F17E5DC06813FC43BA7614693B8AC5E2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274022210502253","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274022210503959","port":443,"proto

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\62c4ce79-4e69-42af-a579-b50fefd90d1b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.53584503942821

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\62c4ce79-4e69-42af-a579-b50fefd90d1b.tmp	
Encrypted:	false
SSDEEP:	384:MIRthLlhjX41kXqKf/pUZNCgVLH2HfDirUwHG5nTMAj94k:JLll41kXqKf/pUZNCgVLH2HferU0G5nN
MD5:	FAC45350AC3C1C753EEAD5D6028C4FC5
SHA1:	6872BEF4968B1451E985516D9949DBA8AEC4CCA0
SHA-256:	E017EA158CB5F16F105BB698F591AAD7464CE93B47EA55DB6AB28E9DB0C63BC2
SHA-512:	C08DD29FECE313F2CFA9C0D399EF41C219E1FAD675F78645EA401BF8D36F1DDDCD0222F851B622ACF3C97A52BC1C2C3DCA81C50C685CC61B06D0EE693D270E
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":"13271430205172878","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\88aeebf2-a130-44ba-bdc3-04b4f87990d3.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):	4842
Entropy (8bit):	4.954420459172528
Encrypted:	false
SSDEEP:	48:Yc4UklSLklwHjwcBqA8dqTlYqlQKHoTw0IH3CH3G/s8C1Nfct/9BhUJo3KhmeSnz:n6CzoXMpcKI4ok0JCKL8VbOTQVuwn
MD5:	CAA7BADF1789D0E073D0B942576338C2
SHA1:	74201CFD1A25E185B12AF2052D4F63BA10205504
SHA-256:	26D8CBD90A470EFF6E7B6F4E1159DCC57B1E6CDA05F9BDF8262E5496BC47BC7B
SHA-512:	693689B1615D07A128B33409D7E434CE434140BEFF53739F7AC9E5CFC23AB9BF431F1505B6254A647FE4A7D31300534EEE8AF1FBCD4F7130DB4CC4C5943051D
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271430205436900","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.239990707768353
Encrypted:	false
SSDEEP:	6:mdNSMq2PWXp+N23iKKdK9RXXTZIFUtpAYAZmwPApdkwOWXp+N23iKKdK9RXX5LJ:2Pva5Kk7XT2FUtpg/PS5f5Kk7XVJ
MD5:	AC70CE300848360B839D028CE3EE3EAF
SHA1:	0454C395CBAE90EA21F25565673C80BB7A58C4CC
SHA-256:	FF70ECD5AA0A6F42DE29FE2648AEE25B907D11D64D2E78730DF66A6220A6E655
SHA-512:	F3D976847E159E3B2AEB07D9F3CC47EC4806CD2316FF69D6683F767810FB43E4733C3777EC42F6F459E0133C0BAAB3E0750FF0831E238BEC153DD21836CEB85
Malicious:	false
Preview:	2021/07/22-05:23:41.650 1a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/22-05:23:41.677 1a54 Recovering log #3.2021/07/22-05:23:41.680 1a54 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):	5.2132553495247755
Encrypted:	false
SSDEEP:	6:mdyFIq2PWXp+N23iKKdKyDZIFUtpA29ZZmwPAZdkwOWXp+N23iKKdKyJLJ:Uva5Kk02FUtpXP/Pi5f5KkWJ
MD5:	CD86F94BE52F294AD0C5993695168F1C
SHA1:	869682A3BE1E984AD749B9624B60A2300E28A5E3
SHA-256:	082274BD1239C09AC79330F77D63A6DF72B2A455C2C4A74B00BBE6CA1B2FE41B
SHA-512:	949E614942ECC1E5B5626BDADA12809A559B306EA83F51659720BCFF105FEF5D5D8D1829B4004CB5136A3DF78184C3771677370AAE086A125828D0B8D9B91319
Malicious:	false

Copyright Joe Security LLC 2021

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Preview:	2021/07/22-05:23:41.641 1a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/22-05:23:41.643 1a54 Recovering log #3.2021/07/22-05:23:41.644 1a54 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9690271780581045
Encrypted:	false
SSDEEP:	24:g2cLgAZOZD/UYVqLbJLbXaFpEO5bNmISHn06Uwf8:g28NOZ7Vq5LLOpEO5J/Kn7Uc8
MD5:	D89092527D8F1F8DB76A8F8228660006
SHA1:	F2F8375659A8D6AB20DE5EB6745D184B9D656F17
SHA-256:	97660F91ADF0BAC019DA78E1B330BCBEFEFF598773B448CA4B7927FFDA28A217
SHA-512:	6F0E5D451C17ECDDCBA29C7A386467B97EB7020E45A9B80A19EEE9F8632662911E7C2AADCFABBE0916EEBE6ACFC7629E823D041738C9CFF008A8E7B252E77E8
Malicious:	false
Preview:	.....6.>..... ....

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):	2068
Entropy (8bit):	3.1963966676990716
Encrypted:	false
SSDEEP:	24:34SnswlrlAko+5v2QJ+GdRkMeQ3LbS6jt6F+2lLlL:346/xlgQliQQ7bSiCRL
MD5:	B0B3FDEE83B93322FA5FC2FD380AA216
SHA1:	B68B8FDF47C1D4C081C3F4DD3222C18A8A4F1E1A
SHA-256:	A6BAA423FF2BF0EEBC5F96F73245FE19C6F841468FFE38FBEC2E67F3188431FD
SHA-512:	243D726CD8E73A3D6E33F2697333FE28642C111E702D66B27C41449F6F7A4C1855FF75EEA25570B16CD4E1D08AFB11AB3F0602BCACD202BC45CDD66175DE309
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...243360de_e106_4b65_8053_cba03ca4ea2e.....t.&G..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....q..l.....file:///C:/Users/user/Desktop/Remittance.html..... .....h.....`.....?.Z.....?.Z..... .....d.....f.i.l.e.:./././.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.R.e.m.i.t.t.a.n.c.e...h.t.m.l.....8.....0.....8..... .....file:///C:/Users/user/Desktop/Remittance.html.....C=".K&/.....file:///C:/Users/user/Deskto

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.250922658627497
Encrypted:	false
SSDEEP:	6:mbeE+q2PWXp+N23iKKdK8aPrqIFUtpGejOZZmwPGeB9VkwOWXp+N23iKKdK8amLJ:WQva5KkL3FUtpGSM/PGOD5f5KkQJ
MD5:	F6D682C9F4072A971E356614B387D6AE
SHA1:	25CE65563C47C16213358C78B50EE6A189ED6E81
SHA-256:	1D4F3EB4498C0CF7BFC65EBA5E934589402EB75BA628AC0A2BB2D6A0DC49781C
SHA-512:	C4364133D46716FBCE03C4B1BF22B1BFF8A1701F4765616DC4440F9EA5473E0C65C651D898C32E57C78869010CA59E8CCC1003B22B6D041BF1D180E92C108B4
Malicious:	false
Preview:	2021/07/22-05:23:25.479 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/22-05:23:25.480 12b8 Recovering log #3.2021/07/22-05:23:25.481 12b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.186168360887635
Encrypted:	false
SSDEEP:	6:mbb3+q2PWXp+N23iKKdK8NIFUtpGy2WZmwPG6iVkwOWXp+N23iKKdK8+eLJ:W7+va5KkpFUtpGRW/PG6iV5f5KkqJ
MD5:	FD22E1BB507431D0E49B92DEE5AD2878
SHA1:	04798332587B9C4967288FB0B256934580EBD5BA
SHA-256:	4C8A5DF8A27237D0FB501317950A16DD998EA901D7570271FA931DDB40FD7283
SHA-512:	A7B3439AD7F8C78A1E3063AB7859E6FD790C95781C825B2DCB0DA2DC2EFB86BA5B2E3B58773F1BD834D10CB06BE8D61B42C1C7297BFF103577D2DBC368F952 60
Malicious:	false
Preview:	2021/07/22-05:23:28.099 fec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/22-05 :23:28.100 fec Recovering log #3.2021/07/22-05:23:28.101 fec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5 n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/ 3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq 4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQ RpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl 32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc="," eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKn MKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9u qQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	198656

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Entropy (8bit):	4.093112329321939
Encrypted:	false
SSDEEP:	6144:gzsUg4n4eH3StZS5SISb4QkTLfEwgUj4aR9M7StlSlSUSbUEoTG:rQCW83R+9MGq4DD
MD5:	ECFE0A740E2213508D7C1B1DA362A7E4
SHA1:	C548FEFF926254901AB029A14F45C43A2F5997EB
SHA-256:	D3BE4BB13845B41D844CABD42D25252CC6B8BA16FE4F0B2CFE6273E2A4580CBF
SHA-512:	217094C8E7C87FBCB8639E37F827705ED22FE1C24AF10D3D1A352104BFFF1F252029073CA7618F80475CD8F6229754A2880662AC3D759C03F4DC428704729F78
Malicious:	false
Preview:	....AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	17496
Entropy (8bit):	0.7666091946087683
Encrypted:	false
SSDEEP:	24:ryLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwdrd4:rdBmw6fUard4
MD5:	C4ACC771AA3D5E285B3392D58C000EC6
SHA1:	8BAF9E714EBA45EC753AADB440EC84D4F1DA3A7B
SHA-256:	5F96CDCD1E666604394B662EBC55DB32459A0073E0F81E5E8D8BE791FA63F15D
SHA-512:	0CEC7EFE781638BBD679E6FD3E0BBA0B9A65454A731F0C297F385C0A72DDC3193CB5D74957A6F26EDBC229443868D7933B990DC23F9BEAAC198A95018661D6B
Malicious:	false
Preview:	..............SV.. ....SQLite format 3......@ ....C..........g....._.c...~.2.. ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Preview:	.f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.260389122809939
Encrypted:	false
SSDEEP:	6:mduNOq2PWXp+N23iKKdK25+Xqx8chI+IFUtpAujZmwPAuyjzkwOWXp+N23iKKdKI:BNOva5KkTXfchI3FUtpRj/PRGz5f5KkI
MD5:	7BA91440F950468A762A266ADF0D6D43
SHA1:	E244A88E0E36F5E87220E4F3A892E3198C128147
SHA-256:	245984F6F792A8B23FD44F922D3C2E54F92FB306AA17EA1EBA4694BF1B9D0C4D
SHA-512:	DC54F1DC6A4F79939EC9E96898A00E647434A907943131ED1961A78731907791AEDD13F160F010B38F9B5097C0D2AB080412D7432DAD4F0A47A3133D22A6C6AC
Malicious:	false

Copyright Joe Security LLC 2021

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/07/22-05:23:41.575 1a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/22-05:23:41.577 1a54 Recovering log #3.2021/07/22-05:23:41.578 1a54 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):	5.200992098392447
Encrypted:	false
SSDEEP:	6:mduF1q2PWXp+N23iKKdK25+XuoIFUtpAurZZmwPAurzkwOWXp+N23iKKdK25+Xu6:BF1va5KkTXYFUtpRl/PR35f5KkTXHJ
MD5:	4B235BE978D87F50A5CA3BCEB716CC04
SHA1:	A36FF12D4BF5B3A4AC40BBF248DFE9AEAFF92FEF
SHA-256:	9D2A9A6EB3E6862B7A83E797192CF06143301B85B3631B4C48E33613980CEC4E
SHA-512:	254D193E011E9E19D0F5F714EF9CC42F08A4217318AA2B1A59F748E8C8846CFDF695B14DEA11D950B7F48A1DD4892142ACEDA4A94C81611BAD94B0ABF4274F71
Malicious:	false
Preview:	2021/07/22-05:23:41.570 1a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/22-05:23:41.571 1a54 Recovering log #3.2021/07/22-05:23:41.571 1a54 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.241967750402056
Encrypted:	false
SSDEEP:	6:mdMnVq2PWXp+N23iKKdKWT5g1IdqIFUtpAMNgZmwPAgKIkwOWXp+N23iKKdKWT5i:dva5Kkg5gSRFUtpi/PX5f5Kkg5gS3SJ
MD5:	9FFC0AD04D11A9102608D44CEAA1FDCE
SHA1:	5AD2AE7E09ADC3026D441556BC402A0091A0F925
SHA-256:	CBBF1F6AB27AB0B14444B92B58C7C4ADABE25A5DB38CA51C39178170C9ECD38C
SHA-512:	37450813AAECC65401F4BBB611585DF52567B475834F7A7EAADC3A7834D38FAC62E22A8142CA0A7DAA16C690608957004637D58B1B1A9BAD4F0C5FAE5DC9582C
Malicious:	false
Preview:	2021/07/22-05:23:41.333 14c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/22-05:23:41.339 14c4 Recovering log #3.2021/07/22-05:23:41.341 14c4 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
Encrypted:	false
SSDEEP:	3:8EflEzB:8lt
MD5:	FEA13813DCADD185F25439091FDAFB9E
SHA1:	9DA367EF8AFCDAF7D8AD6C6526A0B3F0066F3EDA
SHA-256:	7D1E99CE35C8FEB1E7F61038FF861C9EDD88653FAA177BD1A90FC005B4DA3325
SHA-512:	1C2F02A82A035A2AAE59A0A7837F9FDE7A34206EDE1F939C7798F11EFC517071FF91C06601A204535A7040FC1751ED98FA9F13AD769B80C28577456E1BB7E05F
Malicious:	false
Preview:	.'...(..... ....e|.K&/.....

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):	0.11402143900275602
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvDCjYbjF1K+yU18gFqLCLmecOo/lCxthihGCxC+/erj5jF1K+yp:TL+A/VCkBwKHLcNuQhGI/8Bwp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
MD5:	FBF4C306F742E2FF8AAFD319DEC91CE2
SHA1:	58B9716F3E6CA7221CB5F8BD309518EADF54552D
SHA-256:	11E30D04829C01FE104B772DC9B210DDD0EA27F413A82E163D6D62D21BF88219
SHA-512:	ACACF54AA6CEF748067FB2272BE16700379429FC7A737F26C6329315351C58DAACBC3A3F2DB63B8D6108805BAEBD0B96420CEC06D9EC99AE75A395B88DD9E(3C
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):	668
Entropy (8bit):	5.240385834408557
Encrypted:	false
SSDEEP:	12:zgoKQa3yZxxk6yRdmOOtVSLNR2v/xf+H1TBk778B/xgskZBa9sNiy/YQUBwyrLbF:z3t8yq6yYVYNRI/xfaY78BJgskfa9yB2
MD5:	A339279EC3FD136027FF7EFD83F844EB
SHA1:	BC04C9BF08933DBE682F97DEDF85A0A538B2F839
SHA-256:	6CACCA30E3EE22BD4CCC1BB5357C934113E97CA0FF94A7D940FA84F40336C1A0
SHA-512:	9F721761859039063E7759173C738F34FB8E8A8F0E20774466955BD3DD364512A70D41BB38B410ABB5904345596FC64EA45E3ADBFF47DAD8C2075F085CFF07F0
Malicious:	false
Preview:	....."P....adobe..c..desktop..file..user..html..online..pdf..reader..remittance..users*|.....adobe.....c.....desktop.....file.....user.....html.....online.....pdf.....reader.....remi ttance.....users..2.....a.....b.....c.....d.....e.....f.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....z...:e..... .....Bp...l..... .....*.file:///C:/Users/user/Desktop/Remittance.html2.Adobe Online - Pdf Reader!:.....J.....*. .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.1163741381295549
Encrypted:	false
SSDEEP:	12:eIKrqLBj/ylM3lKvs4nMWQA9L4BQZ8fOM3:WqLBgM34dbN4Tf7
MD5:	7E37B84DD1754EAD0178E98D98EA2431
SHA1:	2F35B73391A5934C10D3FE1615BA43FC7BC7E9E0
SHA-256:	A54156B931898AF3E2CE7A04B74563CE4AE30899F4EA24E413701EAF1A71F6A0
SHA-512:	3C4EF83FA897817CD09D0CB774188BDC27A344859D93E8075C569A63DEAAB06DEB53800653E4340294093A5D99BE9F812D93F50D87A5DAD8073632622E202FE5
Malicious:	false
Preview:	....

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):	2954
Entropy (8bit):	5.471540239556505
Encrypted:	false
SSDEEP:	48:zZGCxSa7xMU8dbrNdx3bQSefgkNrS0U9RdiN9Pz:Pka7xMndbrNdxbQ5fgErS0Zz
MD5:	301B4CA9A0A80C5FFC17C614410248D6
SHA1:	DAF906ED3D2DCAE7240E2935FCA14A8B08767822
SHA-256:	F2550D62C9803B9089963921F7B03D07FA80926ED228373D0B8CBEB60418D823
SHA-512:	8E5B66BE560804028023A34A9170DFE753DCC2EF5C7A35A499B40E047620E5A1B5518E9130FDAB1B2DCCC5C0AC44957C12987FA15A3DCE505C908868CFB651
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Preview:	k.....*.....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..428789000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-22 05:23:43.11][INFO][mr.Init] MR instance ID: 4d71f8b3-8bac-463b-a9c0-03112d59917b\n","[2021-07-22 05:23:43.11][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-22 05:23:43.11][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-07-22 05:23:43.12][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-22 05:23:43.12][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-07-22 05:23:43.12][INFO][mr.CastProvider] Query enabled: true\n","[2021-07-22 05:23:43.12][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.184025215178001
Encrypted:	false
SSDEEP:	6:mbe3+q2PWXp+N23iKKdK8a2jMGIFUtpGeYZmwPGe1VkwOWXp+N23iKKdK8a2jMmd:WTva5Kk8EFUtpGl/PGM5f5Kk8bJ
MD5:	9C773E346DDF7C6689863B6594AC8450
SHA1:	811832832B724C4E29A5C08E807F645F328FB8C9
SHA-256:	A9BF039C1880CF89CD22FAF08C7A8E253ACA385294FCEDF6BA11528ED00C18BF
SHA-512:	641FF671D61048D3AF57E53A9912D2F2A30545456050B29504EFC68A77F12B58EB2AA248ADFF7E1C0E7053FA1F6CCE3E3532073D97F6D7581A72212FF249DDFF
Malicious:	false
Preview:	2021/07/22-05:23:25.204 14c8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/22-05:23:25.205 14c8 Recovering log #3.2021/07/22-05:23:25.206 14c8 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):	5.21929221452538
Encrypted:	false
SSDEEP:	6:mbe5FU9+q2PWXp+N23iKKdKgXz4rRIFUtpGeBWZmwPGeBtVkwOWXp+N23iKKdKgi:WuFU4va5KkgXiuFUtpGZ/PGK5f5KkgXS
MD5:	4123DAFAC7438E466577089A210C1555
SHA1:	9D34F159084885D52FD7F4E77D3B7383945CF4CE
SHA-256:	68E1CCB2DE7CF809390A50FB217ABB86A34D773099536EF24ED78DE2A8204A87
SHA-512:	0BB7575FF31B3ADF11375AE35953D536C2322B42FAC8844ABDCCA352F97373BF46523CE3D28FF7563F0264A24C071600B41C9E42139CD1F0D9D394DE18E8760
Malicious:	false
Preview:	2021/07/22-05:23:25.509 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/22-05:23:25.512 12b8 Recovering log #3.2021/07/22-05:23:25.513 12b8 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\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):	0.8766215531408712
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUYzic76xigxFWQ:wIElwQF8mpcS/xZxFfxZx
MD5:	3658F2921B9E4895677D8E9BAA96484B
SHA1:	140E53E36782ACB834A6181A3153C75D7CED536C
SHA-256:	A7EAE3B7D5D4AEADDBEC3B048EAFE544DD3BB52E630FD7755F34198EC348567D
SHA-512:	C2D37056C96897061ED847AB7352265664E3A60E05899E8102ED0F88D05DF78B2309F023EC4F80B8875FF171B29983801E74DF40B3A8BF532A31DD7915040AA2
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Entropy (8bit):	0.6268527760586761
Encrypted:	false
SSDEEP:	48:+D8qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUp4:+D8hIElwQF8mpcSy
MD5:	4377066EE917553470A0035F48BDE71E
SHA1:	FBFE00D97B7941EA185E24FF2ACD1245ABEDC334
SHA-256:	781DCEE2A43334F2B96A1BB9B0F6E0EA52CA33083429FCD2DC9D9C32A5D9D962
SHA-512:	11F957C5C23F4D58CD14120FAED8C7DBB29C67C3DD4527A23A63BB41E8541FBC9F6E195A5A5FA0D22A16C83452854D4FE33FE4EF710E4E3E6E70C49302B03AB
Malicious:	false
Preview:	.....?1U..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.130501831364045
Encrypted:	false
SSDEEP:	6:mbehvOq2PWXp+N23iKKdKrQMxIFUtpGeGFeZZmwPGeGFezkwOWXp+N23iKKdKrQq:We2va5KkCFUtpGRoZ/PGRoz5f5KktJ
MD5:	8C7512808D2DE9C27ADFCAAD1FA80B4E
SHA1:	33FA722F4F898D0204C73184A63390CCD69BCE4A
SHA-256:	F7219350B93DD11A0F07DA5184D3C2C7DAFB44E505DFED00825F34C613F8DFEF
SHA-512:	B2F8E205C275F2A563A4FC945F7C302453E5A9A9506504246D9EF0B252EDF464E270A211F1881DF18C6BE5A59066458E6A9E3C1B2AA064EAA519F231E7004196
Malicious:	false
Preview:	2021/07/22-05:23:25.409 1550 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/22-05:23:25.410 1550 Recovering log #3.2021/07/22-05:23:25.410 1550 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.187898016441016
Encrypted:	false
SSDEEP:	6:mbeL8v4q2PWXp+N23iKKdK7Uh2ghZIFUtpGeLINJZmwPGeLhzDkwOWXp+N23iKKF:WmW4va5KkIhHh2FUtpGm6J/PGm1D5f5m
MD5:	51EE4313ECDE43E506B905CF0E7034A9
SHA1:	2AD63B417806A13F565C8BA38A95A026D7866B33
SHA-256:	0DFB5A911D9139EB95A788DB983732EBAA1A2ADA9FDFC8D4C6A22E4F463E837A
SHA-512:	55F668E9129DCD3F69995464E4B14B56DE2C654FEB6BF0799004444693B1DA0DD73EF437D3CE01083CEFAD125589E625AD2E6A6132E1326B785208B7994E347B
Malicious:	false
Preview:	2021/07/22-05:23:25.174 1660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/07/22-05:23:25.178 1660 Recovering log #3.2021/07/22-05:23:25.179 1660 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\892a86e7-b00b-4adf-aeb5-0be4fe83df99.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.281723190779525
Encrypted:	false
SSDEEP:	6:mbe0Q+q2PWXp+N23iKKdKusNpV/2jMGIFUtpGeOgZmwPGeOQVkwOWXp+N23iKKdD:WJVva5KkFFUtpG3g/PG3I5f5KkOJ
MD5:	54D01916244CC4731F0DD14FBEBE7529
SHA1:	EAA902D7E2ED1E72BF8E3E55814D6D355FE20D2D
SHA-256:	1D16717806A992537BF64B906E2B2BE7FAC061350824E013A47AEA8F34FA773F
SHA-512:	A9DD7E903DEFCE0B4E2B036C08209AEC7BC2DDB15C577D0F3F476D79A11D3F94705EA6D8AEEA96ACE8DB75563BC3CAEC890D263697BAEAF1D1B6A874B00541E5
Malicious:	false
Preview:	2021/07/22-05:23:25.464 df8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-05:23:25.466 df8 Recovering log #3.2021/07/22-05:23:25.466 df8 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):	5.254550650022475
Encrypted:	false
SSDEEP:	6:mbeUQQ+q2PWXp+N23iKKdKusNpqz4rRIFUtpGeBagZmwPGeBNQVkwOWXp+N23iKV:WtQVva5KkmiuFUtpGtg/PG6I5f5Kkm2J
MD5:	82EB9EDBC9984FD0BF6127B23D7EDF3D
SHA1:	A617FF312FCB57961AFADF85984A2F6E0AF5C508
SHA-256:	7E2FCACB938CE48F7A503C162D6FE3EA86A3407A5BBCE37B7BC3E809716245E8
SHA-512:	D3B0EE3DE28E2CC33A2F098848C9326B4DB8FEC8699AD9551BF1007C14A1FCE9F280CA4B0BEEDCE4D1E6D5B70EC9CAB2CB498B6DB468EEA02E88E2B90ABC0487

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Malicious:	false
Preview:	2021/07/22-05:23:25.502 df8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/07/22-05:23:25.510 df8 Recovering log #3.2021/07/22-05:23:25.511 df8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.255367808971241
Encrypted:	false
SSDEEP:	6:mdgDM+q2PWXp+N23iKKdKusNpZQMxIFUtpAoPfSgZmwPA2DMVkwOWXp+N23iKKd0:G+va5KkMFUtprX/PkV5f5KkTJ
MD5:	D438D4CD59F4E9403E2C42C6B0BBC643
SHA1:	4696C0696420367A05D4FA8B59FE428AC39CF66D
SHA-256:	E826E1FDF5324F8F00E702EBDFC7C1D1EE1EC186858312B69F1BE64DEAD04C95
SHA-512:	97D892D9E0505735B22CF941DC28DB89FDF610D0FF3182835247B279D693407D45FEFED6471B73C30A9588EFC4EF475D4E5CB69A062DA98352794E5CA13D741
Malicious:	false
Preview:	2021/07/22-05:23:42.107 131c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/07/22-05:23:42.108 131c Recovering log #3.2021/07/22-05:23:42.109 131c 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\5ea4ab61-ad13-4b75-952c-b82929c22263.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.207252274751026
Encrypted:	false
SSDEEP:	12:pd+va5KkkGHArBFUtp5e/P503V5f5KkkGHAryJ:pqa5KkkGgPgjayf5KkkGga
MD5:	7AEE353A96479FA273CEA482278DAA92
SHA1:	76C842921B1836F3422BCAEA1CAA830B87B71E99
SHA-256:	004F2D8434A6E50498D5454F5CECF7F7E0C0D34042873CF4CFFA85824383567C
SHA-512:	4DDCEC68B4233241FD68ED1AB165B73DBC42A04D606C956C0C210AA2C745BFC300AF902E421DBB180617F788732546FF23CB21DAE828FA085481F869218ECF9
Malicious:	false
Preview:	2021/07/22-05:23:41.792 131c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-05:23:41.797 131c Recovering log #3.2021/07/22-05:23:41.799 131c Reusing old log C:\Users\user\A ppData\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):	5.260331791166343
Encrypted:	false
SSDEEP:	12:pnova5KkkGHArqiuFUtp5dq5/PmF5f5KkkGHArq2J:paa5KkkGgCgjlwXf5KkkGg7
MD5:	B95E1D373D52CE42D4077E75A5A19991
SHA1:	6C9232A95D8C57DD0FD7838F5C0DEBB6546B74E7
SHA-256:	19E7378004DE1AE252A7D17D2368CBB87CA8FFB23C5C575EED0EFC9448FF3AC2
SHA-512:	94E96E24968E6104220CAE3817EE233F1B499D809B1C96C41CDE6B914B4C539B87DAE851A1B4DDB687D2B7D34D272A32BEDA79725998CBA68A7316FDCB83F95
Malicious:	false
Preview:	2021/07/22-05:23:41.793 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/07/22-05:23:41.798 12b8 Recovering log #3.2021/07/22-05:23:41.800 12b8 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Entropy (8bit):	5.185915263476516
Encrypted:	false
SSDEEP:	12:2Vva5KkkGHArAFUtpMg/PMI5f5KkkGHArfJ:25a5KkkGgkgiJSf5KkkGgV
MD5:	D7AAFBF1FA269F039A994DDEA9D61DFA
SHA1:	20AC872E19DAA2A3536938884C268DBAA1D9247D
SHA-256:	00440C770C3E6EBD4605EB7D2DCC62B9D3953304077BADE4F272318F2A06A4FD
SHA-512:	17D2DD4F93C5332BADB3BD5DCC625182378CE930D2B21C51E67798828CF2063EB932B77F9DDC4C9C4041E64CD2D545B3B21F58CC1CA738320F464F95787623
Malicious:	false
Preview:	2021/07/22-05:23:57.090 df8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/07/22-05:23:57.092 df8 Recovering log #3.2021/07/22-05:23:57.092 df8 Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.2343830527293145
Encrypted:	false
SSDEEP:	6:mbeLB6yq2PWXp+N23iKKdKpIFUtpGeLF1ZmwPGeL5RkwOWXp+N23iKKdKa/WLJ:WmBva5KkmFUtpGmF1/PGmf5f5KkaUJ
MD5:	ABC0ACC2307ED4C44CD214D5F4DC16D6
SHA1:	3B53DA0B2D4A69B17464E21A799B1571C0273C1A
SHA-256:	0FA30BF8C1F21863A46BC62921F8C8AA20478CE24C3A2AFAB6C0BFC27A0925D4
SHA-512:	AEFC50A05424BE0BD9826DDD31EDCCB4279130EAC1DB793A0F3F6646A54EEDAAE37BCC02F87CAAA971CD1A7412E134F646EF458B71A0D434E50187F972D24 5C
Malicious:	false
Preview:	2021/07/22-05:23:25.173 1430 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/22-05:23:25.176 1430 Recovering log #3.2021/07/22-05:23:25.178 1430 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):	5.3288772052846705
Encrypted:	false
SSDEEP:	12:6Vva5KkkOrsFUtpewg/Pewl5f5KkkOrzJ:65a5Kk+gTYSf5Kkn
MD5:	08258B520C148D3FC4FA32115D6EEB0B
SHA1:	93E91D3280B182465FB3813E8366D6D701D00FC6
SHA-256:	D36171BCDC0FF40BC5AE0DF8E5A79BA7C0EDB0722ED738833523A9A669CE92C2
SHA-512:	E1D9225BB0E3890963DBA1E0E6C686904D034D9E8DCC7ECFF37D86CD16EC4FFFED9BB7C774700F3859BD54259EB3690DC2388C089E37AE2356340F8AB5D9E8 F
Malicious:	false
Preview:	2021/07/22-05:23:43.112 df8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbm eomcjbeemfm/MANIFEST-000001.2021/07/22-05:23:43.113 df8 Recovering log #3.2021/07/22-05:23:43.113 df8 Reusing old log C:\Users\user\AppData\Local\Goog le\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):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:Jarvn:J6v
MD5:	F2AFBAC7923571A857BD5FBD59A3D25E
SHA1:	4D82DE558DE8DCAD88C8F6F0EB4467C87EB979E2
SHA-256:	D9705122DBC535E9324A7B4710F4C9361EBC51D82A0E16920299A569857C87B0
SHA-512:	44EEDD15FE5239EB369E8746E67FC21F574C222D5CDCAB70BE422AB9E117FB4D4319A8717FEBEA7067ABAC190F17D36425989298EADBDEDF7C3EA9B32D6FDE0B
Malicious:	false
Preview:	..........:.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\af5b9a4e-a8a4-4a99-8e80-859f148e830e.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):	5464
Entropy (8bit):	5.181521512753212
Encrypted:	false
SSDEEP:	96:n6Cz7mMCVR9mMduicKI4ok0JCKL8lbOTQVuwn:n6C2MCP9VIicl4Ka
MD5:	D5E772219A716C94A6D29E21B390EBE5
SHA1:	7E2A36A399373733EBF336C56A866FCAD4BF6516
SHA-256:	98842BB960C345EF91069BC73267359E1FAE3A454179F20E0F7AAF6CD9024DA1
SHA-512:	7B477A287A306BA306DD1F5803DB3A6E0DAF768E494838CC86654AF15C8A936CCAC5788266192FF5B01124674EE7DEF1A134B0479EE5A189874BDA7DEFEE1B14
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271430205436900","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b3f3b828-c5a9-417d-867f-161ae7acd0b2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b90020b2-e898-4f74-a004-ded2185922b9.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):	5438
Entropy (8bit):	5.177571272262914
Encrypted:	false
SSDEEP:	96:n6CzPmMCVR9mMduicKI4ok0JCKL8VbOTQVuwn:n6CaMCP9VIicl4K6
MD5:	4F560A3D3A63C76B7890CED2DD538825
SHA1:	C45564C6EAFD15D818B4CD2AA2BB1EF65439B147
SHA-256:	CA608AEAFF4864C3282DBEFD2D48492D1901A60CFAF1844B320A8A5A3DFF3DF9
SHA-512:	A277BC6548E1373E46CF610276A86D1273EA0FBB870F4B6065DE53751AD7F7184A1F352EB804A457A927AFFB63B97A8EEAD575FCC106FF550F5ECF77673D0B3

Copyright Joe Security LLC 2021

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b90020b2-e898-4f74-a004-ded2185922b9.tmp	
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271430205436900","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c03bc6ab-7acb-4afb-8f96-0ec45bef29f1.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):	1207
Entropy (8bit):	5.569094439115563
Encrypted:	false
SSDEEP:	24:YetnWswUOy6H0UhVsTG1KUerkq/HeUeXby2qUeXv/L7wUpRUenHQ:YCVwUX6UUhVseKUewqPeUer2Uef/HwU+
MD5:	D22E767485BB2D148F8729EF9F797FA6
SHA1:	BBAB56820B0049DBBFC7C79E0F5B14E773AD1548
SHA-256:	CFF0DB7305E8AE0BE2FD920B1E4841284368C9C80DA168D4EE0587A4C792CE35
SHA-512:	8E8A26DD1C4419B326E29E6DC5E991499287FCD4AF00163A663946960886DC722242DA389ECE149CF41206A8A4C262FE10F6EA8F7688D30978ADC9DF33DC03A
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1642736610.471589,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626956610.471597},{"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":1658492610.504022,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c83148c2-1eb3-4d82-b82a-8f5b7bd67330.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.5774612662413325
Encrypted:	false
SSDEEP:	384:MIRt8LlhjX41kXqKf/pUZNCgVLH2HfDirU/Ag94e:ELll41kXqKf/pUZNCgVLH2HferU/T9N
MD5:	B6E80D4A631D432A9145EEBF223FA9BC
SHA1:	E8A170EAC28F0FFFE50B39A8A3E902E4196D5727
SHA-256:	6D3CC7523ACA5DFB4344B36285DD0C6C4DA4EF0853ABCD1F0FDAFEB2C1D13C6E
SHA-512:	EC07B2756222AD3306F0F322F247D94EB62B5D367C7473CF12281656DC3EC499D8F1E71099BD0A05CBBF4E175791FEA74A730F3ACC36B9E70E72D955E142301
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":"13271430205172878","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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\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\de806212-0c2d-49b3-8f73-ea4c28ef3629.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.53590766487945
Encrypted:	false
SSDEEP:	384:MIRthLlhjX41kXqKf/pUZNCgVLH2HfDirUwHG6nTMAU94K:JLll41kXqKf/pUZNCgVLH2HferU0G6ny
MD5:	9019E8D8CF0AAE7070C8F96CC149A0CD
SHA1:	2A70BC5211E9D09DFD6713BD8CE91228ECF30BC1
SHA-256:	64EC2B28ED8F274CA0B293CDEFF02DBEC1BE9F9C7AD17F9B1E138EB79C143768
SHA-512:	36CC27C9F044D5A405D82BB40EE67228BCCC4976510F663875CE586882517ED0B794571356DEE336B94414012FCB70B4FC39F3C37F7413A59F1AC9BC83834A34
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":"13271430205172878","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	5.2626667845017385
Encrypted:	false
SSDEEP:	6:mdII+q2PWXp+N23iKKdKfrzAdIFUtpAI6XZmwPAIRVkwOWXp+N23iKKdKfrzILJ:Vva5Kk9FUtpCX/P35f5Kk2J
MD5:	F9FA3EFDA3859E25CAEB36158615F1AB
SHA1:	86729F69E2D5A422DCA105080707D93B9C00A467
SHA-256:	B0E46E48892E523B93FF26D83E1CB66C38494B0AFBB418B8BA259E0CA248BC3F
SHA-512:	E5F99C6E559BADF4F0DEFDD89590C51DECC0BFEBE2CE0E010E673A5D9BEDD6034BD1953E19503EA866778F90CA97804B83CBA0E80C8BCD6473DA9B5BF388690
Malicious:	false
Preview:	2021/07/22-05:23:41.954 12b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/07/22-05:23:41.956 12b8 Recovering log #3.2021/07/22-05:23:41.957 12b8 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:	3615498FBEF408A96BF30E01C318DAC2D5451B0549981190 80E7FAAC5995F590

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
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
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):	0.44812403665442346
Encrypted:	false
SSDEEP:	3:8EflWuD+l:8Dui
MD5:	1BB60F2F4E0D3758B7342D2939D46F3E
SHA1:	07B2ED42DB0CF16A1FB916220629EAD25648AF01
SHA-256:	6FB36BD6C62927A9BBDC55B06A1A31D36B68D6695646BD6578E50A9844F09654
SHA-512:	9F1B5D28C4ECD55D0E37C8C3A1D01F3B9E7FDEFC041B2DC2849C9BE0AB6C605C2CE5A072C33F3989C95271FEAB98E1CD1C0822F3CDF531318D7EA889B436576
Malicious:	false
Preview:	.'..(.....<.K&/.....

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_dir4168_49711109\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir4168_49711109\Ruleset Data	
SHA-512:	F49A4487C245DE86158EE6BD675BF70C74D8FE7164A5AA5D71469AFA94071FD4C06BB09E88E06B1CCDE9ADE6C124C957E45179C25891E12BD7C9FD419B7EBF 72
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\a2f37609-331a-4194-825e-6b4a4033371f.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):	166160
Entropy (8bit):	6.050038750386979
Encrypted:	false
SSDEEP:	3072:DLkZExZKKJEuwA4x37SiHnDcWYKWFRFcbXafIB0u1GOJmA3iuRA:DqExzgRx37iWYFhaqfIlUOoSiuRA
MD5:	228765F7DDF58E35F6E5ED35772DD5A6
SHA1:	EF8D02FC7A050E72BE24C7895DF783F7497CEBA3
SHA-256:	9D80B5A07B6AC0D259F82C7BEA7FD9D9D93BC8F9008E284FF06E25E1C72E2BF0
SHA-512:	54C4CD46AABD99EA2597E6445DEFC723009B706ABBC9CD46998EFF98E76AC472D31DBE615972553F8C68C8B0011A9E70F6AAD5A2452904DCD6C70F9B7DE7C E3
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":1.626956608543805e+12,"network":1.626924211e+12,"ticks":5491858375.0,"uncertainty":5181276.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016170022"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\e14c9e22-b0dc-477b-a0a4-d0fe1636aca3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7454289815694524
Encrypted:	false
SSDEEP:	384:1bkLzxOcJi9BVawXeN3rUvjp3MbVsHFlG4XridbjxU1xZArq3my2Iep3TvcO9t7+:hCa9tSps8Meb/xdcPL+RKvpzpQ
MD5:	2830C371DFCB113FEDDB55C7AA976F53
SHA1:	A825955872D6CAB7879626CE9863659C632C54F2
SHA-256:	E1AB34B0BFC890FC386F9F980CE5568D03177B9180AF5E48DA1C77964A328B9A
SHA-512:	D4987D8901FC7C23ECA97C9059A7D52BBBA64451426D9D46A0247BD0674FB7EA340F0405E38F124565B4311E5C8E3197CFBEBB217A62D157DC0EB3EBCFCCB2 DA
Malicious:	false
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...l@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\f9f813c3-3b44-4bd6-86d2-7a80f143e3be.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):	166160
Entropy (8bit):	6.050038750386979
Encrypted:	false
SSDEEP:	3072:DLkZExZKKJEuwA4x37SiHnDcWYKWFRFcbXafIB0u1GOJmA3iuRA:DqExzgRx37iWYFhaqfIlUOoSiuRA
MD5:	228765F7DDF58E35F6E5ED35772DD5A6
SHA1:	EF8D02FC7A050E72BE24C7895DF783F7497CEBA3
SHA-256:	9D80B5A07B6AC0D259F82C7BEA7FD9D9D93BC8F9008E284FF06E25E1C72E2BF0
SHA-512:	54C4CD46AABD99EA2597E6445DEFC723009B706ABBC9CD46998EFF98E76AC472D31DBE615972553F8C68C8B0011A9E70F6AAD5A2452904DCD6C70F9B7DE7C E3
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\f9f813c3-3b44-4bd6-86d2-7a80f143e3be.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":1.626956608543805e+12,"network":1.626924211e+12,"ticks":5491858375.0,"uncertainty":5181276.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016170022"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Temp\3c78cb66-206a-4278-bf9a-f05e94f16e4b.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...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."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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\4168_13234485\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

C:\Users\user\AppData\Local\Temp\4168_197583760\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	66
Entropy (8bit):	3.893948431036658
Encrypted:	false
SSDEEP:	3:SVbHhID/aE7RR8JIKLEXxXTQ9gG:SDI77q9wJygG
MD5:	0B46A559724C0403EF7FB286B713EC99
SHA1:	D7EBD7D59199305F13474C8E0E18DA72E6373148
SHA-256:	B71EC26B0F0FE87A91C47A91B6AFB5C2729478C83337D141FC136C9C02CC6B7D
SHA-512:	5E7F535A3A62EFFB329A94FDE728DAC38A5D26B91B6E225F33716970CD06CAAF00A6D90E967793A570776F0EB60F0C221A683F45E778C87ABE647CD1E35B1A4
Malicious:	false
Preview:	1.0727b38159b38ffa3633510444ece15c86417962e8cac59c59002f13b50239ac

C:\Users\user\AppData\Local\Temp\4168_38619290\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):	3.9265057735423707

C:\Users\user\AppData\Local\Temp\4168_38619290\manifest.fingerprint	
Encrypted:	false
SSDEEP:	3:Scy/szkTqhKDKVXGWjGd5n:ScCPqhYKVFK5
MD5:	72AC97F196EAA5A1E6C61113B4931B84
SHA1:	B23CC7C005A3BC6AD1517B9B1CB86E4451E92021
SHA-256:	A51A8D5EF5856EDD33EBDBD68AE67B9F0BDDB6FD3C0256637EA688429C36525D
SHA-512:	3F60837DACB8B20A8E87E432A61D0C59E9D39152167AE2C6D0FFC3CA9DE25C4CC9ECAB4A7FF1762B27F2C53FFD8AFD5B8F519CC8B242E2DD801AC29822275C4
Malicious:	false
Preview:	1.91ee417000553ca22ed67530545c4177a08e7ffcf602c292a71bd89ecd0568a5

C:\Users\user\AppData\Local\Temp\4168_97928390\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:	7EF8A13685078E5D08EFB5C8C265ED732053750D006D62F0E700898681AF607C02D0A4F91B88F574DFD0EAE0D5DAA75647307EDBC062DD3A5DB864BD541B930D
Malicious:	false
Preview:	1.694636bbb2f68d5629d1e4a499aabd2d82f93c95c49c20e270b301d94cae333a

C:\Users\user\AppData\Local\Temp\45727cf2-7f79-44d7-89f7-60f82240ae6a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
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.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\76a8a4fa-9ac0-4bc0-a93f-62a6382f7d7d.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\ce67efad-4bfe-442d-b7db-acc69b34c98d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\ce67efad-4bfe-442d-b7db-acc69b34c98d.tmp	
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\scoped_dir4168_1312877925\45727cf2-7f79-44d7-89f7-60f82240ae6a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
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.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.lpr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0lprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\ar\messages.json	
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": ".. .. ..".. },.. "12827687646031907 5": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... .....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": "...".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": "..... .....".. },.. "18503975003120203 88": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Preview:	{.. "10189845614885205 17": {.. "message": ".....".. },.. "12139579827238759 20": {.. "message": "... .. ..-..... ....?".. },.. "12827687646031907 5": {.. "message": "..... .. ..".. },.. "14284488690781267 31": {.. "message": "..... .. ..".. },.. "15221406833188603 51": {.. "message": "..... .. .., ...".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": ".... .. ..".. },.. "18503975003120203 88": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:lPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Preview:	{.. "10189845614885205 17": {.. "message": ".... ...".. },.. "12139579827238759 20": {.. "message": "..... ....?".. },.. "12827687646031907 5": {.. "message": "..... .....".. },.. "14284488690781267 31": {.. "message": "..... ....".. },.. "15221406833188603 51": {.. "message": "..... ....".. },.. "15509040647108289 58": {.. "message": ".....".. },.. "16366867476874943 76": {.. "message": ".....".. },.. "18027627465894571 77": {.. "message": ".....".. },.. "18503975003120203 88": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DB1
Malicious:	false
Preview:	{.. "10189845614885205 17": {.. "message": "Es congela".. },.. "12139579827238759 20": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "12827687646031907 5": {.. "message": "Detecci. de dispositius".. },.. "14284488690781267 31": {.. "message": "Flu.desa del v.deo".. },.. "15221406833188603 51": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "15509040647108289 58": {.. "message": "Correcta".. },.. "16366867476874943 76": {.. "message": "Perfecta".. },.. "18027627465894571 77": {.. "message": "Volum".. },.. "18503975003120203 88": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "m essage": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$ST ART_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. " END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $ START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\el\messages.json	
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djlV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C013
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "......... ....".. },.. "1428448869078126731": {.. "message": "......... .....".. },.. "1522140683318860351": {.. "message": "......... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "........ .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir4168_1312877925\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdI
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chromecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.891804304950461
TrID:	• HyperText Markup Language (13003/1) 100.00%
File name:	Remittance.html
File size:	655802
MD5:	1dd3d108e04a63ab04097cab5f10a921
SHA1:	f4efed64ae9894307197126c22a21e57e8783114
SHA256:	bbde5d42af6fd69db1901c341452a98c25fd5b8499c661b94cc24d45ea67bc86
SHA512:	74b10dec9ee8e00b79e417881a3a80cc6e893c7a9f5cb2a3074ea009883b66ee611df3445f60243827e5b5533f2d3289821985e5e20cbb11fdeec3d770f44677
SSDEEP:	12288:HeQx02SeaXwyF5/QyS666o68wldZUO2PM/8ORgYOW3FcvxZ4PI8klE8fqhGdMS:0ead7HNfXUrPMTuS+ZmPI88ECMS
File Content Preview:	..<html xmlns="http://www.w3.org/1999/xhtml">..<head>..<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">..<title>Adobe Online - Pdf Reader!</title>..<link rel="icon".. type="image/png".. href="

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 05:23:31.140974045 CEST	192.168.2.3	8.8.8.8	0xc479	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.143563032 CEST	192.168.2.3	8.8.8.8	0xa7e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.145680904 CEST	192.168.2.3	8.8.8.8	0xc966	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.645260096 CEST	192.168.2.3	8.8.8.8	0xfba6	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:42.302248955 CEST	192.168.2.3	8.8.8.8	0xbeb5	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 05:23:31.202012062 CEST	8.8.8.8	192.168.2.3	0xc479	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.202012062 CEST	8.8.8.8	192.168.2.3	0xc479	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.213810921 CEST	8.8.8.8	192.168.2.3	0xa7e	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.214663029 CEST	8.8.8.8	192.168.2.3	0xc966	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 05:23:31.214663029 CEST	8.8.8.8	192.168.2.3	0xc966	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.695482969 CEST	8.8.8.8	192.168.2.3	0xfba6	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 05:23:31.695482969 CEST	8.8.8.8	192.168.2.3	0xfba6	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 05:23:31.695482969 CEST	8.8.8.8	192.168.2.3	0xfba6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.239.65	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.695482969 CEST	8.8.8.8	192.168.2.3	0xfba6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.136.132	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.695482969 CEST	8.8.8.8	192.168.2.3	0xfba6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.121.178	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.695482969 CEST	8.8.8.8	192.168.2.3	0xfba6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.92.227	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.695482969 CEST	8.8.8.8	192.168.2.3	0xfba6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.216.118	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.695482969 CEST	8.8.8.8	192.168.2.3	0xfba6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.224.49	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:31.695482969 CEST	8.8.8.8	192.168.2.3	0xfba6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.16.238.218	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 05:23:31.695482969 CEST	8.8.8.8	192.168.2.3	0xfba6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.190.106	A (IP address)	IN (0x0001)
Jul 22, 2021 05:23:42.368715048 CEST	8.8.8.8	192.168.2.3	0xbeb5	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 05:23:42.368715048 CEST	8.8.8.8	192.168.2.3	0xbeb5	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 05:23:32.054611921 CEST	50.16.239.65	443	192.168.2.3	49722	CN=*.ipify.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Feb 20 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4168 Parent PID: 2592

General

Start time:	05:23:24
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\Remittance.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: 672 Parent PID: 4168

General

Start time:	05:23:25
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=1556,10324375867687729821,3875551371938988928,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /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

Disassembly

Copyright Joe Security LLC

Copyright Joe Security LLC 2021