ID: 433328
Sample Name:
VM64DGCRMN5XGK.htm
Cookbook: default.jbs
Time: 16:39:57
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

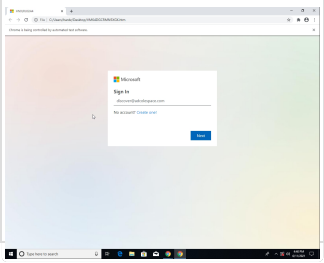
Analysis Report VM64DGCRMN5XGK.htm

Overview

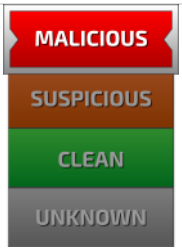
General Information

Sample Name:	VM64DGCRMN5XGK.htm
Analysis ID:	433328
MD5:	be59593c1b8874..
SHA1:	bac3b5ed310ca1..
SHA256:	808b36fb0d39cb3.
Infos:	

Most interesting Screenshot:



Detection



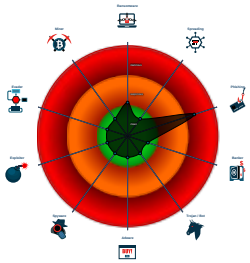
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish44
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- None HTTPS page querying sensitiv…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4580 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\VM64DGCRMN5XGK.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3152 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,10561022475399133662,8554087899327668488,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1704 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
VM64DGCRMN5XGK.htm	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

Phishing:

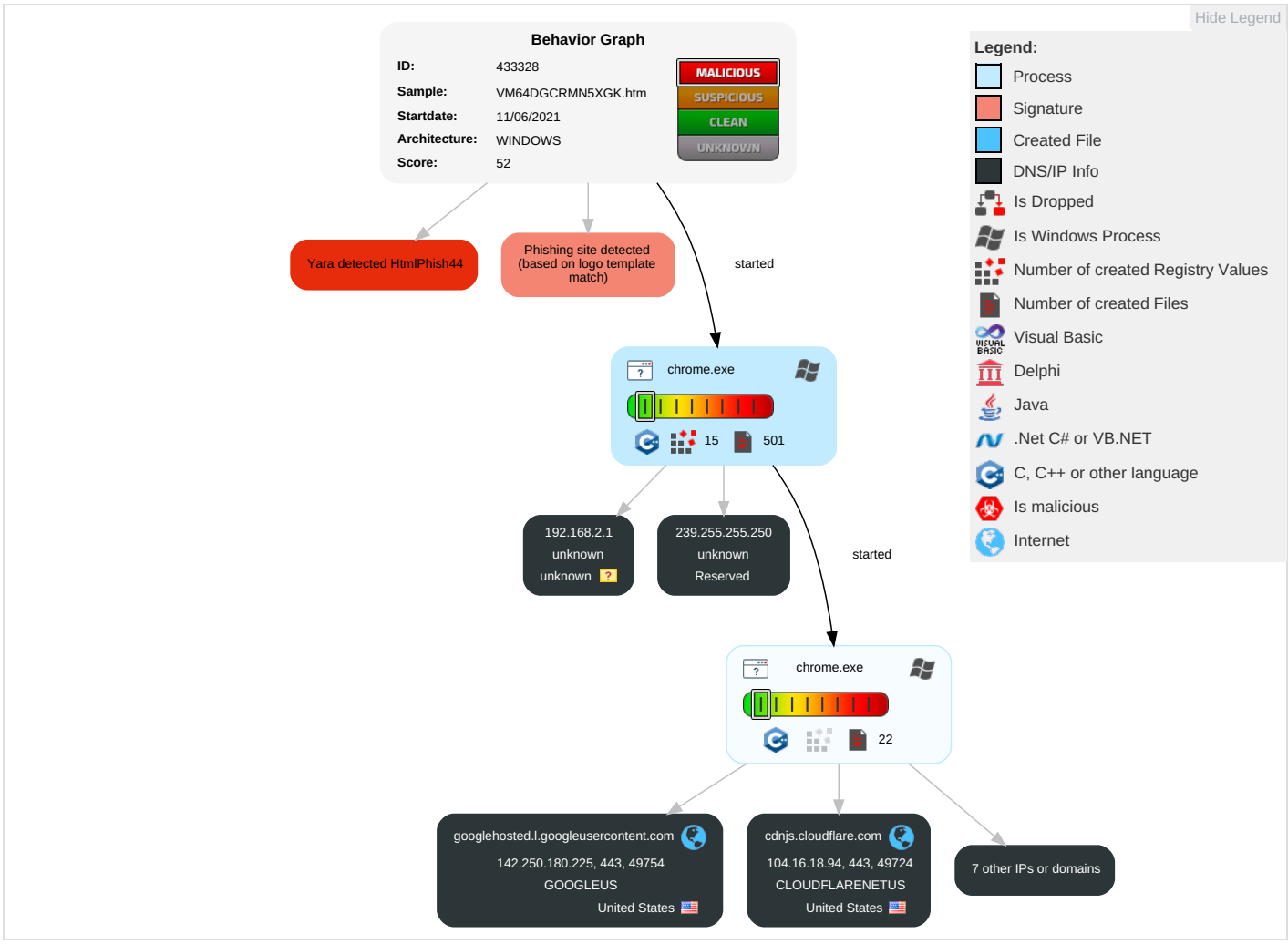
Yara detected HtmlPhish44

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

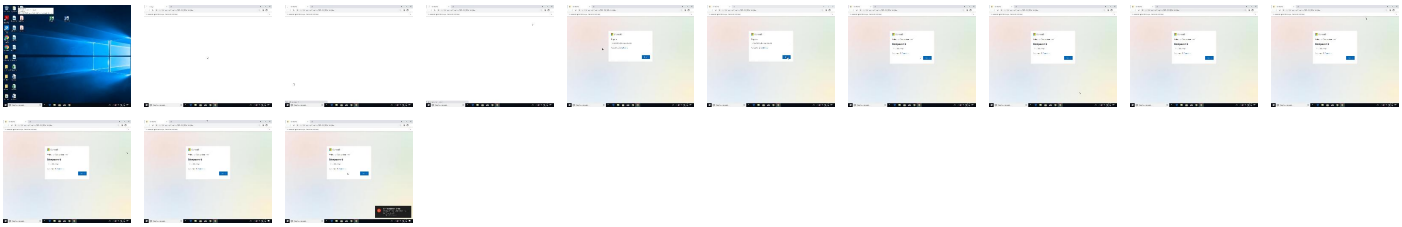
Behavior Graph

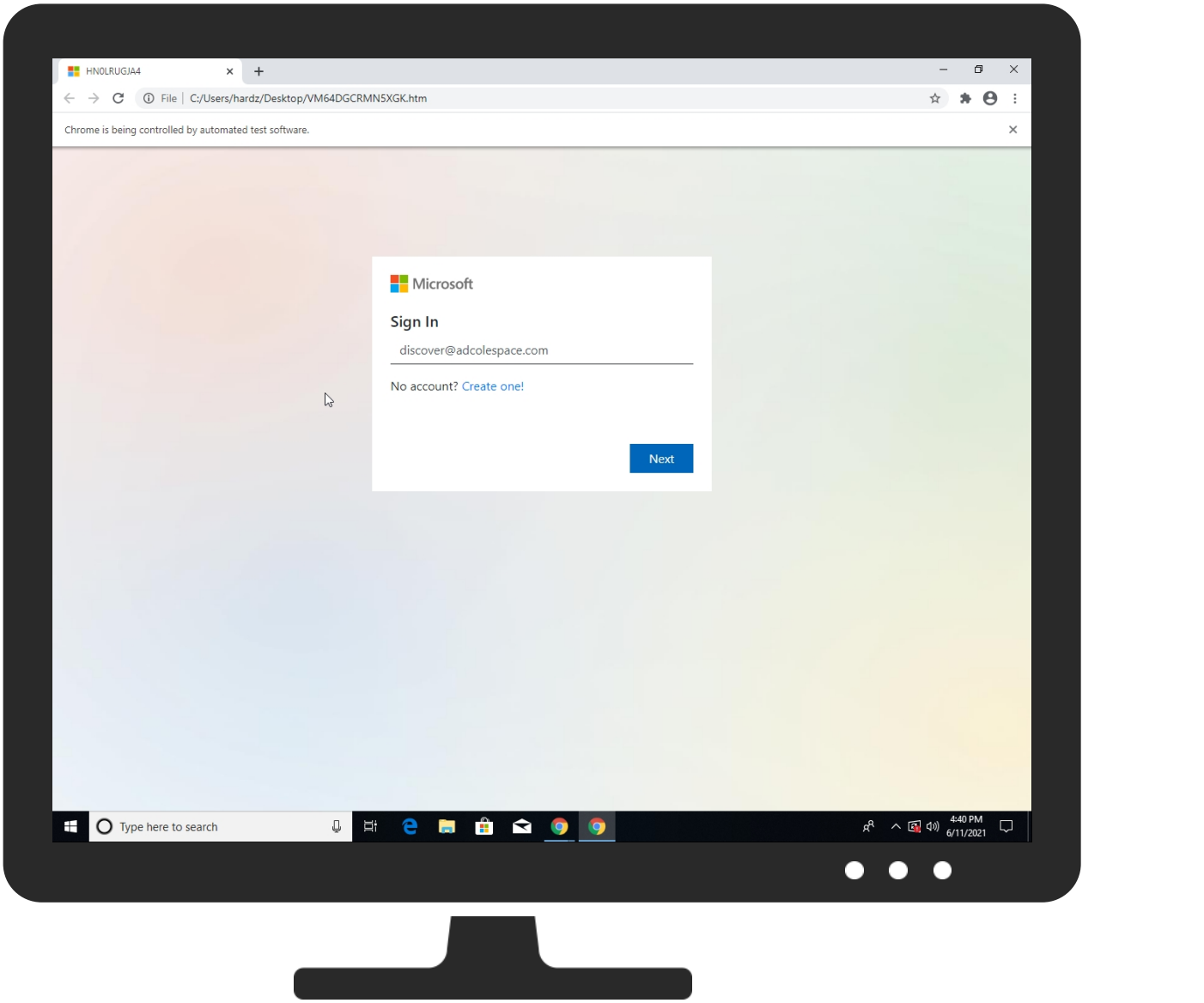


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdnjs.cloudflare.com	104.16.18.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
googlehosted.l.googleusercontent.com	142.250.180.225	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/VM64DGCRMN5XGK.htm	true		low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.180.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	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:	32.0.0 Black Diamond
Analysis ID:	433328
Start date:	11.06.2021
Start time:	16:39:57

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VM64DGCRMN5XGK.htm
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.phis.winHTM@41/234@7/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:40:52	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
104.18.11.207	#Ud83d#Udce9-peter.nash.htm	Get hash	malicious	Browse	
	Check 57549.Html	Get hash	malicious	Browse	
	#Ud83d#Udda8northerntrust.hscni.net 692233150-queue-7828.htm	Get hash	malicious	Browse	
	Paid INV for Robert.landis Khs-net.htm	Get hash	malicious	Browse	
	Payment Advice 006062021.htm	Get hash	malicious	Browse	
	New_Messagejacob@steinborn.comMessage.html	Get hash	malicious	Browse	
	Return-message4928.html	Get hash	malicious	Browse	
	new_fax_message.html	Get hash	malicious	Browse	
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	
	Secured-Message_7634-7.html	Get hash	malicious	Browse	
	_Vm064855583.HtM	Get hash	malicious	Browse	
	VM60VWPCVNQS5D.html	Get hash	malicious	Browse	
	PAID Invoice name@gmail.com.htm	Get hash	malicious	Browse	
	Ao_Scan_item.htm	Get hash	malicious	Browse	
	redcape.com.au-857585.htm	Get hash	malicious	Browse	
	#U266c Voice_Audio_845021.htm	Get hash	malicious	Browse	
	Wynnlasvegas_Scan_item.htm	Get hash	malicious	Browse	
	Sait_Message.htm	Get hash	malicious	Browse	
	DOC597-597.htm	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Retrieve_Messages65904_40_55am.html	Get hash	malicious	Browse	
239.255.255.250	fuoAl0V94I.exe	Get hash	malicious	Browse	
	Fax_Doc#01_5.html	Get hash	malicious	Browse	
	ATT00005.htm	Get hash	malicious	Browse	
	Evershedsnicea NDA file attach...htm	Get hash	malicious	Browse	
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	
	Kancelaria Marszalka's-Protected-Fax.htm	Get hash	malicious	Browse	
	Docc.html	Get hash	malicious	Browse	
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	
	wzdu53.exe	Get hash	malicious	Browse	
	WheelerIndustries_Doc#92543.htm	Get hash	malicious	Browse	
	Remittance-Advice.htm	Get hash	malicious	Browse	
	#Ud83d#Udda8rocket.com 1208421(69-queue-2615.htm	Get hash	malicious	Browse	
	INVOICE-PAID_02PDF.html	Get hash	malicious	Browse	
	Payroll Adjustment for employee.html	Get hash	malicious	Browse	
	0F4F0709D120ABA22D4687BFABFA5004DD54B0FCC6EF1.exe	Get hash	malicious	Browse	
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm	Get hash	malicious	Browse	
	212161C3EFE82736FA483FC9E168CE71#U007eC2#U007e1B6B2C73#U007e00#U007e1.xlsx	Get hash	malicious	Browse	
	212161C3EFE82736FA483FC9E168CE71#U007eC2#U007e1B6B2C73#U007e00#U007e1.xlsx	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.383129.23206.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.383129.29566.exe	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://j.mp/2URXSx8	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/33I4Nht	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2Gwx0iC	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/3jDHDOo	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://Kardanan.com	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/datamaps/0.5.8/datamaps.all.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	payload.html	Get hash	malicious	Browse	• 104.16.18.94
	Ref#Doc30504871 Wyg.htm	Get hash	malicious	Browse	• 104.16.18.94
	Evershedsnicea NDA file attach...htm	Get hash	malicious	Browse	• 104.16.18.94
	Check 57549.Html	Get hash	malicious	Browse	• 104.16.19.94
	7 #U039c#U0456#U0455#U0455#U0435d #U0441 #U0430II#U0455.htm	Get hash	malicious	Browse	• 104.16.19.94
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	• 104.16.19.94
	wzdu53.exe	Get hash	malicious	Browse	• 104.16.19.94
	The Village.html	Get hash	malicious	Browse	• 104.16.19.94
	#Ud83d#Udcde VM_58490931 Recoding.wav - 20223 PM.htm.htm	Get hash	malicious	Browse	• 104.16.19.94
	#Ud83d#Udda8northerntrust.hscni.net 692233150-queue-7828.htm	Get hash	malicious	Browse	• 104.16.19.94
	2ff0174.dll	Get hash	malicious	Browse	• 104.16.18.94
	Paid INV for Robert.landis Khs-net.htm	Get hash	malicious	Browse	• 104.16.18.94
	06.08.21 Inv & AP Statement - Copy.htm	Get hash	malicious	Browse	• 104.16.18.94
	#Ud83d#Udda8rocket.com 1208421(69-queue-2615.htm	Get hash	malicious	Browse	• 104.16.19.94
	Payment Advice 006062021.htm	Get hash	malicious	Browse	• 104.16.19.94
	A4C57DF59F0C85EEBCB7B40263D8C3DE037F41B7D2D43.exe	Get hash	malicious	Browse	• 104.16.18.94
	receipt620.htm	Get hash	malicious	Browse	• 104.16.18.94
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm	Get hash	malicious	Browse	• 104.16.19.94
	original phishing email.html	Get hash	malicious	Browse	• 104.16.18.94
	212161C3EFE82736FA483FC9E168CE71#U007eC2 #U007e1B6B2C73#U007e00#U007e1.xlsx	Get hash	malicious	Browse	• 104.16.18.94
maxcdn.bootstrapcdn.com	payload.html	Get hash	malicious	Browse	• 104.18.10.207
	#Ud83d#Udce9-peter.nash.htm	Get hash	malicious	Browse	• 104.18.11.207
	Evershedsnicea NDA file attach...htm	Get hash	malicious	Browse	• 104.18.10.207
	Check 57549.Html	Get hash	malicious	Browse	• 104.18.11.207
	7 #U039c#U0456#U0455#U0455#U0435d #U0441 #U0430II#U0455.htm	Get hash	malicious	Browse	• 104.18.10.207
	The Village.html	Get hash	malicious	Browse	• 104.18.10.207
	#Ud83d#Udda8northerntrust.hscni.net 692233150-queue-7828.htm	Get hash	malicious	Browse	• 104.18.11.207
	Paid INV for Robert.landis Khs-net.htm	Get hash	malicious	Browse	• 104.18.11.207
	#Ud83d#Udda8rocket.com 1208421(69-queue-2615.htm	Get hash	malicious	Browse	• 104.18.10.207
	Payment Advice 006062021.htm	Get hash	malicious	Browse	• 104.18.11.207
	receipt620.htm	Get hash	malicious	Browse	• 104.18.10.207
	original phishing email.html	Get hash	malicious	Browse	• 104.18.10.207

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New_Messagejacob@steinborn.comMessage.html	Get hash	malicious	Browse	• 104.18.11.207
	Return-message4928.html	Get hash	malicious	Browse	• 104.18.10.207
	Sealant Specialists, Inc. Projects #2021-Proposal #19100.html	Get hash	malicious	Browse	• 104.18.10.207
	VM60VWPCVNQS5D.html	Get hash	malicious	Browse	• 104.18.11.207
	PAID Invoice name@gmail.com.htm	Get hash	malicious	Browse	• 104.18.11.207
	mal.html	Get hash	malicious	Browse	• 104.18.10.207
	mal.html	Get hash	malicious	Browse	• 104.18.10.207
	mal.html	Get hash	malicious	Browse	• 104.18.10.207

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	1EFNborqwh.dll	Get hash	malicious	Browse	• 104.20.185.68
	OrderKLB210568.exe	Get hash	malicious	Browse	• 104.16.13.194
	Purchase_Order.exe	Get hash	malicious	Browse	• 104.21.64.212
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 172.67.188.69
	b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe	Get hash	malicious	Browse	• 104.26.9.187
	LsWgkxVLk1.dll	Get hash	malicious	Browse	• 104.20.184.68
	HHHyXsu7Vj.dll	Get hash	malicious	Browse	• 104.20.184.68
	7Nboq835Fc.exe	Get hash	malicious	Browse	• 104.21.19.200
	moq fob order.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQP000001488.doc	Get hash	malicious	Browse	• 172.67.188.154
	proforma Invoice (2).exe	Get hash	malicious	Browse	• 104.21.19.200
	0900000000000090000.exe	Get hash	malicious	Browse	• 172.67.188.154
	3.exe	Get hash	malicious	Browse	• 162.159.13 5.233
	01ekkRSMzb.dll	Get hash	malicious	Browse	• 104.20.185.68
	Invoice_OS169ENG 000003893148.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	INVOICE.exe	Get hash	malicious	Browse	• 104.21.29.70
	Request Quotation.exe	Get hash	malicious	Browse	• 104.21.19.200
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 172.67.169.41
	Shipment Invoice & Consignment Notification.exe	Get hash	malicious	Browse	• 172.67.188.154
CLOUDFLARENETUS	1EFNborqwh.dll	Get hash	malicious	Browse	• 104.20.185.68
	OrderKLB210568.exe	Get hash	malicious	Browse	• 104.16.13.194
	Purchase_Order.exe	Get hash	malicious	Browse	• 104.21.64.212
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 172.67.188.69
	b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe	Get hash	malicious	Browse	• 104.26.9.187
	LsWgkxVLk1.dll	Get hash	malicious	Browse	• 104.20.184.68
	HHHyXsu7Vj.dll	Get hash	malicious	Browse	• 104.20.184.68
	7Nboq835Fc.exe	Get hash	malicious	Browse	• 104.21.19.200
	moq fob order.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQP000001488.doc	Get hash	malicious	Browse	• 172.67.188.154
	proforma Invoice (2).exe	Get hash	malicious	Browse	• 104.21.19.200
	0900000000000090000.exe	Get hash	malicious	Browse	• 172.67.188.154
	3.exe	Get hash	malicious	Browse	• 162.159.13 5.233
	01ekkRSMzb.dll	Get hash	malicious	Browse	• 104.20.185.68
	Invoice_OS169ENG 000003893148.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	INVOICE.exe	Get hash	malicious	Browse	• 104.21.29.70
	Request Quotation.exe	Get hash	malicious	Browse	• 104.21.19.200
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 172.67.169.41
	Shipment Invoice & Consignment Notification.exe	Get hash	malicious	Browse	• 172.67.188.154

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wlEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,....,qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j._iK..|[.w.M.!<- .}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vI..x.R4...L.....%g...<..}'{....E8SI...E".h...*.....ItVs.K..... .3.9.I..`D..e.i`....y....,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._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):	328
Entropy (8bit):	3.1179760176564173
Encrypted:	false
SSDEEP:	6:kKvOe8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:3O8kPlE99SNxAhUe3OMx
MD5:	2D343F0418570D460F5B836D59FC35AE
SHA1:	4FCDF8CA37FD5D5F3B581DCEA2FC6007343A40C3
SHA-256:	3D44DC9038715860 97B7862E32594A026E27A81899260F14D0E0BBFFE40F617D
SHA-512:	C1C737FCC1584135E23E96A6D4500108644265456AF6548749C865ABCBA5553B11DBCC40C7472B3E0050626B8DCB4E4CF6CAE44EF958498C9942D3C85B54FF7
Malicious:	false
Preview:	p..... .....3]7._..(..... ....L.....&.....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..."..0.9.0.e.6.c.f.e.3.4.c.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0b001933-9d40-4ea5-a5d3-02b86b438f6e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\0b001933-9d40-4ea5-a5d3-02b86b438f6e.tmp	
Size (bytes):	164210
Entropy (8bit):	6.050682562801691
Encrypted:	false
SSDEEP:	3072:7UdLgVDqfsAtDzQFU36fdYPL8JPfFcbXafIB0u1GOJmA3iuR3:UgIRXv6fWPL8VtaqfllUOoSiuR3
MD5:	11647D5104EB6C93F1E9F620D3F1FAC7
SHA1:	34FCBB8B3BB237032D8D7225E12E8208FED7D8AF
SHA-256:	3CF54EBD62963DA387D33FD1562B735F7DCA70989CBC2D10913305F69B7480A9
SHA-512:	F62D6DD3409F90A85D004E52B6DB5F801FFC9E774E125DD1DCF6CAD87E3B392044D4D8A5EB98A9306247EFF2598B9604CAFE6ABFE7AE881F919E526DEF03436
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":1.623454850981402e+12,"network":1.623422452e+12,"ticks":100003068.0,"uncertainty":3344572.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016525165"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\2377f8f9-75a9-45c2-958f-f3a657af669d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7522044667729593
Encrypted:	false
SSDEEP:	384:h3NyqUPNw3AuVn52pNar/vOG3luQ9H4tGRorzQOcxdIkQnrvWmDgzgqaWJOIE6N3:xG+5ZqoxpAengq0ov3meK4Ga5T
MD5:	882712EB897C64E54563DD6DFBF3FFCD
SHA1:	86015FBD1ADE55B0F7B944F16661EB9AEF787663
SHA-256:	B1A6712D3C693A754A6CFA8682639F9295863C2F53518D6657226F8B4F009D30
SHA-512:	EBD7B7FCD33228090EA3A33974587DC2251C8FA152B603540A064C88E14F0BDA97BF56AF13409D941CC655D56E636721B66BADF4FF189D8DF1580BFF5C988C6
Malicious:	false
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<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\31c2f8ec-ba94-4c15-88d8-274265b99884.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):	172395
Entropy (8bit):	6.079974640951283
Encrypted:	false
SSDEEP:	3072:34PfdLgVDqfsAtDzQFU36fdYPL8JPfFcbXafIB0u1GOJmA3iuR3:Q9gIRXv6fWPL8VtaqfllUOoSiuR3
MD5:	4DCF7DFD6D309C968E99FFC8EF9ACFDE
SHA1:	329334F38D9D969D7A2F28B6748347812852916F
SHA-256:	52F69E0CD796FFDB7D54D4C48F0B51D1D892D59154609F58DFFF3ED40B0B7E6B
SHA-512:	C4F5C0CDB72BCC76521042C09DBBA3B18390148810098579BCB8C0FB0D5AD6B4A511F2FC73987F981F5AB98752CE8C63F16BA37818005CB5AD286F939B93601
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":1.623454850981402e+12,"network":1.623422452e+12,"ticks":100003068.0,"uncertainty":3344572.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\3572c2fd-4f60-4e08-8dcf-89b881f8f909.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7519403790863466
Encrypted:	false
SSDEEP:	384:R3NyqUPNw3AuVn52pNar/vOG3luQ9H4tGRorzQOcxdIkQnrvWmD3dzgqaWJOIE6L:BG+5ZqospAengq0ov3meK4Ga5V

C:\Users\user\AppData\Local\Google\Chrome\User Data\3572c2fd-4f60-4e08-8dcf-89b881f8f909.tmp	
MD5:	8B082EE2CE4BD0DC5CD49731E5BD20A1
SHA1:	235563907E0D29B3C6DE94C6E3951ED73814CFE4
SHA-256:	D318EA0350E6B7843218178FD8FAE1F1E17EABDB91C5714865D4D106FAB5779D
SHA-512:	A4C937222CF37E554629EF70AD14222F9918103EDE634182887179BC108B8FF73F77C1C7795EF82742A02A921255F1BB16BFD9D0FEF407CC692B905C8C7A3DCE
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....<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\38a1d290-51a7-4b8a-a294-37ff7118c434.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):	163919
Entropy (8bit):	6.0498186494420825
Encrypted:	false
SSDEEP:	3072:7tdLgVDqfsAtDzQFU36fdYPL8JPfFcbXafIB0u1GOJmA3iuR3:jgIRXv6fWPL8VtaqfIlUOoSiuR3
MD5:	1839C43B8EA9407E13B28A120AC328F1
SHA1:	B9BCB17497F7976D85BF62CF5A01A497B8002D26
SHA-256:	18380A5557FF3114F3B5F94D423A54D282CA64B75478506E2E61E597CFB1946F
SHA-512:	985716DB0FDD7B757F8FDE60F147F2F1B2FBF56B63C6FAC0C66AF82481E5DF748A9BFC353626C30A91C0B67EE722224E26ABD1C3EEAA02BFDB62DDD1C7A1AF67
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":1.623454850981402e+12,"network":1.623422452e+12,"ticks":100003068.0,"uncertainty":3344572.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016525165"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\567590dd-fe12-456d-8b67-f1de7c8ea158.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):	164367
Entropy (8bit):	6.0512092099065535
Encrypted:	false
SSDEEP:	3072:7pdLgVDqfsAtDzQFU36fdYPL8JPfFcbXafIB0u1GOJmA3iuR3:PgIRXv6fWPL8VtaqfIlUOoSiuR3
MD5:	951422860B08B4D29503A981B753C430
SHA1:	E0553A030297B736D4F2861FF4229C95F0159CE5
SHA-256:	59C5B9A77D01CEB53EA4521BC7A16348DA46F508BF6FC5447089DF4D3778E995
SHA-512:	89CAE6758C201518121EF1460284782C32BE7105DF31601ECBA9911E73A68D70E1CF67D36DD425D02948D6BA0368DEE55164D87B2BF8528C35BB8B501DF64A4
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":1.623454850981402e+12,"network":1.623422452e+12,"ticks":100003068.0,"uncertainty":3344572.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13

C:\Users\user\AppData\Local\Google\Chrome\User Data\65a2381d-810a-40a7-9bde-7aecd6c22517.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):	164117
Entropy (8bit):	6.050410163043138
Encrypted:	false
SSDEEP:	3072:7ldLgVDqfsAtDzQFU36fdYPL8JPfFcbXafIB0u1GOJmA3iuR3:TgIRXv6fWPL8VtaqfIlUOoSiuR3
MD5:	F1BD7416FB7A4BE455EC0AB1C077FB9F
SHA1:	D2E4F46A1D71BDFB61CE8C23C2F346625AF51F8E
SHA-256:	DCBCDA7CCD66C266D3130B325BD90B726A5B21D6E893CDD770CA57BB57743F2C
SHA-512:	2257135460BC9CB2C9E69D731B6F53AAB56918AABE415ADC55E649E89F7FE77E207953069A8FF1312D1A8014161CE19A09216E48E9560C96216FFB60C55661A6

C:\Users\user\AppData\Local\Google\Chrome\User Data\65a2381d-810a-40a7-9bde-7aecd6c22517.tmp	
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":1.623454850981402e+12,"network":1.623422452e+12,"ticks":100003068.0,"uncertainty":3344572.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016525165"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\90ffe7aa-65be-4d3a-94c2-aa320f15c1d3.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):	172395
Entropy (8bit):	6.079974547830846
Encrypted:	false
SSDEEP:	3072:y4ePdLgVDqfsAtDzQFU36fdYPL8JPfFcbXafIB0u1GOJmA3iuR3:UNgIRXv6fWPL8VtaqfllUOoSiuR3
MD5:	6490A2CDF022F8340CE5DB45BA6E1A18
SHA1:	13A0660E7560C9BE402A842597A982616DBD0445
SHA-256:	7151E0E3EFAA83B5AE48E94A448B97CF8310C7D624D8E5BB0C3A6470D4D97445
SHA-512:	FEC663BD17EFBD8DD6195ACC91E779213B15EF7073CA2434830899EE50D892E3D160E20E04619B8ECB3325011CAC7DB43A3A7F7F99AB82D5258B490692C37AB
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":1.623454850981402e+12,"network":1.623422452e+12,"ticks":100003068.0,"uncertainty":3344572.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016525165"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\965857ce-1b9d-4598-8b36-215d0e9ede38.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.75184448494432
Encrypted:	false
SSDEEP:	384:n3NyqUPN0Av2pNar/vOG3luQ9H4tGRorzQOcxdIkQnrvWmDgzgqaWJOIE6Nb1KDO:3+5ZqoxpAengq0ov3meK4Ga5R
MD5:	0E5D48605A7B20ED6FE42B92BFFBD9C2
SHA1:	B808C590F04283466AA119706D2C3EB7AA9FAB41
SHA-256:	80FC1A7906C311D8C60AED5F63F419680EDB088A029D87E092F7F5E8F4071EFA
SHA-512:	26A785D759E4F350D2D35D3058A5F35E9C92E340F19D3053AF2EC3C90AE0E981FC3F48C1AC46E24A16FA054367234A4FBC62EAE7F42DFA10355F2F1FD3E2D42
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....<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\24e7542d-63e6-4729-b9bb-fef50aa04faf.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):	1709
Entropy (8bit):	5.594505051475484
Encrypted:	false
SSDEEP:	48:YDVwUQl6UUhwLeUaiKU+UVqPeUer2UefywUwYIsYU+Uenw:TU1UUjUFKU+UAPeU9UE/UR5YU+UD
MD5:	8D9E9056A2D91EFA7C7E64BF04DA8AD7
SHA1:	3EEA31D2881A167001D107757F472FBD77EBEF84
SHA-256:	861832F6D0232A98915246FB1124C750757874DBF04FB77CF92E5AE29ABADCE1
SHA-512:	E5C201983F5959C74979C344F5C010BD16DD1F95B5D00E7561D4C4E4C6B482E88B27D6F9C8DD5D4EB67DB458DA7EE91A6A3F1BFE4061E327B1DC2934BDF169 E
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1639234852.464363,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623454852.464367},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1654990852.247365,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623454852.247368},{"expiry":1654990852.246729,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623454852.246733},{"expiry":1654990852.450791,"host":"qaDeFdT1UTirY0OQe+c5LKw+zjx6vF/+3vFh7CgrAOY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623454852.450796},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\43680336-f854-4d75-b675-1439ef88035f.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):	5.536574134444547
Encrypted:	false
SSDEEP:	384:6j1vu+tQsLlfYgaXGZ1kXqKf/pUZNCgVLH2HfDuhrU0HGInT9S0Nk4x:6JGhsLlfrIGZ1kXqKf/pUZNCgVLH2Hfw
MD5:	76613D5AF26F9015D52044D4C0ECB4EC
SHA1:	9377753161BCC046B17FF0FC0638B5C475FB9B2E
SHA-256:	C3C9375AC0211D3E1D9FE123D34851F19698D32E4A864602D588D5A8E95A2953
SHA-512:	7DC85922810339C365866CEAA2C53329AD9CC31A1521F9E1FB62A72C5EACD52616378F60289FDBF887F6426959DE87290903D7D13D570E02EDEC653D3F01B28A
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":"13267928448515303","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\5d8a35a9-9fbc-4d84-b1e4-0f2fc94eccd4.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):	5465
Entropy (8bit):	5.184530186529403
Encrypted:	false
SSDEEP:	96:nLOgCB5I2RzZxJUUcVcvok0JCKL85bOTQVuwn:nLOgCs2Rz7JUUcd4Ku
MD5:	ED2E2289CCF51EB8F6C51E772F92AD8A
SHA1:	0567E8755EF8B237E1B4A7F02B4D6742CA7D47C8
SHA-256:	13EED98E6F93887D02553A6C08A252495CD25A1CB65EB1FC917D6DCE600E41B4
SHA-512:	8A163D942C75F046CA149EF0D35D79BFEC154496EC9240918E654615831C2369F8B97D290AF912EFE1D2E095313495139EEFBADAEC9FCDB810672C9E3C1764E
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267928448771950","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","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\98f9dc64-bb1e-4b43-a717-d8d23b01889b.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\98f9dc64-bb1e-4b43-a717-d8d23b01889b.tmp	
Entropy (8bit):	5.5780753897942414
Encrypted:	false
SSDEEP:	384:6j1vu+tnsLlfYgaXGZ1kXqKf/pUZNCgVLH2HfDuhrU1S2/k43:6JG8sLlfrIGZ1kXqKf/pUZNCgVLH2HfH
MD5:	60496506BA03ACF06E9BA656AB5C26D2
SHA1:	DC4217696E05B000CDB252AC2D6EE9E030645A5F
SHA-256:	F97254501E5C57AF5DBC586424454B568C17A1A7AD4D85BC5F39081175489F00
SHA-512:	94B4DC0A14B44FB941D2D05725663B2C05A08B82B9823DCA6CF6D903F199ED9FF5F59F72966841BB1B05E9B31F49994B35A2D333A17AFC5BEA51751759ED8CB
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":"13267928448515303","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\992f9b34-29ad-4029-ba89-6a7ae3abacac.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\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.190096521328156
Encrypted:	false
SSDEEP:	6:mwASIq2PWXp+N23iKKdK9RXXTZIFUtpDAIJZmwPDA1kwOWXp+N23iKKdK9RXX5LJ:wva5Kk7XT2FUtpDJ/PY5f5Kk7XVJ
MD5:	94E23CA4700D52BAE52BA0D31136CD48
SHA1:	73B6523C4AD54B57809568C2ACD1696117AE99DF
SHA-256:	67B9792010D887ED30CF08A7C49523CBC239CC79734CEF9407DE9AE2645F077F
SHA-512:	B67084BD076CB63E0AF7090CD697081314E49E7F6722E36F9149B6D7BAA931FC21DACF8275AF63B1CA5A84E40AA4F6E14C31F5C96D934E5AD09ECCFE1B2F2D8
Malicious:	false
Preview:	2021/06/11-16:41:01.810 a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/06/11-16:41:01.814 a54 Recovering log #3.2021/06/11-16:41:01.815 a54 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.178072148382863
Encrypted:	false
SSDEEP:	6:mwAVq2PWXp+N23iKKdKyDZIFUtpDAvVJZmwPDAvVDkwOWXp+N23iKKdKyJLJ:eva5Kk02FUtpWJ/PWD5f5KkWJ
MD5:	A22D9DBACBF2205F6C767CC5A02D82BC
SHA1:	78CE66D3AEA9CF9CCA4F8014BBBF1180E3C0E55A
SHA-256:	FC9A2DBBE14FF25AE6CE10D74906A67C6DB73B725EF5E385B18176CBBD3CD824

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
SHA-512:	03F1041A1B1FA4272A825F5D2F78D1BC8F5A47F3FBD63CA167AB58CFBBA8AEEAF48E3A4EFD52A198F756D097788C64FD0C3BE64CAFF03428306828EED71274 A
Malicious:	false
Preview:	2021/06/11-16:41:01.805 a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/11-16: 41:01.806 a54 Recovering log #3.2021/06/11-16:41:01.806 a54 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:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC761 F
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):	0.9695883551006309
Encrypted:	false
SSDEEP:	24:kcLgAZOZD/Gl4qLbJLbXaFpEO5bNmISHn06Uw+t8:k8NOZGl4q5LLOpEO5J/Kn7UL8
MD5:	BF2F423EAAFECC148C47B0F8C68B9222
SHA1:	F39AD5CC3BF49795D7755080D4DFF508151FA25C
SHA-256:	D608B30A09D12EE89D78EE6E9D9605461DEF142856367B5D894AF030BDB4B198
SHA-512:	232609D9AEA8A76A19B6314ED6525293EDFA119B9D95693C9F4B069DE4D51FC51014252C8026156BCCCAB9DAC590EBC7B8DB650E9D9F25A493C6954211C760
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2017
Entropy (8bit):	3.2432847374586355
Encrypted:	false
SSDEEP:	24:34SWWmalrlAKZuh7sU83wuO+MuoDsff3mLe6WuO+J+gt/lr:34t4xPm7n8G2fY3Lr
MD5:	4C0CA67B60B7E230A5C35045E17EAB61
SHA1:	5B2468200A0A15C32D40B952898D3F9D75117BE2
SHA-256:	BE8EC1F727CA22DB97ED89BA1DC5B823E6080E00B06FB3D58DBE172FCF4CB766
SHA-512:	3696AABF6BFAC85812E72C95F28D946263CE7271546AACE1BCA11197FD96A0C7014D21CDA2BFAC7DD469987355D29F821DD1AB2624F9945AF4BF81FDA5FD23 F
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...90682165_97bb_436f_88f6_ac5d7fe64e16.....C..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....|.....1...file:///C:/Users/user/Desktop/VM64DGCRMN5XGK.htm..... .....h.....`.....(.....j...1...f.i.l.e.:././.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.V.M.6.4.D.G.C .R.M.N.5.X.G.K...h.t.m.....8.....0.....8..... .....1...file:///C:/Users/user /Desktop/VM64DGCRMN5XGK.htm.....=*R.#/.....1...file:///C:/Us

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.224511250437663
Encrypted:	false
SSDEEP:	6:mwArJwVq2PWXp+N23iKKdK8aPrqIFUtpDAr8gZmwPDAr8IkwOWXp+N23iKKdK8a4:5va5KkL3FUtpC/Pu5f5KkQJ
MD5:	FD71D2492766CB237E1718FD0970B51D
SHA1:	AC914A30C3D595E34305FA88DE7784560492BE44
SHA-256:	E548693DE2A997ED36FB09F148E11619F58811B227E3F0B40EC87C19D9109AF6
SHA-512:	3235741E872E02A9E11FDD819CC0E9CB6E8285C3D42774EBDECE0B47FF51CF48BF44D7820EB1624CE782B967B5260159D5997CBCA75F9BC1197623CCAE64D3 3
Malicious:	false
Preview:	2021/06/11-16:40:48.769 604 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/06/11-16 :40:48.770 604 Recovering log #3.2021/06/11-16:40:48.770 604 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4 C
Malicious:	false
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5................f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.212366727608324
Encrypted:	false
SSDEEP:	6:mwArl0Vq2PWXp+N23iKKdK8NIFUtpDArtgZmwPDAraT2IkwOWXp+N23iKKdK8+ed:Bva5KkpFUtp9/PTh5f5KkqJ
MD5:	4B3A3658A73EB1D2170BE64024DF46DC
SHA1:	E62FB2155EA6A753D62E8EF226E82F307909CE37
SHA-256:	12747B4239015F836FE9CAC92F5FFD0B1D7B2ECA0411357A79AFFFEFFD7123A7
SHA-512:	372148E65FEF4F73C6D15E60D63C4A44E9ED84B601D6102FB8996CA8CCD8186E924A79A81988DF11C9253725564DDA3EA1F3C4DB8390CA526DD65941D8F3C8(
Malicious:	false
Preview:	2021/06/11-16:40:50.928 604 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/06/11-16 :40:50.929 604 Recovering log #3.2021/06/11-16:40:50.930 604 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+e5QxYbUsclJ5 n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","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+e5QxYbUsclJ5 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	43008
Entropy (8bit):	5.156379119633358
Encrypted:	false
SSDEEP:	768:xZ7FZnNTNyN2LODl8vdQNoNTOcZRLbD18vdQNVmjm:xZRZnNTkN2LQuuoNTzZRLfeu/
MD5:	C44D624BA7D82623D26718BD5FAA1E5C
SHA1:	E61182D9FB3A53713EC7DDE061349F3D419F7689
SHA-256:	0B1F2CF4047BB092607E5DF17B94990215433049D3F8D4932B1EFDC6BDE1CB9A
SHA-512:	80624C9481FB6E2E2C8A1844D9A099084BA08F031875EC63775A951AF6C197F8D0A5130E35C11C5C7CE954B630BE8D0AF91A05EB1F201D72234ADB4DA8CA848
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7766092042978093
Encrypted:	false
SSDEEP:	24:y/yLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwf5CM8SSsUE3n:y/dBmw6fUi5CM8SSsUE3n
MD5:	910DC5331C56657320AF6FB39D054537
SHA1:	F0EDC46EC916A2A38D82E85D3E0FEE77C7424548
SHA-256:	6CF2549A14DB05513D365B8A3ED71352D79C74B08CBCD795D53C58221514E1F0
SHA-512:	7167EDFE46369079892C637783A7325C8460AF2418524393EB9BA4E9000E2C52532079DDDCC88BAE3F2852C80262720D7BDD0803FA707B677BAA4D095BA651B1
Malicious:	false
Preview:	.....X..... .....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.251263876101758
Encrypted:	false
SSDEEP:	6:mwAd4q2PWXp+N23iKKdK25+Xqx8chI+IFUtpDAaZmwPDADDkwOWXp+N23iKKdK2L:64va5KkTXfchI3FUtpJ/PcD5f5KkTXfE
MD5:	2F6609ACF06E5D69E268C827096B3F3B
SHA1:	4401A6EF902B98B753A15F07AFD21EF18ADE4521
SHA-256:	498D24346C2C93A17B95FE4A762D7F598D276AE993AF77AC1C212C4D2982B04F
SHA-512:	878ECF526A852B16B6B9A1C274D6FF612A1589BA7EFA7CE5CF837E62055ED87D8D0E6C02D5590BF3CE79BB413B5084337CD8F87C6D2AE4CBD041152DC020929
Malicious:	false
Preview:	2021/06/11-16:41:01.774 a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/06/11-16:41:01.775 a54 Recovering log #3.2021/06/11-16:41:01.776 a54 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.2239160232272575
Encrypted:	false
SSDEEP:	6:mwA3QMq2PWXp+N23iKKdK25+XuoIFUtpDAlVJZmwPDAZkwOWXp+N23iKKdK25+Xp:w1va5KkTXYFUtpO/Pg5f5KkTXHJ
MD5:	F04FF5A00438D84E4559D1BDB51887B2
SHA1:	053E3CC9092A9930400433D412F9D78F2E939870
SHA-256:	5C9DEC956A88008F40A0BC7C5EBC554EA2FD1B5FF2414CA818E2823C3AF9CDED
SHA-512:	EC7138B9C5544B14D8CBACF7ED6ED38425AA16FCF8723D29297B7F0BEDBCEB24AC07E643936FB3CE19FB1C2756D14AFB698A8B4D5A96EC7BBD4725A040C6E5F21
Malicious:	false
Preview:	2021/06/11-16:41:01.768 a54 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/06/11-16:41:01.769 a54 Recovering log #3.2021/06/11-16:41:01.770 a54 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):	5.2379196424836625
Encrypted:	false
SSDEEP:	6:mwAWQ+q2PWXp+N23iKKdKWT5g1IdqIFUtpDAFgZmwPDAFQVkwOWXp+N23iKKdKW4:a+va5Kkg5gSRFUtpf/PfV5f5Kkg5gS3e
MD5:	140C62CE8D24EB6FD2ADA74F71D487CC
SHA1:	54E71DB673AF417D6984E9343ACA6078611F001E
SHA-256:	5BBCDEAB5D4FDB601E3F977806F0AEC6C234FE24E484EDCABEC5ABE1654DC04F
SHA-512:	790ABDB8C90F14954D543028BB098D222C1F5E2B46EA354F5F1FAA327257430F9841122E38DDECC502B161FF7632303DF5F6F1916E73F83E722FF235EC609BDE
Malicious:	false
Preview:	2021/06/11-16:41:01.293 179c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/06/11-16:41:01.294 179c Recovering log #3.2021/06/11-16:41:01.294 179c 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):	0.44812403665442346
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
SSDEEP:	3:8Efl+5G:835G
MD5:	7E0BE4E60B3FA598F205BE0D6DFCC05F
SHA1:	014820BAF881EDD042576756441787130B3F24BA
SHA-256:	8CDEC09ECA5A40D02277B8E86FD635B62BA6047709764575B359F75DAC6CFD45
SHA-512:	A14274ADA7C1D7A3B1DEF371D466DE49C8C600A060F3ED9DB5375E63F2982530952C60D15746B077B8BABC19895082BF1617344FBB2AC10F0EB275B917B6430
Malicious:	false
Preview:	.'..(.....L.S.# /.....

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):	0.11137777872063645
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvIlsSbjF1K+GeeMIzbtoOo/lCxthid5iAGCxC+/er1cZ6CjF1KE:TL+A/8BEkImNuQ7iAGI/3gCBE+
MD5:	AE732B93A76FE38DEEE83F1E001C06AC
SHA1:	E581774BC63F08BEA72EC1A91B55686CC651ADC0
SHA-256:	8CE630916568D3B8773BC74625AFDF23A573FA3D67068B335E457DE963A54671
SHA-512:	4093AD8D1616B712193C40E8C6D9F6B105C8F6666392A4877AC549FD68861458C974B65C2E5132CA3AE1461F70AC4591310F70D6C16B1FE3E23467439F1DD0AA
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):	639
Entropy (8bit):	5.270369122276418
Encrypted:	false
SSDEEP:	12:Vq3h6Oq3N/uLXcornE60Y134wWWjbBLR7fLdzn1KXHBk778B/xgskZBbt1MZw4B1:GhzYNosorn8Y1ldgBL5fx1QhY78BJgsH
MD5:	41B755A1D7A58AAFBD4282C53B43583C
SHA1:	EE3712CE36FC3CE69C2FB728715F16BC5609B733
SHA-256:	EFFF93216DDC97633C58B08F868047F61DE853D4F9253F2BA7A7E46B62541A34
SHA-512:	AE105DFF52B00508530643DEA1A9EAE2537C5F16FD8CF79693246D9561C412708F53244D59602137DCB7FF6ED22702D2C87AEDC8AF78B23B942DBCBC1A9974C
Malicious:	false
Preview:	....."C....c..desktop..file..user..hn0lrugja4..htm..users..vm64dgcrmn5xgk*c.....c.....desktop.....file.....user.....hn0lrugja4.....htm.....users.....vm64dgcrmn5xgk..2..... 0.....4.....5.....6.....a.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....x.....z...: J.....Bc..._..... .....*1file:///C:/Users/user/Desktop/VM64DGCRMN5XGK.htm2.HN0LRUGJA4:.....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):	0.11660142839720934
Encrypted:	false
SSDEEP:	12:RMquMSMXpMDMuDMdTMoM/vqLBj/w3l+V94nMWQA9LDOmBQZ8fOv:5YvqLBw3rbN6mTfO
MD5:	3944C30AC9482E9FA0279720EE2C794A
SHA1:	3F45AB6438400B65C224BDD5104688BB695A6634
SHA-256:	123D28A417615563F5F199B534B598C764F50EE801A4EA99D96E349D04911E9D
SHA-512:	667595A7F337F2F2721194D05E739F0A6B2F4F1DF4876186071A71FEA55582064888788FA6D6B635E7806F3E49B8FFE73B7269E0A5B65035F07F1DE83D2799EA
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.464045928103709
Encrypted:	false
SSDEEP:	48:vxGUda7xMs8dbSaRwbQSefgG6NrS0U9RdiN97y:5a7xM/dbSaRwbQ5fgGmrS0Vy
MD5:	96748215F9BE9C3D07670B3D4596F966
SHA1:	8CAEFBA558DF3D5FCD247FA50053BAB9C26A1693
SHA-256:	1D2004182C844263523597D229852AD5E3F4892BE6AD8F5AE030E9230746EE5A
SHA-512:	8ABFF0DAF859B9ECCF7A8DA1316A7EE7B87BD51E8D692565B3E305E73BA13B25FF2769D0235E4B2148DCA877FE1DFFBBBAF4F787E5379781C6433A6125A45ACE
Malicious:	false
Preview:	.PC....*.....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..182035000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-06-11 16:41:05.11][INFO][mr.Init] MR instance ID: e9145708-9dbc-49cb-951f-1d3832f63790\n","[2021-06-11 16:41:05.11][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-06-11 16:41:05.11][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-06-11 16:41:05.11][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-06-11 16:41:05.11][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-06-11 16:41:05.11][INFO][mr.CastProvider] Query enabled: true\n","[2021-06-11 16:41:05.12][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):	329
Entropy (8bit):	5.143355418154902
Encrypted:	false
SSDEEP:	6:mwArivwVq2PWXp+N23iKKdK8a2jMGIFUtpDArg70gZmwPDArYIkwOWXp+N23iKKV:NAva5Kk8EFUtpD9/P25f5Kk8bJ
MD5:	9A720B95D893421565FF160AECCF9064
SHA1:	7BBC90A595DC8515755CEF9F5AE3C709B0FD3DFF
SHA-256:	100C652B8F5300FB9F34720B532762A4EB69CFAE5BC5345BA8AA131AE15BF6A5
SHA-512:	5817A16690617AA210F53B902DA855B2025950ECFA822DDFECFC598CB56411FA9B40CD91290BF57215209718C279E2AB63F47EEF54F777067A1A6A20B8F38D76
Malicious:	false
Preview:	2021/06/11-16:40:48.601 604 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/06/11-16:40:48.603 604 Recovering log #3.2021/06/11-16:40:48.604 604 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):	331
Entropy (8bit):	5.238928318135494
Encrypted:	false
SSDEEP:	6:mwArzAq2PWXp+N23iKKdKgXz4rRIFUtpDArcZZmwPDArXkwOWXp+N23iKKdKgXzW:fva5KkgXiuFUtpFZ/PO5f5KkgX2J
MD5:	A589701B90781B5F56F9D3A64AA834A6
SHA1:	5DC81C29B8F51165F0B253D557F6A93F471FF1E4
SHA-256:	09208431103989 22AAF9AE5466DA96AEFA5673B82784750D6B8A95228D37E917
SHA-512:	74B0E826B34BC76CF9AD31B39B41C618DD23C4FC0B520A9652C455D0B94C2EBECAF2312D55EFEDC93BBD11D916DE96D214C072C025C04DC974A4C384AB7F63E
Malicious:	false
Preview:	2021/06/11-16:40:48.798 2f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/06/11-16:40:48.799 2f0 Recovering log #3.2021/06/11-16:40:48.800 2f0 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):	1.2340098357622473
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUdzF2Zjha3aI4s:wIElwQF8mpcSVW3KdzisvmEr1
MD5:	2477754B2A231EE4873AD5F9A00AB416
SHA1:	B7B4660151F2363B7894611EBA081D9AA556E82B
SHA-256:	FAC2F28F109B221D0AA6ADB618CF1E32555220AAA4E30F063B90D1AE193261DC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
SHA-512:	DC56A96983695018306D02AA34278B20C362C487934D6A82529881EBF3FA8BE34CE74120BC74F30EE2838599E97D1E508903A6F065C98435B161892E1196D770
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6288607939044842
Encrypted:	false
SSDEEP:	48:JMqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUg4:JMhIElwQF8mpcSL
MD5:	DF824086C6D6382119CC1380FDDDC646
SHA1:	0F40D1746AC39985E8C99C0E37923C573A67E643
SHA-256:	B5B121964ED75546C262E84EFED58C41334EE60B8C9389A8AF2808D593101315
SHA-512:	9F11B12067ED1944C80C5A7F2E9447B2D812737F58CF5CF92632853CD1ECF1AC62EEEACC1B3D1A7373E310B04D33C60D71E1EB26BA5C55A0BB59BA02FBBC3I 7F
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946 B
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.1894775491312455
Encrypted:	false
SSDEEP:	6:mwAruVq2PWXp+N23iKKdKrQMxIFUtpDArM0gZmwPDArTwIkwOWXp+N23iKKdKrQq:5va5KkCFUtpb/POz5f5KktJ
MD5:	B5EB53FC06B92993287DCEE1CCEEE8E8
SHA1:	7295B383977692ACC869A20A9EDBF0F39B2EEC6D
SHA-256:	DBEB61B2CA607BACEFC5ADB699B23880EFC1D9F23ACBC477FD7687F2C416F4FB
SHA-512:	7131033CC5FEB75485A6F00B1A2B6AD54B753900B032F69AEEE1AAE8BA963056E0D72842370DEA80110F3587A7E05AF65C54787D6AC74914C19790E0C6F962B5
Malicious:	false
Preview:	2021/06/11-16:40:48.725 604 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/06/11-16 :40:48.726 604 Recovering log #3.2021/06/11-16:40:48.727 604 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Stora ge/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Entropy (8bit):	5.19834684427775
Encrypted:	false
SSDEEP:	6:mwArWAq2PWXp+N23iKKdK7Uh2ghZIFUtpDArp6ZmwPDArpGkwOWXp+N23iKKdK7w:1Ava5KkIhHh2FUtp5/PT5f5KkIhHLJ
MD5:	633B7F5907F5D887F81BFE5DEC210C2C
SHA1:	F7D490B3E1E7E1F8C25F55A936E9F1D607BD6279
SHA-256:	F214D29ABFB2A32D6F08690F3920EAF84D27D5D5B80FD3527D14D9B560EA9708
SHA-512:	882E73DC25E2300C69A7064E5D42EABC9969DD0E105754F841472DD080188AFBA1C2648F21B93EFD39546737428D746A5D199D820D37A9D6419A7C7ACF976C8
Malicious:	false
Preview:	2021/06/11-16:40:48.499 1790 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/06/11-16:40:48.501 1790 Recovering log #3.2021/06/11-16:40:48.501 1790 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site C haracteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
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):	5.285671355792563
Encrypted:	false
SSDEEP:	6:mwAr/T2Vq2PWXp+N23iKKdKusNpV/2jMGIFUtpDArpgZmwPDArpIkwOWXp+N23i3:hva5KkFFUtpd/Pv5f5KkOJ
MD5:	F1E40A66AF8F1FFA5DEEB9CB454443B2
SHA1:	6943AA86FFDC59C2A1F6FDB3DC75789C453E532B
SHA-256:	6B0CA1DE24BB6B2E5244A8EEFE380F9CD2848885B65AC076E6944E6452C6DA3F
SHA-512:	2E633503A3D2805C4A87BD486E77636B4B2A5C36748A4EB81109E8314DD9367348854F0F797774B084EE72A4D15AEC3EB9DBA7610A13AE905A43259D2E9130D5
Malicious:	false
Preview:	2021/06/11-16:40:48.754 604 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Local Storage\leveldb/MANIFEST-000001.2021/06/11-16:40:48.755 604 Recovering log #3.2021/06/11-16:40:48.755 604 Reusing old log C:\Users\user\AppD ata\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.31241408649465
Encrypted:	false
SSDEEP:	6:mwArU59+q2PWXp+N23iKKdKusNpqz4rRIFUtpDArtWZmwPDArl39VkwOWXp+N23n:99+va5KkmiuFUtpsW/PUV5f5Kkm2J
MD5:	62C5E6448ACD7CEA82A06873CDB6D67C
SHA1:	798C7C201079E0EC535E80E90B1506DEB6369F35
SHA-256:	DFDB152D1252F6253DD3E5E8DF32C673D1DF855AD533CAD74B8D0FE1AF2F8D70
SHA-512:	0B72F41C3ED7F64DD36EC6CCB262DBCBF5B22BDD63A84BCA5883218FCB38A89FD5CE39CE134EE8361BA46A53D95BA5313F54D259EE5F0B81ABA87D10475F1 B7A
Malicious:	false
Preview:	2021/06/11-16:40:48.795 d5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Platform Notifications/MANIFEST-000001.2021/06/11-16:40:48.801 d5c Recovering log #3.2021/06/11-16:40:48.802 d5c Reusing old log C:\Users\user\AppData\Local \Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.2350124197388865
Encrypted:	false
SSDEEP:	6:mwA3sKVq2PWXp+N23iKKdKusNpZQMxIFUtpDA3CgZmwPDA3SvSIkwOWXp+N23iKX:Ezva5KkMFUtpUn/PUSvF5f5KkTJ
MD5:	BC901FDFAB583AD8086F80CE6F6F00C6
SHA1:	2869EFD6F014C37E3613224C7E96C6C8F1FD3A6C
SHA-256:	96D6DCBB4E74EA57D3BE9509895DF3A6DE2A2FAAD452BE90F4335C989DEE3DEA
SHA-512:	1CB3704A44934D3A4BF95B59A81A73D521A2F7CAD26304AB4A9E4D1E59A37EFB3783CC2A9B7D8C20474F2DE31ABCFDA787A87E79E358322AF1A9751C42DDE7CE
Malicious:	false
Preview:	2021/06/11-16:41:05.054 604 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/06/11-16:41:05.055 604 Recovering log #3.2021/06/11-16:41:05.056 604 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\d79c022c-e7ad-4437-af33-04ab38c26a65.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Preview:	.'..(.....'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.161211471344112
Encrypted:	false
SSDEEP:	12:1va5KkkGHArBFUtpfZ/Pih5f5KkkGHAryJ:Za5KkkGgPgqzf5KkkGga
MD5:	A385255467D7D7A844AC9B5118CA65A8
SHA1:	0933167F73C5A5FE70180629CF9B5384192C39C9
SHA-256:	B334193DBB1E6EBE65E932A3AD0744024A8BB176A5D0C1B5F21E38A979075846
SHA-512:	F5FCA3052CBC010C278AC824D3FCF32082DF0DC877B01CC9DF76F8E57037318D1BB34E5386DEECAD6E06CA3195CDE2DC9882D8DC3B7376798E384466325D9 0
Malicious:	false
Preview:	2021/06/11-16:41:01.514 604 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Local Storage\leveldb/MANIFEST-000001.2021/06/11-16:41:01.515 604 Recovering log #3.2021/06/11-16:41:01.516 604 Reusing old log C:\Users\user\AppD ata\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):	5.208001273070682
Encrypted:	false
SSDEEP:	12:wN+va5KkkGHArqiuFUtpu/PXIV5f5KkkGHArq2J:w6a5KkkGgCgKKf5KkkGg7
MD5:	1D3D950F1F668295A3AA458DDA8B334A
SHA1:	B4B79F1ED1106578BFF3D258044A91534411C527
SHA-256:	7DC50B12690976349F5563A87DD4594FCA8D894B40982329E1C87D7835F4E509
SHA-512:	E2C9A6B01C06667768E4FA5C6F16637CD3BC96F6391E825D654E7BDD3EC03C06FCE10FBDE6B754EAD8670F8E6AA1F39CD81981F679F804393885DA75FB007BI 2
Malicious:	false
Preview:	2021/06/11-16:41:01.497 180c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/06/11-16:41:01.499 180c Recovering log #3.2021/06/11-16:41:01.501 180c Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Preview:	..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.173038808445225
Encrypted:	false
SSDEEP:	6:mwAh9+q2PWXp+N23iKKdKkGckArZQMxIFUtpDAfJZmwPDA99VkwOWXp+N23iKKdX:Tva5KkkGHArAFUtpg/P+5f5KkkGHArfJ
MD5:	CBB7C1666E34E623E726657F9825F7EB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
SHA1:	92456EF972D7C0C1AD3123E0576AF383DCF69FC5
SHA-256:	A6597BB915EB4490D908AAF08B8D8D2A63CD9B84B2A38BC9AFE4F66D15899FD2
SHA-512:	B6EFF63B380D00C1D1DF5F94DBDD73D53DB05471CF906D9761A26031DC3AAE9AC17F217A96E7691BF0D9DB65197D3620869FEE589010944A93E4E20E25054FA
Malicious:	false
Preview:	2021/06/11-16:41:16.807 1808 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/06/11-16:41:16.809 1808 Recovering log #3.2021/06/11-16:41:16.810 1808 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\ce3da4e2-971e-4f02-b85e-77a99a8de432.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"},{"adve rtised_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\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):	5.297428471186759
Encrypted:	false
SSDEEP:	6:mwAreAq2PWXp+N23iKKdKpIFUtpDArPvZZmwPDArPvzkwOWXp+N23iKKdKa/WLJ:ZAva5KkmFUtp4vZ/P4vz5f5KkaUJ
MD5:	0A8AA2F027C8CF8DFDDA39D11C112269
SHA1:	7ABC4565A91F4C06F3A91E19CF04FB7E4591DE2B
SHA-256:	8292EC87861711D81933CB60E0C9AE86F1E6FB86E0BBB961DA7295D71964181B
SHA-512:	EB229AD085CFA995A21FF4A97C892941D2282B84ADB97F32E9AFDDEC7040597763414CD122B80AE77204603B4E77BC2799AE0DD45818E7291C5F56378A303BA
Malicious:	false
Preview:	2021/06/11-16:40:48.536 1790 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/06/11-16:40:48.537 1790 Recovering log #3.2021/06/11-16:40:48.537 1790 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Entropy (8bit):	5.314959102557906
Encrypted:	false
SSDEEP:	12:E2iva5KkkOrsFUtpU99/PUM5f5KkkOrzJ:Foa5Kk+gAf5Kkn
MD5:	DED63E60235885FBD0A388EDBAF0A847
SHA1:	A005263BE86BB57A6B8375AE2EBE6DBD03C48F80
SHA-256:	C7B1994FE7C59C27DCA2705E205D6ECFAA322C4EBA4CEAC62DD5E66DA099029B
SHA-512:	2EE787B16FC3DD26E376ACDFC10E4468E4CEDB2B2BAF85B9614E69D21D8377B04383B98F0A9830F918647C411FDD41AA340565C896FF73279DD0E3AFB9486C6A
Malicious:	false
Preview:	2021/06/11-16:41:05.094 604 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/06/11-16:41:05.095 604 Recovering log #3.2021/06/11-16:41:05.096 604 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:BXwpS:BXcS
MD5:	08589974BD3AF038AD2E3CEEC869BE17
SHA1:	3591646F421845E76D2D88AAE20BEBC87DA165C6
SHA-256:	7E013DBA193C7181A7C7712D789DE4992ACA14A233A34AC00BF746560F0D4176
SHA-512:	63FD2C4C7204D8D35F5AC3E35942F61BC1D8E4C0281E7573095868945DBA31C917B2AE9B7837F24B1F008B493B7AB1D813DD2BB4F2B0D6E6C933CF0A469EE19
Malicious:	false
Preview:	.....4..naLw

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\a13f43c4-3148-4c8f-951b-c4c84ac71fbe.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\a13f43c4-3148-4c8f-951b-c4c84ac71fbe.tmp	
Preview:	.... .H............ .... .p............. .h...n......... ....n...((.... .h.......00.... ..%..~H..@@.... .(B..&n..``.... .....N......... .(....D........ .w`...M..(............ ....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.......X...E.....I...k}....{.m.t.CP..........E...\..............=H..,A..,J..;P...nn p}nnp}........~~~........!...!---2---2... ....(............ ....!...7.#.:3,";3,!<.&'/...........NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.......P.. .Q.....1...x...tqpyxuux...0D..DP..........G...........uojuppnw....t|..9F..-=..+:..5:..rr......llkrkkmw................................ggitllkv................................hhgssss~............YY\eYY[e........ ....nnnzXXXa.............................RRR\..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b4283bca-3692-496c-8438-e439852f0d6e.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):	24055
Entropy (8bit):	5.534012198775042
Encrypted:	false
SSDEEP:	384:6j1vu+tQsLlfYgaXGZ1kXqKf/pUZNCgVLH2HfDuhrUuHGsHGDnT9S0x7k4Y:6JGhsLlfrIGZ1kXqKf/pUZNCgVLH2Hf6
MD5:	BE0A14C9728C84BD47459F26D149E88E
SHA1:	8C8EA00B0EDD666D69F4135817982AB74181FDCE
SHA-256:	2EC75DB39973D6C938AD434A6340C3C6CBD7223D63477B670804D536E427C243
SHA-512:	C336AFC089F0CFB0465A3651861E9FADE3AE51280DDAE9AED8B742AA91FB627D09DF291CB09F4E234F8D6AC42CAE7B68FBAE9BBFE1C001956DAACA32D310F 7FF
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":"13267928448515303","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\bd6d1c11-995c-4c67-b884-217709775028.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ca7617ce-1ada-4a8d-bba5-f09736f6826d.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):	5439
Entropy (8bit):	5.181671713058268
Encrypted:	false
SSDEEP:	96:nLOgCBoI2RzZxJUUcVcvok0JCKL8VbOTQVuwn:nLOgCD2Rz7JUUcd4K6
MD5:	2973AA0650F2B4D7F0EB68E5751EE0BC
SHA1:	D063696181D6EF590C35E2A2DA932A38681E5C0E
SHA-256:	26DEDE77F0222B13D46F3B5C9899E920CA3E13D0577E5E4332CCD1CB903C0F28
SHA-512:	41A5CD8C2FBE3AC5D1934EDDF610E0A3BF6FE24BE0EBA9AC5FD7BD80EB09548BE001BFA02BF2520009B02BA8F7909F3F8D0092D4EE835B2F4F54981EC968B2 94
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267928448771950","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d107641d-8fec-45e2-81d5-417329a46156.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):	5.536368636520261
Encrypted:	false
SSDEEP:	384:6j1vu+tQsLlfYgaXGZ1kXqKf/pUZNCgVLH2HfDuhrU0HG9nT9S07k4J:6JGhsLlfrIGZ1kXqKf/pUZNCgVLH2HfN
MD5:	D51A887E454F3AD6D4455122E2532719
SHA1:	5663ADC09CC30BED6D979585C1205E23BFC2949B
SHA-256:	CA8084D30FEE0ED9813E46334146402586D1CDDB087F4B0F713BE9B87A080181
SHA-512:	7295AB0307415D456E478FFAE686DB89948F8D46C09890BAED0D18AF5CB1B453F88BDB499241ADB38329C14BE8F572F18DBC0D72E5BFC795A2407522C0CAA5E 8
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13267928448515303","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	136
Entropy (8bit):	4.543179247982291
Encrypted:	false
SSDEEP:	3:tUKUUAx1ESdTyZmwv3GUA+gdh7V8sGUA+gdh7WGv:mwADEXZmwPDA+Qh7VvDA+Qh7tv
MD5:	8FAFF6D4B0FEBD86940BAAFDC5F90CBC
SHA1:	7827098A9815AA80509F2A7465CB3D4C7E62F496
SHA-256:	F93DA1012CBA22B8E37F9EDE74D40A059A12A9FA28B5D6D04B439624C122E550
SHA-512:	AA804684A62AD7EF1DEBF4E655F04B8CD3ACD277B8F414D904420DCBBFB538EADDE4A3611E09CE4F8D4A90ED949B78671314C8705A7AC8050FEEDA556E909 5F
Malicious:	false
Preview:	2021/06/11-16:41:00.783 a54 Recovering log #3.2021/06/11-16:41:00.856 a54 Delete type=0 #3.2021/06/11-16:41:00.856 a54 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Preview:	V........leveldb.BytewiseComparator...#...........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e02a83ba-3a7c-4ec0-be0e-deea6ba48947.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):	4.9574821709401125
Encrypted:	false
SSDEEP:	48:YcLOuUklSLklwHjacBqA8bqTlYqlQuoTw0eVH3CH3G/s8C1Nfct/9BhUJo3Khme2:nLOgCBoX2pcVcvok0JCKL8VbOTQVuwn
MD5:	17819C0D9CA33B5534F4918DD1B0679A
SHA1:	898F122DE8698F2861AC35B07B6CEA4B5382566B
SHA-256:	940A81EB76E27040569B052A892BBA4C03A0AB77C84C9C1CC97D51EE6642CA54
SHA-512:	3230DB79F6349DA1297B6E17AB971372E85C75875D029902AD56B6E4CCBD5DA55F1F7A26CA935C46D8A17767E18CAA7B7C684C83ED112F2EE8BB1E7B2257B6C
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267928448771950","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","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\ea328c80-2277-4292-92e3-1b2aab310b9c.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):	2936
Entropy (8bit):	4.891981423661566
Encrypted:	false
SSDEEP:	48:Y2TntwXGDHzM5epsvD38zsvVRLs16q6i6N7shTsdVd4YgQscyvhpsAt3zstMH9DM:JTnOXGDHzM5VLNVGx6i6NYNY1+RkG9kV
MD5:	E62A514AD4863CD977E6562D2E675131
SHA1:	418651C3E810E7D14A7A7C0C0450D605E5AF6C1C
SHA-256:	C8819BB740800D137CAFE98F9E196A2A72EC611386452AA73A1F3E2A549333F5
SHA-512:	85856136D5456D9EAA5F1B31504FFD74FEC0D8395B21EB800FDC9B2CA9D1DF8E73FFC0AFB6B7071907F74B8597DFF584F8827F88A00A6807EBAFADCAC1B09B3
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://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://maxcdn.bootstrapcdn.com","supports_spdy":true},{"isolation":[],"server":"https://kit.fontawesome.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270520452074268","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ajax.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270520452074693","port":443,"

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):	5.200038334798678
Encrypted:	false
SSDEEP:	6:mwAHI9+q2PWXp+N23iKKdKfrzAdIFUtpDABIJZmwPDAge9VkwOWXp+N23iKKdKfa:mva5Kk9FUtp6a/P65f5Kk2J
MD5:	3C6329F729CD3DD4E572EDC977E6DBAB
SHA1:	1F58F73BE3F071A650476AEF56F9C963D296B178
SHA-256:	29C87DDDBD0E924FE763C50384642E6AA49EF7FA5EE057846553399FCD6846DB
SHA-512:	5C1EF1841CC39F595465CDD1FEDDE028D805252C235A515ADE8B2536E714CEFB4663101528EB4EB67F85AD5271F232D54DB7A08FAF493B9C1F0EC6E28F68347
Malicious:	false
Preview:	2021/06/11-16:41:01.992 1808 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/06/11-16:41:01.994 1808 Recovering log #3.2021/06/11-16:41:01.995 1808 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\ShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8EflAka:8hk
MD5:	F2D831AF88E25FB3F2663A5CE9FB8CD7
SHA1:	D9A9B3D96C6E7B1B26B4D1BBE9809F055FBEB808
SHA-256:	387145612B66864EE61935CE793B6957ABE67787015CCF23E892392A3E866543
SHA-512:	A25D5621588A0578E6200EF17CED28F52D325706C181CB0B5DA8D623C928A188CA7041EA642BC71E2C49633E02046288D1EF5DE0C99AA55E123120BBADC8848
Malicious:	false
Preview:	.'..(.....4.S.#/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.27.0\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_dir4580_651516800\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir4580_651516800\Ruleset Data	
Category:	dropped
Size (bytes):	197616
Entropy (8bit):	4.955722655128328
Encrypted:	false
SSDEEP:	3072:98Lqy5tdVRpn0eYzR089VDeWLQva3jUmykfftq/3fHn13M+Ya9tKd57s7J4zpd:aLqy5jV70eYzVDYvU0Hnq9
MD5:	715067CF2947DFA3FDABA45D010912D3
SHA1:	71D4506F6DD1BD109F7DA1ECEF70D05BF95CB544
SHA-256:	0F58B5D6F89BFFE34A44803F70AEFD5A435ABD692FDD00D3B1C88575933BA752
SHA-512:	A9216F2839E9F86B4A83770E5E6D9706E788D9ED8EC831CBF51C5F73EC38E03FD96C513601B8A29848B3610D55320DCB44C97F03840657D5E2A50C9EF1CC8C4
Malicious:	false
Preview:	.....(.....Q.....p.....P.....,..... .....geips.....K..8.....lgoog.....(D..P.....ozama.....4...h.....onwod.....{..... ..g.bat.....p.....uotpo.....ennab.....q.....nozam.....@T.....<R.....h...L...0.....|.....t..p.....h...d...`...\...\...\...\...`...P...@...$.....<...8.. .4...0.....(..... .....`...D.....p...T.....(.....\|...x...t...p...l...h...d...`..\...X...T.....L...H...D...@.....8..... 0...,...l...$... .....@..... .....X.....4.....x...t...p.....h.....l...P...X...T...P...L...H...D...@...<...8... 4...0...,...(...$... ...

C:\Users\user\AppData\Local\Google\Chrome\User Data\faac3b83-3b05-4ff3-aed0-325ddd1a96fd.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):	172395
Entropy (8bit):	6.079974421189592
Encrypted:	false
SSDEEP:	3072:34eedLgVDqfsAtDzQFU36fdYPL8JPfFcbXafIB0u1GOJmA3iuR3:1egIRXv6fWPL8VtaqfIlUOoSiuR3
MD5:	E5803BF6CE45494C5B7B952770199C4B
SHA1:	8431C48F8DF72949136CA92853D6A1CE4037ADBD
SHA-256:	D3323C6988EA80D59D4B4B3032E6855C588CE829A50DDD2A90E54B9A0519E9D9
SHA-512:	0917FE388A58A0A1EDE50C352D53113D8B12355DFE8D10AF9916A7D35496F2E410C400C415CA7776D8B7E539B6E2B875653FE01366859F330C83A05F48208CF0
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":1.623454850981402e+12,"network":1.623422452e+12,"ticks":100003068.0,"uncertainty":3344572.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\faf53a19-34d9-4bdf-af13-7e7b93ff547b.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):	164023
Entropy (8bit):	6.050135741478899
Encrypted:	false
SSDEEP:	3072:7FdLgVDqfsAtDzQFU36fdYPL8JPfFcbXafIB0u1GOJmA3iuR3:DgIRXv6fWPL8VtaqfIlUOoSiuR3
MD5:	D94CEFE46EEBA5703D9B3285894D841E
SHA1:	8B20426B4F57635268942D4ACACD3D7F6E9E0437
SHA-256:	024CDE20FE9735A2667694333DB9F9E5079F28AD4B30AACABB88C932E9F014E2
SHA-512:	799C0F8AFA802A082758924A1A3A9DC6E434129F654D4C01BE642C854DFF98E266CE653CAA09F8FC95C7AD08DD3A0F2D0D444781F914617A16F6B12A0B612B0
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":1.623454850981402e+12,"network":1.623422452e+12,"ticks":100003068.0,"uncertainty":3344572.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016525165"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\115e7c88-fe90-4e34-b177-935cedee47cf.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

C:\Users\user\AppData\Local\Temp\115e7c88-fe90-4e34-b177-935cedee47cf.tmp	
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\4580_1673639817\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9301659996057974
Encrypted:	false
SSDEEP:	3:SXlpS0VHAgzlURX/PVdAwtL:Si0G5X
MD5:	FF0CBA325E01ED1EAE9021FBC02D3362
SHA1:	ADD06DA6B8FF5D8234EE155166C7498A5CFF8977
SHA-256:	CBD1231298B252479D8A63155A8FC0CFBC94AC5E8F74D93C683BC182CA3EA245
SHA-512:	7420B818C45FE804ABA451687DADCFD18A80FCF43F5D783D0BCEFC77191C716374B5F4F7989469FF0BEAC422DA75FC534E71ECD8BFC38EF51ABAD42913C3A956
Malicious:	false
Preview:	1.2731bdeddb1470bf2f7ae9c585e7315be52a8ce98b8af698ece8e500426e378a

C:\Users\user\AppData\Local\Temp\4580_274915920\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):	3.8417538334903507
Encrypted:	false
SSDEEP:	3:SRkGDEzGKb2dGMAz5Bi6QPEA1:SSUVKb2EMcXA
MD5:	C5EB6E81FF20793640FF1368767FE2E4
SHA1:	3838AB9769B8EA3F6F3241504099F6FB2591173C
SHA-256:	DB81C2532D8152C4606833C06B818B1C94FBDB0FBF98F0E89365AD4E7A093529
SHA-512:	3AE2FF526D5908E1B3F4AA5FDBBDF0D0859520CAFFCBF84BFA7D6DC31293CD08243B418533A526015BCF3F1A85E08CEBAB55ADE500D66F962EC8A19D3DA84CD2
Malicious:	false
Preview:	1.4302cf764844fc6ca4cd4de8cf5e13481c4dd15b4bd8d667869f9ae2fb54f9bd

C:\Users\user\AppData\Local\Temp\4580_651786049\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\4580_739045706\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66

C:\Users\user\AppData\Local\Temp\4580_739045706\manifest.fingerprint	
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\4580_953868866\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):	3.8671677123292323
Encrypted:	false
SSDEEP:	3:SXHpNLSdcw9MdlD6XcAQTO3mFaW:SXpNLSdnvL3m4W
MD5:	D28B357653A7A5278C82A36E0C405E1D
SHA1:	B8C9453B9934BB97E2A89F050C4E389E4C6D0783
SHA-256:	F2BC3E955B1BB6CCFB8B4C7828D473AB924A3BF9EAC0D51BE6E58C064E520510
SHA-512:	511230C2719EAA29A72E1FF6B066BBDFAED95F3B068E1F08F42076494F54451D3D5C42E65075506992DF1CC0A2E4A9D8F483E870FD0AAB021703B54BCF7D9A8
Malicious:	false
Preview:	1.2bb1e086bca8509078a93cc30229a67f9321a2fa629fdef56f7b224024920633

C:\Users\user\AppData\Local\Temp\63c89905-cc3f-4774-8c6d-ebe35effb119.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\6c521aa1-2fb7-4a74-b84a-77587dea4909.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\7f940001-fcca-4373-a97a-ba7e3fa4b1df.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp\7f940001-fcca-4373-a97a-ba7e3fa4b1df.tmp	
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\88713afa-e061-4528-b150-c920cee9695d.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\d76fa7a6-5afb-4839-8351-c25f05f86e08.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\scoped_dir4580_1219290996\88713afa-e061-4528-b150-c920cee9695d.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

C:\Users\user\AppData\Local\Temp\scoped_dir4580_1219290996\88713afa-e061-4528-b150-c920cee9695d.tmp	
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\scoped_dir4580_1219290996\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4580_1219290996\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4580_1219290996\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4580_1219290996\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\scoped_dir4580_1219290996\CRX_INSTALL_locales\da\messages.json	
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.231469484874774
TrID:	
File name:	VM64DGCRMN5XGK.htm
File size:	158969
MD5:	be59593c1b8874e2d1f30d8ec0368bfa
SHA1:	bac3b5ed310ca13bbcb50e783ed8d4d4683c67a6
SHA256:	808b36fb0d39cb3ac132d430081a696171a44ea976eaef8 894f522c517a86755
SHA512:	dc1c5ff6f7de12642aeece21f3afeff4bd12b2b2fe76a8e00 74dc104d2aaa40c1aba418d331c87e761c6e5d005804cc d625558b66004fb82a06140677b8cbf71
SSDEEP:	768:1DvKLhCwTx+jDieULMdLPWAEsY2J+47JFDy2k0 6wztTS+TeMF+WFvj4+EBLRoupA:N/eoDAoxR44FsGg 4DgqMVGg4DgqM6
File Content Preview:	<script language="javascript">document.write(unescap e('%3C%21%64%6F%63%74%79%70%65%20%68%7 4%6D%6C%3E%0D%0A%3C%68%74%6D%6C%20% 64%69%72%3D%22%6C%74%72%22%20%63%6C% 61%73%73%3D%22%22%20%6C%61%6E%67%3D% 22%65%6E%22%3E%0D%0A%3C%68%65%61%64% 3E%3C%6D%65%74%61%20%6

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 16:40:51.734714031 CEST	192.168.2.3	8.8.8.8	0x3813	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jun 11, 2021 16:40:51.777137995 CEST	192.168.2.3	8.8.8.8	0xdf18	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jun 11, 2021 16:40:51.779622078 CEST	192.168.2.3	8.8.8.8	0x9249	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jun 11, 2021 16:40:51.782387972 CEST	192.168.2.3	8.8.8.8	0xe666	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jun 11, 2021 16:40:51.793224096 CEST	192.168.2.3	8.8.8.8	0x971b	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:40:54.013680935 CEST	192.168.2.3	8.8.8.8	0x34e0	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jun 11, 2021 16:41:01.587172031 CEST	192.168.2.3	8.8.8.8	0xbac6	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

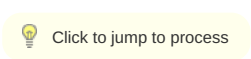
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 16:40:51.794806957 CEST	8.8.8.8	192.168.2.3	0x3813	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jun 11, 2021 16:40:51.794806957 CEST	8.8.8.8	192.168.2.3	0x3813	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 11, 2021 16:40:51.832442999 CEST	8.8.8.8	192.168.2.3	0x9249	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:40:51.832585096 CEST	8.8.8.8	192.168.2.3	0xe666	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:40:51.835624933 CEST	8.8.8.8	192.168.2.3	0xdf18	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jun 11, 2021 16:40:51.835624933 CEST	8.8.8.8	192.168.2.3	0xdf18	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jun 11, 2021 16:40:51.856621981 CEST	8.8.8.8	192.168.2.3	0x971b	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:40:54.076786995 CEST	8.8.8.8	192.168.2.3	0x34e0	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:41:01.654412031 CEST	8.8.8.8	192.168.2.3	0xbac6	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:41:01.654412031 CEST	8.8.8.8	192.168.2.3	0xbac6	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4580 Parent PID: 2996

General

Start time:	16:40:47
Start date:	11/06/2021
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\VM64DGCRMN5XGK.htm'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 3152 Parent PID: 4580

General

Start time:	16:40:49
Start date:	11/06/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,10561022475399133662,8554087899327668488,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1704 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly