ID: 452435
Sample Name: #U00e2_#U00e2_Play _to _Listen.htm
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 10:55:51
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

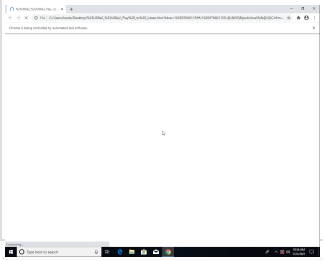
Windows Analysis Report #U00e2_#U00e2_Play _to _Li…

Overview

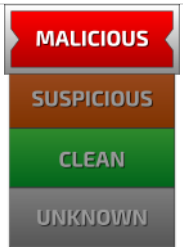
General Information

Sample Name:	#U00e2_#U00e2_Play _to _Listen.htm
Analysis ID:	452435
MD5:	59bcd893624173..
SHA1:	995c8ee3b08106..
SHA256:	51cb67fbe8cc070..
Infos:	

Most interesting Screenshot:



Detection



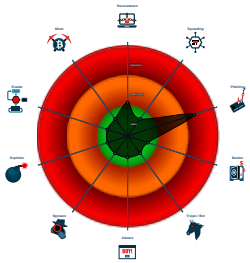
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish44
- Phishing site detected (based on im…
- HTML body contains low number of …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Submit button contains javascript call

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4088 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\#U00e2_#U00e2_Play _to _Listen.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5700 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1640,14482809985186982011,5593868377781062687,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
#U00e2_#U00e2_Play _to _Listen.htm	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

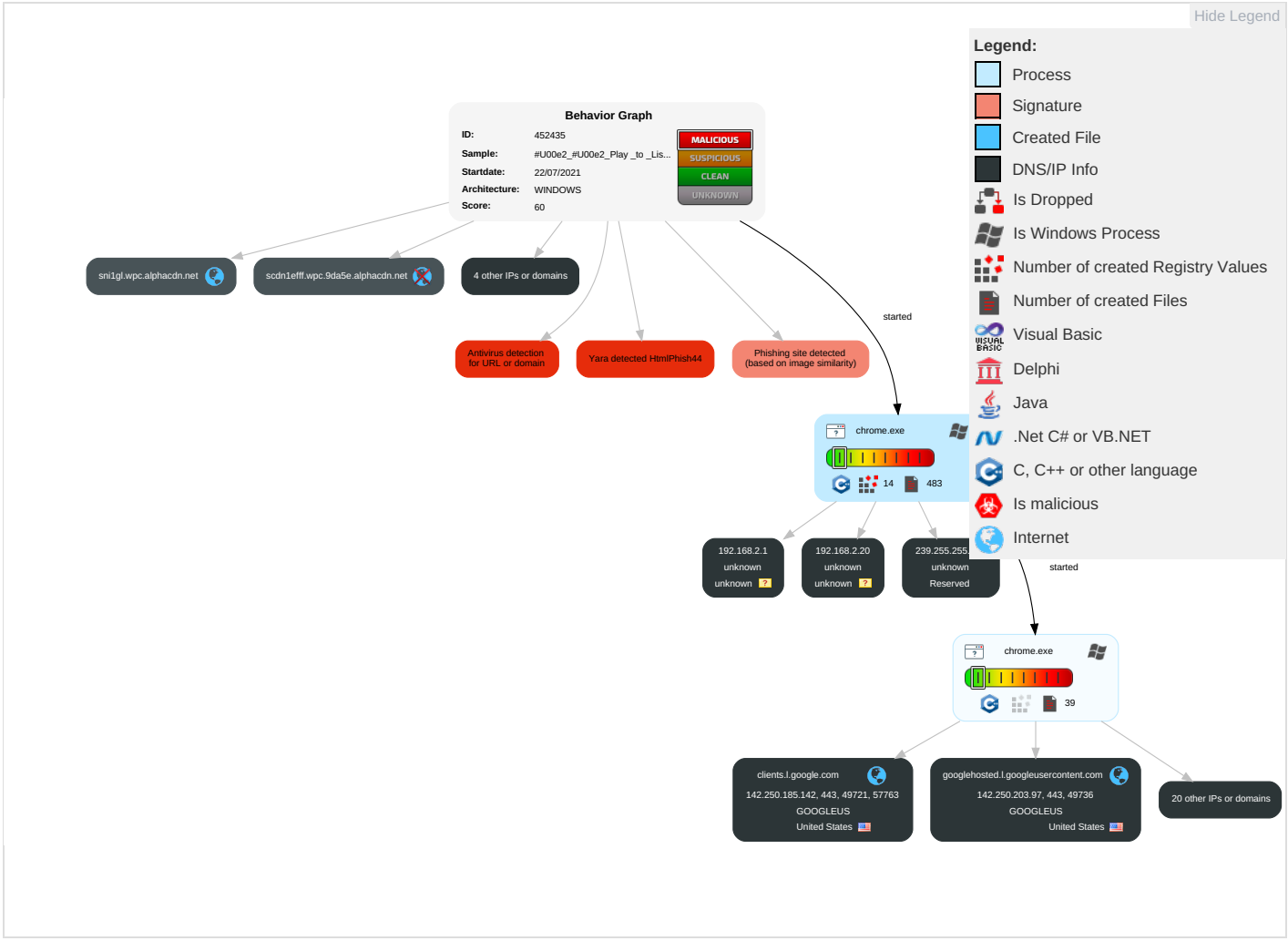
Yara detected HtmlPhish44

Phishing site detected (based on image similarity)

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	Scripting 1	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 Partition
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)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

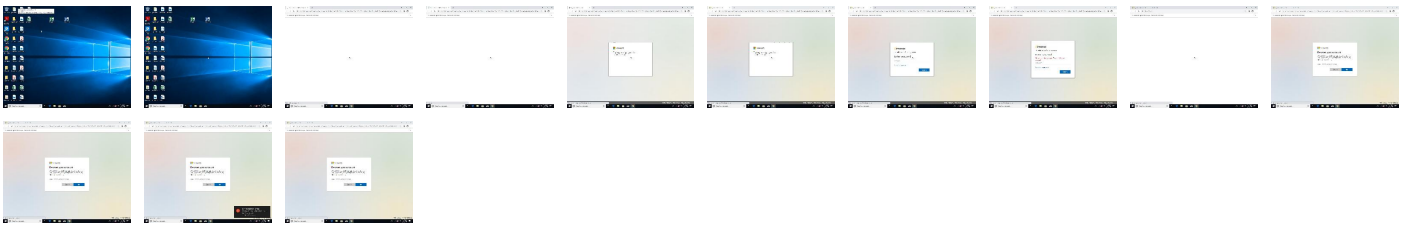
Behavior Graph

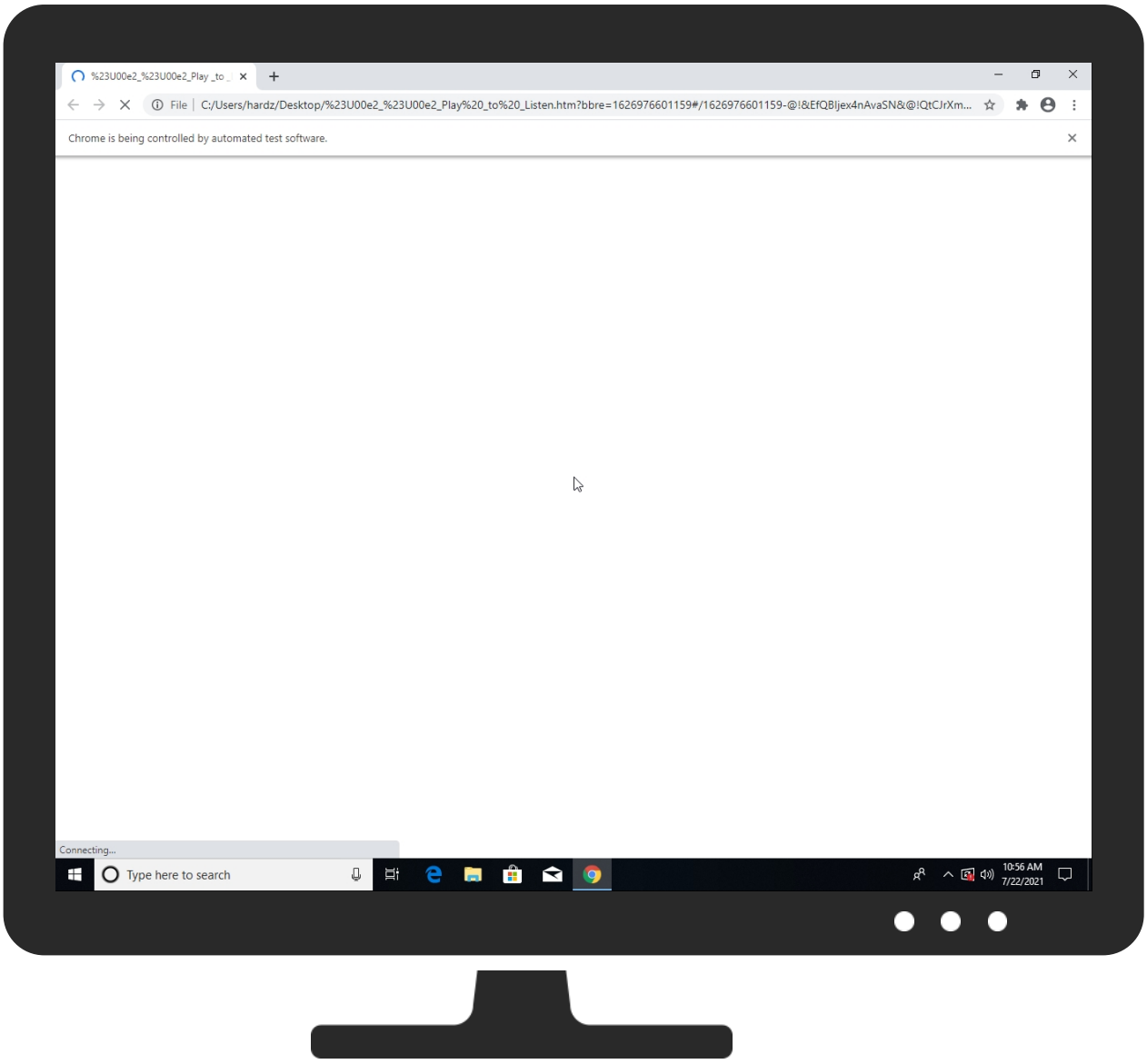


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
#U00e2_#U00e2_Play _to _Listen.htm	7%	ReversingLabs	Win32.Phishing.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://titko.wancdnapp.page	100%	Avira URL Cloud	phishing	
http://https://noem.urll.pw	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	URL Reputation	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico4	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/resetpasswordpackage_X7k_NcCIooflIFuKCGNtCw2.js?v=1	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/knockout_old_GJ62c6D9R5HuKFdkoO8XYw2.js?v=1	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/accountcorepackage_YD-Y5A3nlj0ms1Ks9fXU6A2.js?v=1	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1	0%	URL Reputation	safe	
http://https://manaapdpemtri.firebaseapp.com	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/	0%	URL Reputation	safe	
http://https://aadcdn.msauthimages.net	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/wlivepackagefull_2169QIWB52Tqqm3jo5_AUA2.js?v=1	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
titko.wancdnapp.page	104.21.47.62	true	false		unknown
accounts.google.com	172.217.168.45	true	false		high
manaapdpemtri.firebaseapp.com	151.101.1.195	true	false		unknown
noem.urll.pw	104.21.72.95	true	false		unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
bit.ly	67.199.248.10	true	false		high
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false		unknown
clients.l.google.com	142.250.185.142	true	false		high
unpkg.com	104.16.122.175	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		unknown
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
aadcdn.msauth.net	unknown	unknown	false		unknown
account.live.com	unknown	unknown	false		high
acctcdn.msauth.net	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
aadcdn.msauthimages.net	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
acctcdn.msftauth.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/%23U00e2_%23U00e2_Play%20_to%20_Listen.htm?bbre=1626976601159#/1626976601159-@!&EfQBIjex4nAvaSN&@!QtCJrXmE3YnhHsy5VU2ow!&@-erika.lontoc@enbridge.com-1626976601159/1626976601159	true		low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.122.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false
151.101.1.195	manaapdpemtri.firebaseapp.com	United States		54113	FASTLYUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.185.142	clients.l.google.com	United States		15169	GOOGLEUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
67.199.248.10	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
104.21.47.62	titko.wancdnapp.page	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved	?	unknown	unknown	false
152.199.21.175	sni1gl.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
104.21.72.95	noem.urll.pw	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.20
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452435
Start date:	22.07.2021
Start time:	10:55:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#U00e2_#U00e2_Play _to _Listen.htm
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.winHTM@39/204@18/15
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm • Browse: https://bit.ly/39KyDE6
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:57:04	API Interceptor	2x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.122.175	1.htm	Get hash	malicious	Browse	
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm	Get hash	malicious	Browse	
	efax702702702.htm	Get hash	malicious	Browse	
	eFax_Sg803.htm	Get hash	malicious	Browse	
	metropolitanproperties.com.odt	Get hash	malicious	Browse	
	#Ud83d#Udce0-Twc-159.186.10.243.htm	Get hash	malicious	Browse	
	099-563942-59-5095-73208.htm	Get hash	malicious	Browse	
	VANGUARD PAYMENT ADVICE.htm	Get hash	malicious	Browse	
	PortionPac Chemical Corp..html	Get hash	malicious	Browse	
	http://https://ddghbbf.r.af.d.sendibt2.com/tr/cl/AZ_fzMJRsE3xIeU_QcnTrJNmrQopncatDd-eovbR7xYq9ypiIqtwKWyrTIIdxNfdZBUhEo89L97BvoqW-m0AK8lpY_G1A0R4-OqWFWF7yqRk6lwWGjYQTbxdkNXIPZafVx__3xwAI7RkCXI8CJrNWoLoVVIyiYf1YWtibYMuXAbvq5KxrlLw-G3RcpVIiID2f-TlZx3vckcUFNx1IBpr5JamUxI3ckvzVYmWJV1yS8ZgSAUq_5FOmOxjsnNrYCXLNFt9Ew	Get hash	malicious	Browse	
	http://https://target-care.webflow.io/	Get hash	malicious	Browse	
	http://https://skrolprom.dorik.io/sp_audvc	Get hash	malicious	Browse	
	http://https://skrolprom.dorik.io/sp_audvc	Get hash	malicious	Browse	
	http://800response.com/wp-includes/.../Office/office/voicemail/o5tqh73xyuymo9ivztp5fjp7.php?7iiei0160701082 38d5f18d5c98d37da65eccffe3dfe3e048d5f18d5c98d37da65eccffe3dfe3e048d5f18d5c98d37da65eccffe3dfe3e048d5f18d5c98d37da65eccffe3dfe3e048d5f18d5c98d37da65eccffe3dfe3e04&email=	Get hash	malicious	Browse	
	http://https://secure-file-transfer-link-on.webflow.io	Get hash	malicious	Browse	
	http://https://sanfetaappdevmaozi-noisy-cassowary-es.mybluemix.net/roietri/ipz.php?bbre=gfh565rtdf&d=DwMFAw	Get hash	malicious	Browse	
	http://https://www.canva.com/design/DAEOEcu9Gnc/C6LvqPRfMOYoF6OWlu9bVg/view?utm_content=DAEOEcu9Gnc&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	
	http://https://elharless.github.io/stamapdevmo/tak.html?bbre=oadfis48sd	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://Https://christinescom.github.io/cappdevs/ta.html?bbre=dsiw4risd	Get hash	malicious	Browse	
	903-78848-9145-32-951474.HTML	Get hash	malicious	Browse	
151.101.1.195	triage_dropped_file.exe	Get hash	malicious	Browse	• www.ndsplan.com/qjnt/?r6q=409VEscksmbemh4psNBSYZ81rwPnbusvlC1+acnRVCvPwVqGWkPGglJQMW6w6KHAVJPl&rTFDm=GBOxAlxXYbRxGd
	jH10jDMcBZ.exe	Get hash	malicious	Browse	• www.covidtracksb.com/goei/?hBZpUr88=xBMInsAuN+E1djdIl4AZwlkS2iJ2Ju/hNdjKdY9aIZe6wtX7I1CrmxbEw1ye6jglvUKA0g+SVw==&ofuxZl=yVJLPZsh
	46578-TR.exe	Get hash	malicious	Browse	• www.covidtracksb.com/goei/?jBZx=D8b4q&kfOdRJ=xBMInsAuN+E1djdIl4AZwlkS2iJ2Ju/hNdjKdY9aIZe6wtX7I1CrmxbEw2e35jcdm3/W
	remittanceslip_pdf.exe	Get hash	malicious	Browse	• www.devfestindia.com/cu6o/?uN6x=W+WuFBrln1qCfAXJ5xKULfOGff8dAb86Jvk64PlTVVMLGqhT4HhQij0c0Z21Ont+U/Id&Vtx0E=FDHHERlxjn8PMDI
	Project.pdf.exe	Get hash	malicious	Browse	• www.towatchapp.com/ocq1/?lhudJ=s9fWYY+GRE/zu2qn9kCI0m/+x20wNzaZElH9PrG8sfLhi2QQuUQu3XvRAAgtMskCm9iv&1bm=3fhdLbnpevPXqD
	quotation.exe	Get hash	malicious	Browse	• www.fsjdc.com/x2ee/?iBZLH8e=/LfDiPUOWZnyidNro0j70T8JUoHePLB2D+vct3YQB9mB3q5S0iE8mJFwRkJZflqbRhoGi7RzLw==&_RA89r=ZL3D3PvXurq
	DOCX RFQ#2.doc	Get hash	malicious	Browse	• dropb-cfeb2.web.app/white.exe
	DOCX RFQ#2.rtf	Get hash	malicious	Browse	• dropb-cfeb2.web.app/white.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	12-4.exe	Get hash	malicious	Browse	• www.cvscarepasscard.com/gwg/
	PAYMENT COPY.exe	Get hash	malicious	Browse	• www.firedoom.com/sbmh/?EjRh0d=C5hy1K5oAHBPrT8N397N//2qVHn6YwjigpXcmeWEXRbnBwwwMsoNEjPCOjfDrGfyrTiG&Bn=8pt0_Nex
	PO987556.exe	Get hash	malicious	Browse	• www.firedoom.com/sbmh/?Yn=ybIHmldXUn88Ur&jfIT64=C5hy1K5oAHBPrT8N397N//2qVHn6YwjigpXcmeWEXRbnBwwwMsoNEjPCOg/57X/Kx0DB
	account confirmation!.exe	Get hash	malicious	Browse	• www.firedoom.com/sbmh/?0Tx43p=zbDHwlRpXFN&DV8X=C5hy1K5oAHBPrT8N397N//2qVHn6YwjigpXcmeWEXRbnBwwwMsoNEjPCOjfDrGfyrTiG
	New Additional Agreement.exe	Get hash	malicious	Browse	• www.erraticer.com/bw82/?J2JxbNH=6vRuuEDvqC5+aa5DVmVINCXZAyoyPzPxPo5XFdu9xcvmHzBmwHK9JJE0E4eNhlSLE1w3&BXEpz=Z2Jd8XTPeT
	00d1gI2vB4.exe	Get hash	malicious	Browse	• www.erraticer.com/bw82/?ET8T=6vRuuEDvqC5+aa5DVmVINCXZAyoyPzPxPo5XFdu9xcvmHzBmwHK9JJE0E4eNhlSLE1w3&URiP=qFQxprRp5PPPOfyp
	New Additional Agreement.exe	Get hash	malicious	Browse	• www.erraticer.com/bw82/?8p=6vRuuEDvqC5+aa5DVmVINCXZAyoyPzPxPo5XFdu9xcvmHzBmwHK9JJE0E7ykiluzNWFh0m7Gjw==&Bh=H0GxrDp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Additional Agreement KYC.exe	Get hash	malicious	Browse	• www.erraticer.com/bw82/?Ezrtr2qh=6vRuuEDvqC5+aa5DVmVINCXZAyoyPzPxPo5XFdu9xcvmHzBmwHK9JJE0E7ykiluzNWFh0m7Gjw==&QL3=ojqPsv
	http://roundcubemailagentupdate.web.app	Get hash	malicious	Browse	• roundcubemailagentupdate.web.app/
	http://auto78438787328758792947.web.app	Get hash	malicious	Browse	• auto7843878732875879247.web.app/
	http://salary-bonus.web.app	Get hash	malicious	Browse	• salary-bonus.web.app/
	Client Contact REGISTRATION Sheet.xlsx	Get hash	malicious	Browse	• www.letsdindin.com/mnf3/?9rTpeFt0=G6fRyfWpf4em3a5PxYoprh6KPSSsHaeEr4x3W3Pvzp31VBrhmksxwaIlwF2fZ05EyJsOCg==&rj9L_=qpnTHjlx

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
manaapdpemtri.firebaseapp.com	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 151.101.65.195
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 151.101.65.195
	obfuscated-html.html	Get hash	malicious	Browse	• 151.101.65.195
titko.wancdnapp.page	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.21.47.62
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.21.47.62
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 172.67.145.59
	New Text Document.htm	Get hash	malicious	Browse	• 104.21.47.62
	1.htm	Get hash	malicious	Browse	• 104.21.47.62
	#Ud83d#Udcde_#U25b6Play_to_Listen.htm	Get hash	malicious	Browse	• 104.21.47.62
	Fax.htm	Get hash	malicious	Browse	• 172.67.145.59
	Fax.htm	Get hash	malicious	Browse	• 172.67.145.59
	#Ud83d#Udcde_Message_Received_05_19_21.htm	Get hash	malicious	Browse	• 104.21.47.62
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	• 172.67.145.59
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm	Get hash	malicious	Browse	• 104.21.47.62
	#Ud83d#Udcde_Message_Received_05_19_21.htm.htm	Get hash	malicious	Browse	• 172.67.145.59
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm.htm	Get hash	malicious	Browse	• 104.21.47.62
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen htm.htm	Get hash	malicious	Browse	• 172.67.145.59
noem.urll.pw	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.21.72.95
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.21.72.95
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 172.67.179.200
	New Text Document.htm	Get hash	malicious	Browse	• 104.21.72.95
	1.htm	Get hash	malicious	Browse	• 172.67.179.200
	#Ud83d#Udcde_#U25b6Play_to_Listen.htm	Get hash	malicious	Browse	• 172.67.179.200
	#Ud83d#Udcde_Message_Received_05_19_21.htm	Get hash	malicious	Browse	• 104.21.72.95
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	• 104.21.72.95
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm	Get hash	malicious	Browse	• 172.67.179.200
	#Ud83d#Udcde_Message_Received_05_19_21.htm.htm	Get hash	malicious	Browse	• 104.21.72.95
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm.htm	Get hash	malicious	Browse	• 104.21.72.95
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	• 172.67.179.200
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen htm.htm	Get hash	malicious	Browse	• 104.21.72.95
	#Ud83d#Udcde(801) 451.htm	Get hash	malicious	Browse	• 104.21.72.95

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	10303640_APMC-TRN-C0001-Stability_Calculation_Rev1.exe	Get hash	malicious	Browse	• 104.18.7.156

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	r3xwkKS58W.exe	Get hash	malicious	Browse	• 104.21.51.99
	Westernunionreceipt711 ___vaw.html	Get hash	malicious	Browse	• 104.21.40.98
	MPU702734-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	XuQRPW44hi	Get hash	malicious	Browse	• 104.21.58.112
	Remittance.html	Get hash	malicious	Browse	• 104.16.18.94
	jRPSjUSf.exe	Get hash	malicious	Browse	• 104.23.98.190
	989E2813477A4245E0357E0F8E49AFAE384AF828C95EE.exe	Get hash	malicious	Browse	• 104.21.71.170
	P58w6OezJY.exe	Get hash	malicious	Browse	• 104.25.234.53
	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 172.67.130.27
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 162.159.134.233
	rxfttQnoO5	Get hash	malicious	Browse	• 1.13.147.24
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.21.72.95
	Cotizaci#U00f3n.pdf.exe	Get hash	malicious	Browse	• 104.21.36.131
	aviso de pago.pdf.exe	Get hash	malicious	Browse	• 104.21.39.75
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 172.67.130.27
	kRGc0HgN5b.exe	Get hash	malicious	Browse	• 172.67.188.154
	0n4xyK1WyMB3UE2.exe	Get hash	malicious	Browse	• 172.67.217.147
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28334.exe	Get hash	malicious	Browse	• 172.67.188.154
	Yaharasoftware.com_Fax-Message.htm	Get hash	malicious	Browse	• 104.16.19.94
FASTLYUS	Convert HEX uit phishing mail.htm	Get hash	malicious	Browse	• 151.101.12.193
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 151.101.1.195
	boysLove.dll	Get hash	malicious	Browse	• 151.101.14.132
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 151.101.65.195
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 151.101.65.195
	converter_1626796202.dat.dll	Get hash	malicious	Browse	• 151.101.1.44
	SKM_C258201001130020005057R1RE.jar	Get hash	malicious	Browse	• 185.199.108.154
	recognizerCryptolocker.dll	Get hash	malicious	Browse	• 151.101.1.44
	recognizerCryptolocker.dll	Get hash	malicious	Browse	• 151.101.1.44
	INV #95000987.html	Get hash	malicious	Browse	• 151.101.112.193
	soa-032119.exe	Get hash	malicious	Browse	• 185.199.108.153
	PandaOCR.Pro.exe	Get hash	malicious	Browse	• 185.199.108.133
	PandaOCR.Pro.exe	Get hash	malicious	Browse	• 185.199.108.133
	Software updated v2.6.0.exe	Get hash	malicious	Browse	• 185.199.109.133
	product samples.exe	Get hash	malicious	Browse	• 151.101.1.211
	XFfw6uDKna.exe	Get hash	malicious	Browse	• 151.101.112.193
	cheat.exe	Get hash	malicious	Browse	• 185.199.110.133
	TIJYYlYJpv.exe	Get hash	malicious	Browse	• 185.199.108.133
	another.dll	Get hash	malicious	Browse	• 151.101.1.44
	borderCurr.dll	Get hash	malicious	Browse	• 151.101.1.44

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	41609787.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	B5xK9XEvzO.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	RsEvjl1iTt.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	ORD.ppt	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	39pfFwU3Ns.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	47a8af.exe.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	Comprobante1.vbs	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	ZlvFNj.dll	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	QT2kxM315B.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	Convert HEX uit phishing mail.htm	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	192-3216-Us.gt.com.html	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	N41101255652.vbs	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	FILE_2932NH_9923.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	RDlkHCLRxE.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	Swift_Fattura_0093320128_.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	SecuriteInfo.com.Variant.Graftor.981190.24096.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195
	IPVrDRKfYj.exe	Get hash	malicious	Browse	• 152.199.21.175 • 152.199.23.72 • 151.101.1.195

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

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
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\4D1ED785E3365DE6C966A82E99CCE8EA_216A6C169356295AB09C26D4D7D32E06	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.174485912944054
Encrypted:	false
SSDEEP:	12:JKtfTlUX5BWm+fPyEm7bBzyQdFLtb7An2fGLUZcW/d:JiTlkS/PyEm7bB+4LhUnpUZcW/d
MD5:	224CCB018990BE0A7CA6E61A162E5B1F
SHA1:	DA8622D6A2B548D4A5E14C7E7514572FACB3DD1C
SHA-256:	9A3324FC2832F57368071F152AE94CF5DDF38665E441486207D42E4A02BEA65A
SHA-512:	D50A24F4E815490D8FD25D4730033534B665CEE8078C7011405DF2AC0B5DB19C959DA3FFD4C27B6C38D0D3FD0C778D5E9E04A3FBC5F0391CDFC8D91F541505B
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....=.P.....J`.e.!.....20210721222438Z0s0q0I0...+.....I.....v....@-h;qj....=.P.....J`.e.!.....H.!.. .E....x.....20210721220901Z....20210728212401Z0...*.H.....S...M1./..K^.i[3....{..Y.....l@O.yl.j).nSH...,%...8S0_'.+..3..DG.>..Jz..,.....A.9...fk./r.....p...OSKe..).=u..%..t".....8w:.E....*...OC..U.*eq.U&..i."..,....d. .".+..+6Sz...W8U.....j{...^j'.m..5...N...'....N.....W.\....Cz.^..=.yj.c

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.250984744892131
Encrypted:	false
SSDEEP:	6:J0MlY0EU9c5o78tjTZnDV7hLiU9YBQ+tEnleWhUmurCC8tNQTVBxp2yoeglxv2X8:JY0ET5FZJ9efB+eEDur8cPjto/l5X0Dd
MD5:	B23D7664F3C44250873A2413A010D603
SHA1:	ED52BF36995FAA703CFBF09F4C1EF2CFC5964116
SHA-256:	B7D59B02BCF3C2187A1A228A7FE2C3F83581B2F37FD4AB32C81E2BAB0AEB6981
SHA-512:	4CC9D48BE8D691E70C5FAC3D50013755AC2281A6DC1E8FAF3DF3214D95CBFBADC0A75453D044819BC80A8983F6F44D81687B4271FA4147D1BDE8854F1AB28CC
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....>.i...G..&....cd+...20210721215359Z0s0q0I0...+.....(..A..B..G@B.X....>.i...G..&....cd+....y.D.... .a_.k.....20210721215359Z....20210728215359Z0...*.H.....!w...}.....r...-..I..B.....?.F...4.j #.v.. A....k...8"^;9gYr[...Q.^4*.F...9.z..'L..(X.....@.=.+.....<.8..z.p.,"...!.o..m0.....{..._#|..wB..~.'.9.....Dy..su'...=..i..!..hHZ.....3.....&$v|..w.N....(.....+....}.&.N|.....T.D.)...m.dA.S.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\4D1ED785E3365DE6C966A82E99CCE8EA_216A6C169356295AB09C26D4D7D32E06	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	852
Entropy (8bit):	3.8327702273680964
Encrypted:	false
SSDEEP:	12:MtvmxMiv8sFq3lCvM710z0MqRPtVjNG6//mxMiv8sFq3lCvM710z0MqRi:Evmxxvm4vw1VLVpGK/mxxvm4vw1VQ
MD5:	C7412DA3BCF9BBFED5A4E78CAFC6BE2F
SHA1:	7E58ADD75361F8F4A395EACC47C1F5F9F5D9CE33
SHA-256:	E67A7A384C95F6DC58BA1D9500D52C60DAA51C86BD5628AB7F4B20F97B12CD07
SHA-512:	4560E769365E4F5F518ACD37F1BA35384294C4DF4835EEF212744E5AD34950015966086AFAC47B016819B48B156B45EBD8126009B0B48A9E57EDB4E70D3BCAB9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\4D1ED785E3365DE6C966A82E99CCE8EA_216A6C169356295AB09C26D4D7D32E06	
Preview:	p..... ....."...(..... .....1.~...%.....h.t.t.p.:.//.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.R.J.9.L.2.K.G.L.9.2.B.p.j.F.3.k.A.t.a.D.t.x.a.u.T.m.h.g.Q.U.P.d.N.Q.p.d.a.g.r.e.7.z.S.m.A.K.Z.d.M.h.1.P.j.4.1.g.8.C.E.A.t.I.g.y.H.h.z.C.A.g.f.0.W.o.j.6.G.g.e.O.A.%.3.D...".6.0.f.8.9.e.a.6.-.1.d.7."...p..... ....."...(.....<..}~....%.....%..... .....1.~...%.....h.t.t.p.:.//.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.R.J.9.L.2.K.G.L.9.2.B.p.j.F.3.k.A.t.a.D.t.x.a.u.T.m.h.g.Q.U.P.d.N.Q.p.d.a.g.r.e.7.z.S.m.A.K.Z.d.M.h.1.P.j.4.1.g.8.C.E.A.t.I.g.y.H.h.z.C.A.g.f.0.W.o.j.6.G.g.e.O.A.%.3.D...".6.0.f.8.9.e.a.6.-.1.d.7."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_C31B2498754E340573F1336DE607D619	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.865725547821471
Encrypted:	false
SSDEEP:	24:iijPmxxvnFqYwJiwQQeSjPmxxvnFqYwJiN:iMPODkiwQLcPODkiN
MD5:	D699016833A03973324776232996FB5D
SHA1:	5E3A230C38B14CF4DEAA6DF626ABC832BBBB6ABF
SHA-256:	9CDBCBFF84E2B56F696ADD24B73865A2D724B35E4F9533F0398BD990399DEEC4
SHA-512:	E832B4D955410B168692C91F518DD13E17822BFBBCD46D87BA9FAC05C8A726769CD444B898A43382FDA3EB4325244F9B8E4E61D2950F55BF0910E098713CBB2
Malicious:	false
Reputation:	low
Preview:	p..... .....GD.."...(..... .....).~..R9.....h.t.t.p.:.//.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.x.5.q.U.S.w.j.B.G.V.I.J.J.h.X.%.2.B.J.r.H.Y.M.%.3.D...".6.0.f.8.b.9.7.2.-.1.d.7."...p..... .....GD.."...(.....z~...5.....5..... .....).~..R9.....h.t.t.p.:.//.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.x.5.q.U.S.w.j.B.G.V.I.J.J.h.X.%.2.B.J.r.H.Y.M.%.3.D...".6.0.f.8.b.9.7.2.-.1.d.7."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0649255a-64ea-44e4-a23d-277039c6dd4f.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):	166057
Entropy (8bit):	6.049835134495863
Encrypted:	false
SSDEEP:	3072:Gd5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:S5hnrszc0fZI/xKmaqfIlUOoSiuRY
MD5:	70772D0EEC1E8F338101353457D43DA6
SHA1:	D25D06080CDCC7CFCECF8D8A6EDEDE2186146C51
SHA-256:	C31D38AE6B870A04E36EF8773E18C92E2C11BC974E63F1C6DAFF0AE3C8134E39
SHA-512:	E79CB48E0984DFF56F97FADD1849557D2C8B257340A65F4053AC7F034925461F53AD0460C352201C36CBE4CF27B02F1FD2CE174A8C36F4A600DE6DA5C076FC3
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016772232"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\2a7c8b50-6f47-46fc-8fbb-834d58806ea5.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):	166411
Entropy (8bit):	6.050926611105115
Encrypted:	false
SSDEEP:	3072:SX5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:C5hnrszc0fZI/xKmaqfIlUOoSiuRY
MD5:	42AAFAB3BAD6675C98B3ECF207D120E7
SHA1:	956D08CCA0A36F9DDE3B5AEFE36EF4D86D97A493
SHA-256:	4D6FF17E2067BA3D4B4EF3337DB55A4158FBA95E5F4850A0C8C705B67618DABC
SHA-512:	4B1C64E4CB4216DCFF6847EFBD82DE082A29C5AC050D117E60B15817E77451535111E8D9151C2FAD739219F30299EE6731E3CBBD7032D5281FECFA21B53A5FC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\2a7c8b50-6f47-46fc-8fbb-834d58806ea5.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1

C:\Users\user\AppData\Local\Google\Chrome\User Data\30793f91-41d5-4674-a5ed-dca7d1179b45.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174421
Entropy (8bit):	6.079525395292999
Encrypted:	false
SSDEEP:	3072:QUN5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:jN5hnrszc0fZl/xKmaqfIlUOoSiuRY
MD5:	A6EF43613248CF9528B45AFC3102E493
SHA1:	56383C35F18C41941BD345B07FE3AB311AA7FF89
SHA-256:	6068232CC43260515D92AC9F4E8856492E5EC751D1B6EB52CA644E15F6D6A79A
SHA-512:	99816A3F361499252C46DDC390406A1E82D14B7E2D56EF5EB6024BFDE33EA937306E4B5756A94C72EFAE43FBF8BC99C079D1B3804AB0BB1DD6A7AD57D1723C7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016772232"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\37797b19-b212-4890-b1c2-220e2cbb8560.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	165963
Entropy (8bit):	6.049558173339509
Encrypted:	false
SSDEEP:	3072:md5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:y5hnrszc0fZl/xKmaqfIlUOoSiuRY
MD5:	5008D4ECA1D4C0FD04495D0EC526CF83
SHA1:	352C841D6E4BB57A6E63272B3E86D01EB932A669
SHA-256:	50EF5479457EF08593368F3D77528B1D843A48DE0515F19B32413EC2BD2472E6
SHA-512:	FDFD826BF4E1B7DCEE6D317FD5BFD8D965F1B06086DDDD9E32F3C4568DCC8D5967F580F00096C271992943F7C71B7CE71FA705DC8F5461E2FFE4C05AB7D885
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016772232"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\3b96f2ad-a05d-467d-a53f-1b0f4ebebe15.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.751534895369978
Encrypted:	false
SSDEEP:	384:1f78s+RnGVCEVJ7YPN0rVvQs3PcuXHirGb+rpugux/S2yJrFQmhtH9e80APO+Ss0:Za2BJ22grEe3qsGAvfCgKqkM12
MD5:	34B3F43C477FE4B5AD7A255B7F3BBE30
SHA1:	888FC685A931236CDC8AD3089AABF77FB2DFD929
SHA-256:	AF30ACB52D731385FBB19D79BD01B826DD244CD4D811121A0EA74C2EE5B548A3
SHA-512:	D7023AAB61310D6C173B3A18C3DABD832A2E429EAF35D2CCA6165EF731C80637A81D0BD808EEA95C40CA3FA6376D779CB52691DDD3EB7F4EB20F95AD0DAEF68C
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\3b96f2ad-a05d-467d-a53f-1b0f4ebebe15.tmp	
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...q@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\4c8ad0ce-e74b-4048-a96d-4cddba995082.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):	166581
Entropy (8bit):	6.051234120187718
Encrypted:	false
SSDEEP:	3072:hX5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:F5hnrszc0fZI/xKmaqfIlUOoSiuRY
MD5:	4EFA745C81F1AF49C8B837D7630F320C
SHA1:	F4CEEEABC76419364F5F7E3FC3DD5F6FE98CA2C1
SHA-256:	8A923ABEDDD5CA00D02B2C64867BDFA1E1E015C9C7F3985456C517DF886334F8
SHA-512:	3DCF3D3A9E77E23051AF2FDE4D65C5DF61014099AF0214281FE2533609656FFC6CD6AB3FF29FEFA54A5022E356AC7D9AC6A5EE4198C91DE93138F16254D11FD C
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAA AAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRh NbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyX OajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1

C:\Users\user\AppData\Local\Google\Chrome\User Data\58e5cdb6-b902-4a8c-9fd7-ed6d1f425689.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7515633204820427
Encrypted:	false
SSDEEP:	384:Ff78s+RnGVCEVJ7YPN0rVvQs3PcuXHirGb+rpugux/S2yJrFQmh29e80APO+SsN0:Ja2BJ22nrEe3qsGAvfCgKqkM1M
MD5:	82A0F012A1CD53A9112E3152E0993765
SHA1:	AC720E02E5A930040B7F26562465FF04A0A89E61
SHA-256:	B9709D2C29E3F5FEBEA5B2CD0D2B7C83C7939E739296CA080F6D5E6113D6A599
SHA-512:	802E10D4ADE080FE1EFAD831AE2882AAAED60E10E31BB38A84FC6040DAA3E180B87CF6B10B2EA2A0CA40719B08161B5F5BE5A964A6B149A23D1B4F0A020265 93
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...q@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\5d79c79c-fa16-4d69-b074-eac8f5654963.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.751036635418363
Encrypted:	false
SSDEEP:	384:bf78s+RnyC9YPN0rVvQs3PcuXHirGb+rpugux/S2yJrFQmh29e80APO+SsNx1s1a:92BJ22nrEe3qsGAvfCgKqkM1P
MD5:	1AB2F466F99B4255718FE2768DA41EF7
SHA1:	C49D6BBC967FFF098AD4BBB2AF7267DDD1D1924C
SHA-256:	96A824E36C0C7D462D7FB959F28D828FBD51B5AE348EDB4447EDE23E7AD4F54A
SHA-512:	F41EF41443C34EFF25EA5CE0C91C1C64763DAE16A3EC834770946FD604EA5299BA8431A1EBE2943C7A6B5CF77C6084328FADFCC4BCC46A2A3698ED4AE248F4 CB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\5d79c79c-fa16-4d69-b074-eac8f5654963.tmp	
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...q@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\5e0711ad-6166-433d-a38c-0d20301fad0f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174420
Entropy (8bit):	6.079527387355668
Encrypted:	false
SSDEEP:	3072:mhn5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:sn5hnrszc0fZI/xKmaqfIlUOoSiuRY
MD5:	CDDCA57BF864A233BAFDB583348C0E04
SHA1:	3BA0CFA4113A84F42C19F29C15186108E617635E
SHA-256:	51628A390D3197BC3E4C179D09764BB9827F0C0F56E08C05A463FC53532D0A52
SHA-512:	40964663B2485C3DD538966EBDFCA4389AE58B7B9B2116377016F85C1856110ACA7E5AD8ED2350A748F04DB373B850F2324DB59ECDF016B29A6E3306D7FC695
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":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\89745beb-24db-42db-b351-f8f3e5b69c9d.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):	166254
Entropy (8bit):	6.05040150787962
Encrypted:	false
SSDEEP:	3072:XX5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:H5hnrszc0fZI/xKmaqfIlUOoSiuRY
MD5:	24F99F03A3A5C8794A3986CD84486F8E
SHA1:	DFCBFF6761FF26B69F768B29FAAAD8E3C7B799EF
SHA-256:	379B91A2FF534ABD610C9A2AD2F3720B05F830560122703310011D4E041CD4A4
SHA-512:	9E794C19B5C661547607A093265CCB92B5196DFB3514AA1809076B44B9FAE6BAA7344E310737051AA0042C70AA3CFB378FFC680178A1C75577CB95D7A4B18063
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":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016772232"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\9f077f25-f689-4b4b-ab6e-616e71c28813.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):	166057
Entropy (8bit):	6.049835134495863
Encrypted:	false
SSDEEP:	3072:Gd5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:S5hnrszc0fZI/xKmaqfIlUOoSiuRY
MD5:	70772D0EEC1E8F338101353457D43DA6
SHA1:	D25D06080CDCC7CFCECF8D8A6EDEDE2186146C51
SHA-256:	C31D38AE6B870A04E36EF8773E18C92E2C11BC974E63F1C6DAFF0AE3C8134E39
SHA-512:	E79CB48E0984DFF56F97FADD1849557D2C8B257340A65F4053AC7F034925461F53AD0460C352201C36CBE4CF27B02F1FD2CE174A8C36F4A600DE6DA5C076FC3
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\9f077f25-f689-4b4b-ab6e-616e71c28813.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016772232"},"plugins":{"metadata":{"adobe-flash-player":{"dis

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:+ftIE1G1mkftIE1G1mkftIE1n
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\19607768-f0f6-4625-ac00-d9f28ff1904e.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):	5.576502832648103
Encrypted:	false
SSDEEP:	48:YvVwUu6UUhcUbUaseKUewqPeUer2UefQwUknwUGLxUenw:PUzUUWUbUa3KUGPeU9UE1UkwUGLxUD
MD5:	0BF999E6DC365B9AAFFB068585FD13B1
SHA1:	5BD9799248132CCEE55A5D87E4AEF36DFB92F83C
SHA-256:	8A41354F0117AC0180D882EAE02D8F4AD2026D884FFD122B97DECD391EC98159
SHA-512:	0D4D8511416DF4C568EF60150F3DDCC687F065A950D8AD8E4398E9C94EE5DA982B98EBD5D75AA9DA3584E4354E75B80D64B97835908EBAEA48655C3B9102622 B
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1642756605.463411,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626976605.463416},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658512605.360597,"host":"e3SziuwfuO2UvuBno+qkR1ObHAzZmSUoJhrc7dbP1Uo=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626976605.360603},{"expiry":1658512608.618354,"host":"lRJYtICs8D4kIE+fyDGXLUGmOLmkh+gKc50EU0l4m7I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626976608.618361},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3adc0dd0-6a64-4bb2-8f82-d57b462d75f8.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):	5453
Entropy (8bit):	5.1813677974411485
Encrypted:	false
SSDEEP:	96:nACcPJMvm5DWIF7ScKI8ok0JCKL8VbOTQVuwn:nACkMaDPScJ4K6
MD5:	F2EDE0BC599F0EF97DEFE449A487F615
SHA1:	1E23143D9AB1E3AA3DDEBD3BB66DEB030FFBCC8A
SHA-256:	F7B8E1E09E58D2957580C0CCEB2BD70808B6162263F38A1E3A822FBF92E77234
SHA-512:	8A36A9B3B915F55C5931D98BACD7D9A822202D3D11A3559D31EAB0705FF5611E95AE610285F1615145AEA6E5CA4CB867F3D30073A728389ABDC70F6A17752022
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271450200094422","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\4cb5de2d-46c0-4be5-9bfc-610e16465c18.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4cb5de2d-46c0-4be5-9bfc-610e16465c18.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5453
Entropy (8bit):	5.1813677974411485
Encrypted:	false
SSDEEP:	96:nACcPJMvm5DWIF7ScKI8ok0JCKL8VbOTQVuwn:nACkMaDPScJ4K6
MD5:	F2EDE0BC599F0EF97DEFE449A487F615
SHA1:	1E23143D9AB1E3AA3DDEBD3BB66DEB030FFBCC8A
SHA-256:	F7B8E1E09E58D2957580C0CCEB2BD70808B6162263F38A1E3A822FBF92E77234
SHA-512:	8A36A9B3B915F55C5931D98BACD7D9A822202D3D11A3559D31EAB0705FF5611E95AE610285F1615145AEA6E5CA4CB867F3D30073A728389ABDC70F6A17752022
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271450200094422","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\5ae6876a-337e-455f-be66-1f92e7a8c57c.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):	2869
Entropy (8bit):	4.862656773371538
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHzM15sVZTsWRLsyB+4sY8qO6Ms2yvowsz3q6igqRsYMHnYhbD:JTnOCXGDHzM1oXH+YrO6a+oLahgq7GYV
MD5:	E1654B5D88EE2270014742DC59DD493F
SHA1:	6BB4219A61578A118B605B278F52B84CD5F1FBE8
SHA-256:	9F8679DEC2EA1B7012E33A66B199F2BA4088C7EA22BCFCAC9CE2469651295727
SHA-512:	341FE07F13F14A0A30FFCD0572CB2E106786CA209E2E74ADEFEA63476123795EFA238318548F289671C90F45CDF10CE771117186166424218AD9485416655FEB
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://titko.wancdnapp.page","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274042203676076","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274042203676394","port":443,"proto

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6000b322-d641-44d5-afb2-9ddbad0e5d2c.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):	5492
Entropy (8bit):	5.186628389147887
Encrypted:	false
SSDEEP:	96:nACnbJMvm5DWIF7ScKI8ok0JCKL8WbOTQVuwn:nAC1MaDPScJ4KH
MD5:	E1ECFEB0694DE1083B59CF7EE81F67C3
SHA1:	C3A3F13EA10F4B4B068C40B6787571253ADD5455
SHA-256:	E93EAFD9724163286FF78E1CFF8278C269BEACF8C6E17DAAD5FF441E768171CF
SHA-512:	29827666281A9EF573B76CFC2755D0F7257D2D54EC5987270E0D639A0C05A88F3D966B61200B4D4F495AE7C539619E9B2576EEBFA439B7DFB3EEE7AD6F49EC5
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271450200094422","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\64097c87-b929-47bf-b31f-0f40acc05d47.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\64097c87-b929-47bf-b31f-0f40acc05d47.tmp	
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):	334
Entropy (8bit):	5.301994792421764
Encrypted:	false
SSDEEP:	6:mAxz+q2PWXp+N23iKKdK9RXXTZIFUtpBx75ZmwPBxSGVkwOWXp+N23iKKdK9RXXH:Kva5Kk7XT2FUtpr5/PV5f5Kk7XVJ
MD5:	B384754E793EADFE0EEA68F94DF6124A
SHA1:	115F5775AA10B39E483AC899F8DFDA03A84C19CD
SHA-256:	B7652B80C57261C36256E64C19538F044AAEDB6AF7447B673E71249091FF5E62
SHA-512:	082507925D6717C29B516BC970D9C779126006035745E8477F33B700B6EB2AEC33F355C86A80836C2C82FC0FA2BA3E8CCC0029CF120BAB4C3191416CC9619F07
Malicious:	false
Preview:	2021/07/22-10:56:45.562 1938 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/22-10:56:45.564 1938 Recovering log #3.2021/07/22-10:56:45.566 1938 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.299313893050313
Encrypted:	false
SSDEEP:	6:mAxN4+q2PWXp+N23iKKdKyDZIFUtpBx9ZZmwPBxD83VkwOWXp+N23iKKdKyJLJ:Lva5Kk02FUtpNZ/Pz8F5f5KkWJ
MD5:	B1F47511A24D69A4E9F93410BF43AB42
SHA1:	7756FD954538027E8655985F2678F02E1563C38C
SHA-256:	77D975B7B0EC5CEF2CC21F1D0621025C4B789D09EEC86F2F0D81F7C9E1869D7B
SHA-512:	7C0C7FA81344C042BE6C57509A62E2ADF626AE049C298C989D450FC6FFD4A2F3C93C73FA1F3C051D6B422ED77A60024570AFC55C64F834FEF26500E4A38DD8A
Malicious:	false
Preview:	2021/07/22-10:56:45.547 1938 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/22-10:56:45.548 1938 Recovering log #3.2021/07/22-10:56:45.549 1938 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0decd6ee54701714_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.658005958918444
Encrypted:	false
SSDEEP:	6:mJEYcRTXhr7fFNdCx1l/gdXBrKapzH4U5K6t:tHFNdCxyXRpjH
MD5:	D582B0FA69B2F4FE2EE1D54E75FBAE90
SHA1:	B3E6413D6B414AD17340ABE60A9C30DD3610954F
SHA-256:	3CF9E2B35B8DDA41CA0A498762AE3A75698AEFDF9FDD77DA7042686FB00DEEAC
SHA-512:	586D5A6AD3A5656BC9A48BF7BFC2BAA303414F4A936FEB0E3739BBB6DE964DCF12E11D383E41160EAC6D7D6DD8CCE03517282A527931358604A3003FB5F834C
Malicious:	false
Preview:	0\r..m.....a....._keyhttps://acctcdn.msauth.net/wlivepackagefull_2169QIWB52Tqqm3jo5_AUA2.js?v=1 .https://live.com//a.OP&/.....l...R.U.vh:e.M..a..h..-'....A..Eo.....P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\263002cf0fbb71e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\263002cf0fbb71e6_0	
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.65596161105792
Encrypted:	false
SSDEEP:	6:m3/VYcRT0uLjiyxNdul/gH7+4rpH7JthK6t:E/dNdu0rpH7
MD5:	359039B17C9B9B59694FE64DC7616DCF
SHA1:	1ED1721C35A2C470FE18C310607D303B6D9C6CA7
SHA-256:	F8ECE0E75214B7B03F139B8D45B2FB140B448CC73C595AEF460DF03F1A5CED50
SHA-512:	9B951528F840771ED8E1DF53984C26548F39C40E0AB790E57FC1400EFA750C951D8608EABF09FF3851D19FE66B92D0DEAD97DF4C79CC413F9DD0030AE0186E5
Malicious:	false
Preview:	0\r..m.....c...fj@...._keyhttps://acctcdn.msauth.net/accountcorepackage_YD-Y5A3nlj0ms1Ks9fXU6A2.js?v=1 .https://live.com/.L.OP&/....."........|@._i:...X,.mj..` ..N....p?.E.A..Eo.....C.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4278acc4333443e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.803931197839552
Encrypted:	false
SSDEEP:	6:miJYcRTSMiqIR5NdFvl/gaEdwK4GDK6t:DIR5NddUdwS1
MD5:	450C77AFF4501D3C4D38148C9A43C909
SHA1:	C5A2C79961206832066D24889288E7A6993D24F4
SHA-256:	1A1038E7DECDDEB9A9C42ABEEDE41F3CF6AB4467B880CDF11E789A7FE8F68716
SHA-512:	DB2B14A6B4A244C2C3F4F1F417BF4667BAC113D4D95763983D495CB4ACB19A4E75936B959F39927EFF48B511AFB665F66C96677CDCB0EB56CA41931DD959809
Malicious:	false
Preview:	0\r..m.....c...-9.Y...._keyhttps://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1 .https://live.com/...OP&/.....(....-...5.....K.y....x.\<.. A..Eo.....LI].....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\59f8bbf14d4853fd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.684749258518937
Encrypted:	false
SSDEEP:	6:mYoLnYcRT/REXA5Rhj5l1Z3Nd3i/gBkH6JRGhpK6t:FokAPhFl15NdMr
MD5:	8E92E700BAAA7E8DC4F32B991AE9FF3F
SHA1:	D9582AC8AF82F4AEDC2E480DEF97338BAA8F9485
SHA-256:	37E72FBDA01908024E8EE453FA47B7C563FA06918E1537A4E626CA562F695CB2
SHA-512:	FAD4FAA198D8B97F5EC3ED4388F61E4E4B6BFD8E6085AA28CD0D3DB4FFA65ABB345112A78D4E5A1347C1DC4B831ADDE7C9E9D43F7DB17AE3F935EB90FBAB EA13
Malicious:	false
Preview:	0\r..m....._....._keyhttps://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js .https://live.com/.K.OP&/.....B..%<.....,.%..).H.8.>. Y....Y.A..Eo.....r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7cab34efca253074_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.719019204934808
Encrypted:	false
SSDEEP:	6:mmKVYcRTbVYXvCVJumSrR5NdJl/g59YH69h2bK6t:KBEaixR5NdJe9uN
MD5:	AD2FA180F2394FEDC3354C0FF8BF07E9
SHA1:	17023501660840EDDF7898D0474E7864B51421E6
SHA-256:	B79F04F4C31BE9CE96C5344DC0FBD1AC90BC4AB1345B204FEBBDC90E9A58C1AB
SHA-512:	973E7ACC19A8BD8C9A2FC532C13CBF507FD80FE438B6363E8B1F0080DD5F81B3CFB8AF9BC07F656C176E2C33C5A28E624E638536236823462BE9FB86FC712C(B
Malicious:	false
Preview:	0\r..m.....e...d....._keyhttps://acctcdn.msauth.net/resetpasswordpackage_X7k_NcCIooflIFuKCGNtCw2.js?v=1 .https://live.com/...OP&/.....3.....l.....e.GS.;.m. .5.1.^R.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7e4cea594f77c74d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.710204738035621
Encrypted:	false
SSDEEP:	6:mOEYcRTdFAwhTT5NdK/g3KL2lBy496bK6t:KFAwhTT5NdM7
MD5:	74B0CDDFBC8CBF09722B36230BF4DD09
SHA1:	14216F5B996DECA457AEBC6DB287AC5B56103630
SHA-256:	C045D243049F5C08BE09500D99F809F3FEEDC10770CBCF4D79C161190B24737E
SHA-512:	E169BEABA756B7D6AACB65C12268C20078D1F4E79546BFD2C56B5731327220391E556BC707D964F1C0476E4ED0D22F94D01EB530CE77E3E280EED5D22E8C74D
Malicious:	false
Preview:	0\r..m.....V...$.DV...._keyhttps://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1 .https://live.com/U..OP&/.....}.....}OZ.\.,...mg.:Y...b..;.p.kg+.."S .A..Eo.....B.'.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f469a98fdcf53c25_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.692099302413636
Encrypted:	false
SSDEEP:	6:mTJIEYcRTRKGKcqdsHKT5NddQWl/gkYdzfDLgrhJhK6t:SkcG5NddLYdzLUdJ7
MD5:	356E05F1EC74F0A9ED9243D1C0CCFE1B
SHA1:	5ED71A30ABBAF2F1C8AFF84A17B726DC0E89B515
SHA-256:	A0FA99A860276CA2CB6899A6A11203ABB9756C6718F43EE9E022FCE3ADAACF58
SHA-512:	4A28E0121A71986F1A7AF2E3296806AA433783F8C92914AAE62BD4230510234179A2A23BAE070D8D131FC57F6014EFF70E8B9B5A358FC896A239BB8E5C68533F
Malicious:	false
Preview:	0\r..m.....]...z.>...._keyhttps://acctcdn.msauth.net/knockout_old_GJ62c6D9R5HuKFdkoO8XYw2.js?v=1 .https://live.com/Ni.OP&/...../fe-*h.8.jd...L....J6. .N.$.d.A..Eo.....5.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f6ef8939da32ec75_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.704487314392845
Encrypted:	false
SSDEEP:	6:mKYcRTOWxEDLU4G3eLPDNdy1l/gLsZVl/YK6t:eRLU4MUrNdV4li
MD5:	EF393E32B2793D43B6BF00D3B8D7F116
SHA1:	59F94BEC545FCDB950CC88DB16907BAE97A4F791
SHA-256:	BEDE6380EE0D259FA8B2B74FB6310CB5759AE30F4F495A1D760F00D49E4397AB
SHA-512:	520794138680D67C507C3F39FF7EC8A42D6E994F03A18E3CF4525F98387F84D2E3E83FE8906EBFAAB037F5F6E1B78B161292618F7BBEC1D450675035174370F7
Malicious:	false
Preview:	0\r..m.....`...Z..U...._keyhttps://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1 .https://live.com/<8.OP&/.....&<.}...k4E/q..Py..p.8W .G..*.2....A..Eo.....)..^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	432
Entropy (8bit):	4.836605002330125
Encrypted:	false
SSDEEP:	6:30AXTTFvtZKR9lfpXAkFBAzzQ3zbn3pHkQ+IRwHli:3pHfZKR97FBAzzyz7V4hc
MD5:	1AC2EB732260AAFF66A24969BEF8891E
SHA1:	3FFC8505497D31EDDB6C5BAB41D6A82B628F5B7B
SHA-256:	E920F508E1CF7BBF944700BA3A20DF307D10ADFF4FB2C5DE4BA08E0EF018C1FE
SHA-512:	179B7F359307DE51A82A9850D59A21369EA9764C8FB1D814726188C22CAD6B3078408404CD7D6984923E9096A454A9BB7C9101873A5076C87AB08F5DEF8D00C5
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Preview:	.....^oy retne.....SHM..Y..`LP&/.....M.wOY.L~..`LP&/.....t0%..4.|..`LP&/.....q....0&..`LP&/.....%<...i..`LP&/.....pT.....`LP&/.....u.2.9.....`LP&/.... .....C43.xB..`LP&/.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q....._.KPu../.....+<P|...X.KPu../. .....2.gLP&/.

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):	36864
Entropy (8bit):	1.5356091566010543
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7UOlnH2ZLLOpEO5J/Kn7U1j5p07HVpLLOpEO5J/Kn7UhqFSN3+:dNw/NwfKHNwcy/gK/dA
MD5:	4B1689DF9D7E089B13B373961EA3AFD4
SHA1:	2DD4A8CF8CC5457E198110C4004D40ECCCE3E672
SHA-256:	FB67A9C67C36F2F20D6253F18F434B817CFD6D7A14EBC061B4918EA6ADD1BCFF
SHA-512:	B1F40FDC95C36E8922C014492DBB981AA90F251360272E441F8BFCDE2A3061C9CC2FA19300FE27C68418C1081EB4B8A5DA17EDD05A2F61225AEB9BAA73B201 A
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):	38508
Entropy (8bit):	1.206976501042398
Encrypted:	false
SSDEEP:	48:I8NOZuWq5LLOpEO5J/Kn7U9clnHSqekLLOpEO5J/Kn7U1K5p07HXqZLLOpEO5J/V:ROuWcNwlMNwoK78NwV
MD5:	67849F8FD257864DD79E2BB607FA4CA4
SHA1:	E3A7952F84C5249BBE5038D8972A9CD4E9636AE3
SHA-256:	369410A1C89609E2F7E3E8442B16EF8713FFC8BD1DC7EFF3DC50402AF4AB5A5A
SHA-512:	5A7A340E85AD22DB2021244C6DC86BBD5A9B5438F2CA6275AB6135C5B29D6AC80CE4FECD1181C8DDD741126382B19C5C2CD57093FDDF00EDB6531E0587865 9
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):	7128
Entropy (8bit):	4.176092067696386
Encrypted:	false
SSDEEP:	96:34Px/Ukit41EK7JckiPYpOkHX0MwC5AvFXJIxROkHX0PwC5AvFXJIxV5i:3Ix/Ukit41ZJckiilq5sDAq5szi
MD5:	2E399930FAD110DD1BE86CE5CCCFC66F
SHA1:	62D72EC32524EB30D39CC10AEE6542FACE29157E
SHA-256:	CD42C589B85E625AF5E1BA5F852C0BA66C3A552838D1494653FAE63CF9BCDB71
SHA-512:	ED68DEA01150E8A2CE3805D9481230128A638B4FA227D0448B612AFFF5FBF58AB36E8DAA72A90B283C7586F200D5FE646DF2E371956A77D34BF3210DC6D82F9
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...1d5c6850_8ce6_44ea_986c_3fab7edfeb6e.....%u..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....y..t.....file:///C:/Users/user/Desktop/%23U00e2_%23U00 e2_Play%20_to%20_Listen.htm?bbre=1626976601159#/1626976601159-@!&EfQBIjex4nAvaSN&@!QtCJrXmE3YnhHsy5VU2ow!&@-erika.lontoc@enbridge.com- 1626976601159/1626976601159.....h.....`.....vO^.....wO^.....f.i.l.e.:././.C. :./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.%.2.3.U.0.0.e.2._.%.2.3.U.0.0.e.2._.P.l.a.y.%.2.0._.t.o.%.2.0._.L.i.s.t.e.n...h.t.m.?.b.b.r.e.=.1.6.2.6.9.7.6.6.0.1.1.5.9.#./.1.6.2.6.9. 7.6.6.0.1.1.5.9.-.@.!.&.E.f.Q.B.I.j.e.x.4.n.A.v.a.S.N.&.@.!

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

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.232775432396321
Encrypted:	false
SSDEEP:	6:mAxq2PWXp+N23iKKdK8aPrqIFUtpBtZmwPB+zkwOWXp+N23iKKdK8amLJ:Xva5KkL3FUtpT/Pc5f5KkQJ
MD5:	BCD92D9CAF73FBA22AB9CB44A5C145A4
SHA1:	8C70F0F13314FF5F7EBD0B77EA7CC84E4F706B93
SHA-256:	99148DE1C450BB5F6355B65D63BD3794D743B4937715D5EBB81974E8C5F77768
SHA-512:	66D6E161C1E0555F307D682D758E7384B7D4F8FE068E08434EB3A19E75E36A895DA060A3913293F88A08C65BD59437E816A27ABBF9A63729E0ED927B4E97950F
Malicious:	false
Preview:	2021/07/22-10:56:40.094 544 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/22-10 :56:40.095 544 Recovering log #3.2021/07/22-10:56:40.096 544 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003. log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.256205908389169
Encrypted:	false
SSDEEP:	6:mA3RVnt+q2PWXp+N23iKKdK8NIFUtpB3RRAZmwPB3Rk3VkwOWXp+N23iKKdK8+ed:dova5KkpFUtp5A/PcF5f5KkqJ
MD5:	573E5768BAB1B5D3D43A54B450E905AC
SHA1:	9362B2724B3452D0CE0F4D90111505799990E076
SHA-256:	50D6F3C23EFEA0479B90753D0A5E21EC250B6604ABB22F54D259F09D02343C98
SHA-512:	A4F58225F998508C675B0BD2FAC559A5A6D6D3C6C686ECF5EF610B77D7DFEA071826AD93828C5F6E50D4B1FA958DD7C2332090D742FBFD1745E42222BEFD87
Malicious:	false
Preview:	2021/07/22-10:56:42.342 718 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/22-10 :56:42.343 718 Recovering log #3.2021/07/22-10:56:42.345 718 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003. log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH: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=","VtBwXoadl3EP336rAiL33Gz19KGqtN+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):	34816

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Entropy (8bit):	1.8378863932958847
Encrypted:	false
SSDEEP:	96:yBCNwslG0905bslXNBCqOkHX0+jsl30903090YOkuYslXpOX0:IWg4OWbRDo4C4puV
MD5:	DEC3FEDD9D0DB4DEA060C609CFBA6010
SHA1:	7CC7CA1C8A3F9CC3D1E6D8AA506FC77819E37E58
SHA-256:	C96F9437C906D88C00F9D5239C4FE785C140E904C71104313A76A1F3B4698969
SHA-512:	A1D7946F30D2A87E2B470EC313281C488F6968B68076EC6BAB3E4203BACFE6BF526399F6FDB27F52D55DD3B65A931B223C3FA1E0577705176100F88CAEFBBD3
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):	33944
Entropy (8bit):	1.1394165205370042
Encrypted:	false
SSDEEP:	48:QKdBmw6fUe36sl+sl0tjI90R4lGiNBmw6fU1sc5TCvVTCm/3n:QKdBCgsl+slG090INBCjykx
MD5:	14ADFDC1F0BAC9074370679162D2C0AD
SHA1:	3A6A2E2A37FAD6902BE01505F6EA59B21A206F10
SHA-256:	29867F47C0B94833F438BC99F9BFD560417EA9BA775D6F12D5974A8EFBB36D4A
SHA-512:	4B6C508D2206F69A2A17D5E5BC1C0CDD6F7C95B9066E58A1BFC45091736F81F831162402114742BE25C44933EC3960F9032156F47FC3E49A8D7CD5404FE1E773
Malicious:	false
Preview:	.....@..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.333382444976114
Encrypted:	false
SSDEEP:	6:mAxJHUN+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpBxOdXZmwPBx2GVkwOWXp+N23U:JUIva5KkTXfchI3FUtp+5/PmW5f5KkTM
MD5:	35FD7FBC80434987784633262C96418B
SHA1:	E3B75198C06DB3501E161F0B01717A6BBCC3E415
SHA-256:	E91319994172222E52867A0F150EA1833A449E96BDDBA1C63F64427F481366AA8
SHA-512:	5613AFC67AB50DFD36E8205F2A924EA496A65E800B874E08079439835FB1327F3CE21D37FB7569EBE9FEE18E3325AC24A60E169C93280DCB69309BA1403EFA75
Malicious:	false
Preview:	2021/07/22-10:56:45.468 1938 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/22-10:56:45.499 1938 Recovering log #3.2021/07/22-10:56:45.500 1938 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.2976232628762405
Encrypted:	false
SSDEEP:	6:mAxJRN+q2PWXp+N23iKKdK25+XuoIFUtpBxJXdFZZmwPBxJjUtVkwOWXp+N23iKX:Uva5KkTXYFUtpH/PdUT5f5KkTXHJ
MD5:	22637F5301EA3E944FB1C89B403E3857
SHA1:	59D0FD6CD13E95939F3FBC34790E4F8BF16E4E69
SHA-256:	A2E9028A066C0ECE96368FE1F84D1CB15B6B9BFC5701B3790EBBE059BE36853A
SHA-512:	49F1271CB002F50E47FEB8A5F6D39D07DB22F227A938B6E80EC77A84ABD8547AC52D7EB6B2456C80627BDCF4D431A1BDD65682C57448AE91539F6123A2D0D43
Malicious:	false
Preview:	2021/07/22-10:56:45.461 1938 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/22-10:56:45.463 1938 Recovering log #3.2021/07/22-10:56:45.464 1938 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):	5.321559818796826
Encrypted:	false
SSDEEP:	6:mAxL0N+q2PWXp+N23iKKdKWT5g1IdqIFUtpBxSdFZZmwPBxSdFNVkwOWXp+N23im:L0Iva5Kkg5gSRFUtpC5/PCT5f5Kkg5gZ
MD5:	8A3D5FB636F5BF79DC8E71F5BB502D06
SHA1:	B59B229567CBEA7EE31F942A974B3DCB400DF472
SHA-256:	50A6B0AC3473B11E26DCF731E63148F448E0326A7234ACC992AE21C08CFA43A0
SHA-512:	66F21396731F3688ABE02AA8A550698E2FD4A615531AA6756BFFADE7CE6162F9254F0EFAB14E5BB46B4A9DD0EC8B2D3E0C1B9AFFF311BF39C6FF18A4AB0DFB8E
Malicious:	false
Preview:	2021/07/22-10:56:45.448 1938 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/22-10:56:45.451 1938 Recovering log #3.2021/07/22-10:56:45.451 1938 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):	0.4481240366544235
Encrypted:	false
SSDEEP:	3:8Eflr8:8B
MD5:	37DD4126C4B47E81368D263098009363
SHA1:	D001C8FDE0A73D04DA7A40935A6A7BC38EF1AACC
SHA-256:	FD0AD5D9A9BA787ADE462C7B286D0F8B7B2577DF539F77BF79406CF286D118F2
SHA-512:	7BAA4CB2F6E549A85190C0CBF7669352EC6C3F022B060E8939579AD501CFCAAC607940202B937E3EF692FCD84349EBBB6923807E127BF3713611BC685A975644
Malicious:	false
Preview:	.'..(..... .....'.LP&/.....

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):	61440
Entropy (8bit):	0.5862146805587233
Encrypted:	false
SSDEEP:	48:THGf6TCkcrIAZY5TCvUxOk6UX7rRPmofVRzTCkgyrPRinOk6UX7rRPmMTCvt:TIa+gPxOkHX0aVlOePsOkHX04W
MD5:	7E577A35E56EA937B0D1B2CA7CA86372
SHA1:	77E9E51C1EB9848D0B22C212BE8F595065958ED3
SHA-256:	3788309771FBD6E8C20DFBF9A1546D4E43C1C93A448615E143749C47E8E15AFE
SHA-512:	BA5A5FF6933A82A3E6745FF4F8B77B863027CAF3CA63E8A0273625A7047B8D1AD3132033F7BE753531A50B1E24B4DF3CC779B74D12B24A18386C35A97A79F2DE
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
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):	1413
Entropy (8bit):	5.839743568931357
Encrypted:	false
SSDEEP:	24:J2lyQqPo6WJdOTXA6URGWdPwHNydOjdMY7O2WxvpQFAUC1VR78EUQo1+HPRj:J1QyDTXSZwtndJ7XWxyTCToa
MD5:	D1B7B0CEB7872E822A42593481E84A17
SHA1:	5109153C49F281CA07CCDD23C4114513BF21D659
SHA-256:	09C16402A26D3A39E7C489D1E45A3F2EB20384F5B66F1203465B407018DA998D
SHA-512:	264FA5CCEEAFD61E25F29CD48EBBFFCE354316DC5D52C847F42469F3D15A379849EA6243DC50794B9DB2AD1DDFF7F83DB47CDC1C49FB1E5ABEF7232E5571AC1D
Malicious:	false
Preview:	."....1626976601159.._..bbre..c..com..desktop..efqbijex4navasn..enbridge..erika..file..user..htm..listen..lontoc..play..qtcjrxme3ynhhsy5vu2ow..to..u00e2..users*.....1626976601159....._.....bbre.....c.....com.....desktop.....efqbijex4navasn.....enbridge.....erika.....file.....user.....htm.....listen.....lontoc.....play.....qtcjrxme3ynhhsy5vu2ow.....to.....u00e2.....users..2...$....0.....1.....2.....3.....4.....5.....6.....7.....9....._.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....x.....y.....z...:.....B.....

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):	71328
Entropy (8bit):	0.22952829555360346
Encrypted:	false
SSDEEP:	24:uqLB33iUQFAUC1VRQQFmVQfxcCtQFAUC1VRlc/3C4UeAU1irmgWbNqTfR:uqh3i5TCvFmGf6TCk3C4UeAU8rmNiR
MD5:	17F37F8ACB216182B77B0AC6B60B2BE2
SHA1:	2E07C30D0256CBBC9FEC334D185B1D2D009FD4F5
SHA-256:	C32D681134A5F3EE6DF27C9EDB7F143D50F5C0B75A5D1135472AAF194AABB855
SHA-512:	31F92B7EC52DEE9E69D9BA3AC670DFE0BE9B8AC3E96A02D4F4C78B92E9183D81E0B69403BB510D6D9F334115BF52D1FDC40876E5B5A5CCC5D661ABD3DA00FA1A
Malicious:	false
Preview:	.....R.#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3313
Entropy (8bit):	5.535786566442866
Encrypted:	false
SSDEEP:	48:vDPp/mmlllWdvG61a7JM88dbz0h8bQSefgGTNrS0U9RdiN9M:v19Wa7JMPdbz0h8bQ5fgGBrS0G
MD5:	75648CDB2C7877E056EB101713D791D8
SHA1:	9360B942E9DED6E7C4228A90665E7EF925E002A5
SHA-256:	96FD5F744CED3F301906FE4A9F15DE51EDA93CA0B55F5B7F34F415BA6484D38F
SHA-512:	924BB58E0604C13F00933267CA6B370D992CAE07D7A992D1621A948E79CACF687C258D911AE8B13684AC53B00242968DC2617BFD0AE4219A4EA016F0AC8B50F
Malicious:	false
Preview:	d.>"_..*.....META:file://...._file://..browserkeyN.{"browser":{"detect_browser":"","detect_browser_detail":"","detect_btan":""}}.._file://..userkey...{"user":{"keepLoginLongtime":0,"AuthNBR":false,"AuthKeyNBR":false,"tk_nbr_uc_frv":"","br_nbrcheck":"","br_utcheck":"","testlist":[]}}.!_file://._canWriteToLocalStorage.._file://..nbrteststst...../.....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..455935000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-22 10:56:47.90][INFO][mr.Init] MR instance ID: 73acf0b0-017b-4a31-8452-b74f7ba3305f\n","[2021-07-22 10:56:47.90][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-22 10:56:47.90][INFO][mr.Init] Na

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.26238492506925
Encrypted:	false
SSDEEP:	6:mAoH0Vq2PWXp+N23iKKdK8a2jMGIFUtpB6VC0gZmwPB6uxSIkwOWXp+N23iKKdKw:usva5Kk8EFUtpYVC9/PYuv5f5Kk8bJ
MD5:	0CE901583739FEC50DA5DAC7C5AECD0E
SHA1:	E9C044E905FB1419B1766D9CEE2CC5E1B88F3B09
SHA-256:	E97E62A71DCB27C13A9EFEBB084FA43BE0C48548FCE27C5606BDA06E4858DBF1
SHA-512:	47B22AA7CABB3E94AF95E2365C25BCCFD239F53D8D3BE64C58A7AA82265F83C96F3A215E6F1A6F0814C010DEA5B2C7197E7443F3627B63795AA6E8F5C1B7EC F
Malicious:	false
Preview:	2021/07/22-10:56:39.798 bb4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/22-10:56:39.807 bb4 Recovering log #3.2021/07/22-10:56:39.810 bb4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
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):	24576
Entropy (8bit):	1.1238194639939816
Encrypted:	false
SSDEEP:	48:Trw/qALihje9kqL42WOT/XUHqbw/qALihje9kqL42WOT/3U69:vOqAuhjspnWO20OqAuhjspnWOY69
MD5:	33728A8AD6AA2EEC250B13C256566496
SHA1:	9BF5422A19BADFF94FA595466AE461A225C1EFF4
SHA-256:	3A5B45C1515B4207BB32FF1C8173AFFC01D9BCE20FEF5E629866174739CB924F
SHA-512:	CEEAAEAC302426FD9F9AC93F1442530AC812A892D2A1152C1542F09FC3B8016894FF90ED8CAAB988ABF15ABDD72898FBC54BB9379CA14080982542E1402344E
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.0203246881377737
Encrypted:	false
SSDEEP:	48:g4q7w/qALihje9kqL42WOT/sgqrw/qALihje9kqL42WOT/o8:g4UOqAuhjspnWOVkOqAuhjspnWO/
MD5:	4C3F81DFC83463702AE0322A86053636
SHA1:	4C34838FBAB0D58454C457AD1418E7A54669C5E2
SHA-256:	3E2CC6522DA1A27322C0CD3FED40840A2E816D0AD4CDC3A93105BA87BBEF762F
SHA-512:	17C8E202BF1FB016DCBAC6C94AF7CA44E258ED1DED14AE9D2AA536E44662FF00951936909FC04BC424CA566F79EDF1705FBA5A637AEEC59118D33F48A54C5E DF
Malicious:	false
Preview:	.....].j. ....

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):	5.194452374622653
Encrypted:	false
SSDEEP:	6:mAD+q2PWXp+N23iKKdKgXz4rRIFUtpBlZmwPBJVkwOWXp+N23iKKdKgXz4q8LJ:V+va5KkgXiuFUtpf/PfV5f5KkgX2J
MD5:	1F690DC74B3085B94D4869FF070FB34D
SHA1:	B9DF53CF22F32BE202319B679841008150BC0357
SHA-256:	1E628F071C8E458E0C775AACCEDC37B77B74B0C36D5EAB9EBE0BF7440637F612
SHA-512:	8A8A47A29D38396D7010B99253893F99810B6EE055106DEFF8BF1498214416A9F1C811688E6F12AEE650DE1651F884277B2119132942A3AFEA384EF9C0FEA7E9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Malicious:	false
Preview:	2021/07/22-10:56:40.120 1dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/22-10:56:40.122 1dc Recovering log #3.2021/07/22-10:56:40.122 1dc 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):	1.4385309497709027
Encrypted:	false
SSDEEP:	96:wIElwQF8mpcSH1AW4t/Kjw6L07R4tujw6tsj:wIElwQF8mpcSVL4kiV4oq
MD5:	7309B2D524F17BEB09BA251C979494FA
SHA1:	EF46BB4203353FD0A6EE2C1A3C77BF05BA896E6B
SHA-256:	A7C44425EAD9811414826E8F4B6414E40244F6CA64005B7B3178D8A6F7F2BFFF
SHA-512:	BB377565EB98ED8DEA1A421B7DCA6192EC049349796FB6B60E29DAFB757B881A1C841189D42C38C47BB60AA208C0F89FA979323FA1226D2F6EB991F41A70CD73
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):	0.627536440268224
Encrypted:	false
SSDEEP:	48:qEZqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUc4:qQhIElwQF8mpcSH
MD5:	8CF057FFA9B631ACB093F58EA545480B
SHA1:	D2689B1CA316A95E293B223B18955144CB3BCEBB
SHA-256:	64BFBAD8D7D3DF9C5D36381154B70A7DE41AB74C9E5EC9C39E1BA4845C867CE7
SHA-512:	5AF7787EE4460A6EE35138C303A6354A05B05318B068BA115A2200C41DBBF450D3C621429FD0F1FB0E8658A6F960701ECBFE3E2E399EA30941AFA84219C06CAE
Malicious:	false
Preview:	.....}.o\..... ....

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):	265
Entropy (8bit):	4.3407395327318525
Encrypted:	false
SSDEEP:	6:5lVzb/llaH+dzGz2Jef3ul1kAl1kAl1kAl1kAl1:5l5/lYeI2JKmkAvkAvkAvkAv
MD5:	B87C8611134F3764A54C1EFFA76ECE2F
SHA1:	077851974F47EA497CD33C9BEC40F72EFFE6A57F
SHA-256:	8C88DAAA90C9F3686E44180ED955AA19306B12822C60672984DF2B07991E1A09
SHA-512:	0692C44AD041345573FC16D83DB50A58F1AA6CDF03C8110D5B6CE36310BFE02EBCD7AF0289C13F1C9E629A0F11F21356D58BE4AFB52A4FDECBEA075CDA2E8A9
Malicious:	false
Preview:	..&f.....0..BV.....next-map-id.1.7namespace-1d5c6850_8ce6_44ea_986c_3fab7edfeb6e-file:///.0&U.93.....map-0-ReadyFIle.{.}...map-0-nbrteststst. ....

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):	5.1971297082943755

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Encrypted:	false
SSDEEP:	6:mAqV1WM+q2PWXp+N23iKKdKrQMxIFUtpBZ1ZmwPBgrWMVkwOWXp+N23iKKdKrQMT:UV1L+va5KkCFUtpJ/P8LV5f5KktJ
MD5:	895C1F67926C55D80CA2518793921345
SHA1:	5C378BCE745F472606264CB967A473A96BC8C0F4
SHA-256:	FBBDAC2FEC7F717C881F139467CB1BC1BBB1D561D23F2AD205A5E75BF77B2CD1
SHA-512:	C34923B5635FA73DF7B17A7D37E8A26C2C9BA5F19415EAA6B4199059ED668720395CEA13C91FBB9466681AD789B770A2372C101814990CECC6A1066C81A5E24
Malicious:	false
Preview:	2021/07/22-10:56:40.017 bac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/22-10 :56:40.018 bac Recovering log #3.2021/07/22-10:56:40.019 bac 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):	342
Entropy (8bit):	5.206254760509311
Encrypted:	false
SSDEEP:	6:mAWvIq2PWXp+N23iKKdK7Uh2ghZIFUtpB6V5ZmwPB6VODkwOWXp+N23iKKdK7Uh9:wAva5KkIhHh2FUtpYV5/PYVQ5f5KkIh9
MD5:	0CA9665A72DF2CA331598D1C40116324
SHA1:	948AD163A9CA852716D22D84F46A989F71E03DCA
SHA-256:	F110D550DA82C3AB09463E8139C28923E9D3E3FCCE216801BAE14EB1BC65C838
SHA-512:	22B4E1D634D5BFB2827FDCC49D6C7CDD38C5B762BF0767E0717ADE1D977FF96F18E0659965835A192F7E774245B0351AD85C978A6DCD554059DA27D027CA83
Malicious:	false
Preview:	2021/07/22-10:56:39.792 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001. 2021/07/22-10:56:39.804 f0 Recovering log #3.2021/07/22-10:56:39.807 f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Charact eristics 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):	430
Entropy (8bit):	5.245481178189756
Encrypted:	false
SSDEEP:	6:mA7Iq2PWXp+N23iKKdKusNpV/2jMGIFUtpBLfZmwPBLNkwOWXp+N23iKKdKusNp+:pIva5KkFFUtpVf/PVN5f5KkOJ
MD5:	F6EB65247BDC781CBEBE2D9602DD13DC
SHA1:	38113DC246180B928EDAF3090F6BEE2A89EBC685
SHA-256:	A03C5C1848A472A97DB83FC32B620393539FF55F899F9820226E1A0CC1030DA9
SHA-512:	5E11DED75C8C8ADF8754606666B10206D5A5914CB5FC8BB06ED71B579E2B486B84A6670FAD4404E08BB09F026DC6CC89318BC855ED14E8B6DEA908BD2B2E4E 41
Malicious:	false
Preview:	2021/07/22-10:56:40.082 15e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-10:56:40.084 15e0 Recovering log #3.2021/07/22-10:56:40.084 15e0 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.307275532300419
Encrypted:	false
SSDEEP:	6:mAQX9+q2PWXp+N23iKKdKusNpqz4rRIFUtpBkwZmwPBGNVkwOWXp+N23iKKdKusX:aX4va5KkmiuFUtpmw/P45f5Kkm2J
MD5:	20506978E9E5C138CB3ACD4AF514817A
SHA1:	2F4C1CEA33CC37E11258309B6367896BC609E083
SHA-256:	2D777A433297B66E325A0309AE0F9D0252E814433C63F03195F3994E3BB22615
SHA-512:	72AFF6076675DDD0D29EDE14E7B7DEAABB1BD883DF9AA3951144680E45AA615EDCA8696214D5356A8C528281A622F23B2B97B818CAA3E9C732144EA98B1D8FA
Malicious:	false
Preview:	2021/07/22-10:56:40.117 bc8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/07/22-10:56:40.118 bc8 Recovering log #3.2021/07/22-10:56:40.119 bc8 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):	5.288867972678908
Encrypted:	false
SSDEEP:	6:mAdCL+q2PWXp+N23iKKdKusNpZQMxIFUtpBdc7ZmwPBdMcVkwOWXp+N23iKKdKuG:HCL+va5KkMFUtpXC/PXzV5f5KkTJ
MD5:	72753463A3AFA5CA2AA234213E3660CE
SHA1:	3257A2985C5E234A17AED7DCD0E3A7DE27A699A5
SHA-256:	4EFA01836417809DC2C1BF747A7C521622D48B681BBFE48FBB77DDC9AAEEADBB
SHA-512:	67D0293C9319D119EA51CDA7C2936C72204E64ED9B7AB936CCBFA7A31CD4FAC6DD196CBAD85E0488F4587912513032C9763159AC2A1105DBEED53FE4BEB8154
Malicious:	false
Preview:	2021/07/22-10:56:56.344 1dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/07/22-10:56:56.346 1dc Recovering log #3.2021/07/22-10:56:56.347 1dc 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\d5dd8309-2c52-4367-a472-d42383780cd9.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\d5dd8309-2c52-4367-a472-d42383780cd9.tmp	
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\9209b84d-f87d-4c88-a1ae-740cdded2081.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.2422874515518325
Encrypted:	false
SSDEEP:	12:pva5KkkGHArBFUtpbA/PtWD5f5KkkGHAryJ:Va5KkkGgPg1/Vf5KkkGga
MD5:	7817BB62C7864DA089E687126E480DC3
SHA1:	456678ECAF274C1E42EB6B893BBDB04697DA176F
SHA-256:	E6D8C0574ADA7780D637363CAFC778364A34DB7F09552D150552FBF46BF164C6
SHA-512:	7858B67E3DA09D05E38B0CA5E329A1D75EBDC1AD629D8604CEA8EFEA29969E741682FF688BCDD4D02702E6DEA580AA52D51C539486EF10E34F0E628E0FA4C0E3
Malicious:	false
Preview:	2021/07/22-10:56:46.419 718 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-10:56:46.420 718 Recovering log #3.2021/07/22-10:56:46.426 718 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.273650472439844
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
SSDEEP:	12:9va5KkkGHArqiuFUtpC5/Pi5f5KkkGHArq2J:ha5KkkGgCgEWf5KkkGg7
MD5:	16D50E3A1DF0F473EFE7386DFCABFD0C
SHA1:	F43949D153F7F973C3C1B2E430C57536DE223F67
SHA-256:	39B5AFE7B05AF912910119C6D0A59A835DB0C2DB7A4575D0945207E2B52B7BFB
SHA-512:	66748081BB874AA6AB167C1A55E167AB79F124E64583090FD4CEC057912E0612C498D60187B660819A79C3F4BA45ECB0E8A695B2AA342362B09127C403AE0571
Malicious:	false
Preview:	2021/07/22-10:56:46.437 718 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/07/22-10:56:46.439 718 Recovering log #3.2021/07/22-10:56:46.440 718 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.1533816821426495
Encrypted:	false
SSDEEP:	12:y+va5KkkGHArAFUtpMZ/PMNV5f5KkkGHArfJ:Da5KkkGgkglf5KkkGgV
MD5:	C7C6C6D8107C0E5477151C6F406333E6
SHA1:	898A9ECB8E0DBCF34DB5DF9472D4C3044DF2A34F
SHA-256:	5A12F8E2A0BAE955B4A19E4D465256304CE1D9D3802B871F9FB05121B7657214
SHA-512:	39D2CA3B7E52C49F1E50B197AFF1860871BFE2EBB5C2A3329C110B80307CABCA406C18FAFDB27EAD4AF70E50B779505F13D9F33830A80D8013D726A0DB30AF B
Malicious:	false
Preview:	2021/07/22-10:57:01.925 1dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/07/22-10:57:01.927 1dc Recovering log #3.2021/07/22-10:57:01.927 1dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Size (bytes):	324
Entropy (8bit):	5.283310946388058
Encrypted:	false
SSDEEP:	6:mAG+q2PWXp+N23iKKdKpIFUtpB6VoGZmwPB6VaSVkwOWXp+N23iKKdKa/WLJ:4+va5KkmFUtpYVoG/PYVxV5f5KkaUJ
MD5:	71065050ACCA34ADEF2610A1ABA895A7
SHA1:	1E8CF693FE04DB4B92DEFDED0ACA709CEE7B2E14
SHA-256:	41D6518B06ED1E31E40856ABEC3A27F65CAE0F5FED913953213433E41399611E
SHA-512:	2289AF43D15ABE43B36FE59972CDD2A184621258C2AB86E2241C5CCF39C15D2D5F8504EB38DC52CBE922C0F409AD9CC33682C06E6F4383129EA2CC88C58BE0 0
Malicious:	false
Preview:	2021/07/22-10:56:39.790 12bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/22-10:56:39.802 12bc Recovering log #3.2021/07/22-10:56:39.806 12bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.3490697491767785
Encrypted:	false
SSDEEP:	12:lf+va5KkkOrsFUtpVO/PVlV5f5KkkOrzJ:lka5Kk+gjodf5Kkn
MD5:	08CAE83D37251F85431C02635000919B
SHA1:	57CED769749ABCB6ED0BC0923F65693BF5304844
SHA-256:	B316307BDA0B4D69551D355548948D05D332A65807F32F27E6DBC687549ED181
SHA-512:	912023953C8DB50B3E5E9906C563638111DFABC95F9C04D9626EADA728D16DB0C36324561E514E32FEF0A8D008C3E842C9E8CC943119783A6EF527D568E139C
Malicious:	false
Preview:	2021/07/22-10:56:47.880 1dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/22-10:56:47.881 1dc Recovering log #3.2021/07/22-10:56:47.882 1dc 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):	48
Entropy (8bit):	4.563721875540868
Encrypted:	false
SSDEEP:	3:QRc5V5yl+h8lP2QrvD7:Ec5T2W8IPFTD7
MD5:	12D3A70D8F1EBEC7EABDB17D0A5384D9
SHA1:	143927F302C6FABE4E5633C9657BDAC398DA6D6D
SHA-256:	A671F27227FD10611BB06AA34481FFF484783EEC75BEE7244E7D8AA0F0831D30
SHA-512:	163F0A4824FDDE754C1856021ECADEC65BF3B9B03646026A6F41B0003080FFC1BEE4BD007520D7FD30180B4EDAF0C89E5672D15C2C8D8754F02C20EE3EC136
Malicious:	false
Preview:	.....td..0.....*p....?....A.....a.....J.)1%%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bbabfc87-a240-4b8d-821f-598845db053a.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):	3227
Entropy (8bit):	4.855499336658365
Encrypted:	false
SSDEEP:	96:JTnOCXGDHzM1oXH+YrO6a+oLahgq7G7fjhhH:JTnOCXGDHzM1oXHfrO6a+oLaSq7gfjn
MD5:	E17C72CA51DC2F5DF11DC8195B62F7ED
SHA1:	7C2FDEFDB503B9A50DA271C87F903F7E74FC0C26
SHA-256:	D03BEE820C95CF3951EAC62E1B3365DCA1225A4BC048BBD92BEF185189FF9F21
SHA-512:	EAC0309204499231480C56F939EE8F001226EFE315BD13FA3FC71C050B33ED2BBD73F474F1FE632D6746B08E4E4DEB6F8886EE0616656594C69029A1D68400B2
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bbabfc87-a240-4b8d-821f-598845db053a.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://titko.wancdnapp.page","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274042203676076","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274042203676394","port":443,"proto

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cb0cae96-daba-427a-97a5-92928b23ae34.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):	5466
Entropy (8bit):	5.182711819764582
Encrypted:	false
SSDEEP:	96:nACn/JMvm5DWIF7ScKI8ok0JCKL8VbOTQVuwn:nACRMaDPScJ4K6
MD5:	68DA8A95D83FAEAE121FBF47B989CEF4
SHA1:	7905F7023E2939EC9CB48A4D024A6FC635F291C0
SHA-256:	E8B38DDF60D19EDE87F4D21132F76DC495CB3407115CB33ADCA73D285BAAC6E6
SHA-512:	0D63C0F4226D967D517D21B79E4CDBC183FDF55D84F9022B82BFB2F69DD381E27B80BE705A74F034BAB19903F698478ED0174C2C663AE0C3BE2D6F4BB94F323
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271450200094422","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d79d15a9-5231-4456-956d-c50f29f6f08a.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\da6f5efe-3c59-44eb-a2e9-6c8aed899b72.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):	5.535984495827722
Encrypted:	false
SSDEEP:	384:g6xtyLlNkXo1kXqKf/pUZNCgVLH2HfDurUAHGcnTpbs4z:4Ll0o1kXqKf/pUZNCgVLH2HfirUEGcnR
MD5:	1C42D752B423B85B2B578EFD61D58346
SHA1:	0F71102A5AD46AD6AD9F74D250416E90C71F8968
SHA-256:	06C6BF3AF0A183C1166981BC0AF486A51A594D4484EA2C6D11B5295962BD002C
SHA-512:	68F3CE0305992A70941C1B06149FE3ACC26CA88B216A6AD0188965DE01631ACE39FA582BFCA3EE2043ACC7D44C6EE5F665083AEB842AF836F9D4A863CB2167 4
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":"13271450199787139","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
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):	139
Entropy (8bit):	4.564984459196575
Encrypted:	false
SSDEEP:	3:tUKIeQTOLCv1WZmwv32eQTOLzWdkJA7V8s2eQTOL48FWJA7WGv:mAxOoZmwPBxSl7VvBxhv7tv
MD5:	7F985192F92C29AA07085393E4006FE7
SHA1:	AEE4D96253F2373E0BFB71A046E40026C4A74AE7
SHA-256:	24B996BAD0A6CAB712C1925A2929B3E034D9D781BFA53CD0233EF15A58C90A34
SHA-512:	822EA4000B34FDA661A92713D53E71FEA5A45C90B817F44050129FABF52092F5BCB92A2DB6ABDBC076018BB08FAFDF146733B4B70DA5E61062CFD5F4FA3417A 5
Malicious:	false
Preview:	2021/07/22-10:56:45.270 1938 Recovering log #3.2021/07/22-10:56:45.327 1938 Delete type=0 #3.2021/07/22-10:56:45.328 1938 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ec90fb78-de35-4fa6-9dd2-8b8849b8e515.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22594
Entropy (8bit):	5.535909017914011
Encrypted:	false
SSDEEP:	384:g6xt7LlNkXo1kXqKf/pUZNCgVLH2HfDurUAHGznT2is4E:BLl0o1kXqKf/pUZNCgVLH2HfirUEGznI
MD5:	F0DB655AEEAC8017A6EB5976858EB4CF
SHA1:	EE3866B8EF198F4A07C93C7FA5795B8FE4A5BCB4
SHA-256:	74564BCE94374E1D9F9D4D3CEB8AEE1F4487FA7DEB778073242E22FC836D8B57
SHA-512:	65896CA4C031002A4983D940239EC1C957F853F624F1F65DD483373E48A0EE58D50D1EE4C144764F02F51510A71085A9234FE01B18BE855669C967044E4F5423
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ec90fb78-de35-4fa6-9dd2-8b8849b8e515.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13271450199787139","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fc3906b8-9c0e-4a95-8b07-055643a48396.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):	1875
Entropy (8bit):	5.579034839779326
Encrypted:	false
SSDEEP:	48:Yl5UnvVwUu6UUhcUbUaseKUewqPeUer2UefQwUknwUGLxUenw:S5UneUzUUWUbUa3KUGPeU9UE1UkwUGLA
MD5:	C9E2440925F8EDD397FDAC9858532DBA
SHA1:	F4FD824A18EBD4B1ABBC57EBFC991690D9B57542
SHA-256:	832BEF12E0CDB2B50CBB2F02CCA117BF740550DF0E1EE91DE9D5478D2664C338
SHA-512:	6A14FD6B4DCD318E45D75D1526C2925652DFB36E021A38E8812FCA2998A8A7859AA52E7DFAFB23635A48948D2E359E9C4484422531DF23D4686B3E1BCC05902
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1658512686.96406,"host":"D0BW2hoy2RRjWWDvPgW7xCDsfip0ZHUjP5Pz8YbCyJg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626976686.964065},{"expiry":1642756605.463411,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626976605.463416},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbl1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658512605.360597,"host":"e3SziuwfuO2UvuBno+qkR1ObHAzZmSUoJhrc7dbP1Uo=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626976605.360603},{"expiry":1658512608.618354,"host":"lRJYtICs8D4kIE+fyDGXLUGmOLmkh+gKc50EU0l4m7I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626976608.618361},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_obse

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):	5.200656080085651
Encrypted:	false
SSDEEP:	6:mAxuOq2PWXp+N23iKKdKfrzAdIFUtpBxTMNZZmwPBxTMNzkwOWXp+N23iKKdKfrm:uOva5Kk9FUtpjMNZ/PjMNz5f5Kk2J
MD5:	6131DF205C52ED9BD7C52A1511EB12E5
SHA1:	8E5490A9FD852F84B469DF381F09B7F4CBA46F3B
SHA-256:	26FBBB3095AC2238A07461203644DCB742E2A20E967C549C069BA41BE6373CE2
SHA-512:	AA9CF41BA0E1B36F0ED0CCD2C422944EC8A5B5BB25C321D868D9003E71953C4EDBE0CAC3F3A5824EFACAEAD0C3D24EFC583F0363613E604539D02DAE4A8F990
Malicious:	false
Preview:	2021/07/22-10:56:45.659 15e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/07/22-10:56:45.660 15e0 Recovering log #3.2021/07/22-10:56:45.660 15e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
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:	3:8Eflf:8
MD5:	EE14FFE5465304ADB121B2B03192710C
SHA1:	AABCA77ACB36F290F11BB45AFFD6ACFD7D1FFD4A
SHA-256:	A7F96CCC2E95B3A7EC90B19511D185A5BDB435544C241DCF51AF9ACB5398AF11
SHA-512:	2B613695144E003EBB85E50ED95F460A4DC7639903DFF69DADF826E39084DFFFE4CF5A61B7C16385C208ADCEDF807142F6A645A3FFEC309A30FB982B326E011
Malicious:	false
Preview:	.'..(..... ....i..LP&/.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir4088_621323181\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	186784
Entropy (8bit):	4.915957886381836
Encrypted:	false
SSDEEP:	3072:bl35PHEWQyoghJbTloZq6L45c7wbMn5nezpiKmneSxCgWCCkHjuhjMQBJXS:R3NKghJbTl96BXTChW
MD5:	E4ED6CE0DB78ED18701755E5FF177B82
SHA1:	7D660E76CE91C05FC52FE1AD54C28EAD7E4A04B6
SHA-256:	BBA545E82F5720A1AD3BCB3743EB27BB1F015CB2E1222615CB880DA40CE42C20
SHA-512:	F49A4487C245DE86158EE6BD675BF70C74D8FE7164A5AA5D71469AFA94071FD4C06BB09E88E06B1CCDE9ADE6C124C957E45179C25891E12BD7C9FD419B7EBF 72
Malicious:	false
Preview:	.....$...(.....\.....p.....P.....,.....geips..... /.....lgoog.....6.....ozama.....onwod.....Hi..(.....g.bat..... <q..@.....uotpo.....w..X.....ennab.....S..p.....nozam.....E..h....^.....t.....L.....$.....x.....|...l...h...d...`...\...X...H ...P...L...H... ...@.....4...0...,...(...$... .....h.....(.....\|.....t...p...l...h...h...`...H...X...T...$. ..L...H...D...@.....8.....,...(...$... .....p.....4.....|...x...t...p...l...h...d...`...\...X...T...P...L.. .H...

C:\Users\user\AppData\Local\Google\Chrome\User Data\bcfbd2dc-723f-4359-a515-c75e0e03b969.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	165963
Entropy (8bit):	6.049558173339509
Encrypted:	false
SSDEEP:	3072:md5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:y5hnrszc0fZl/xKmaqfIlUOoSiuRY
MD5:	5008D4ECA1D4C0FD04495D0EC526CF83
SHA1:	352C841D6E4BB57A6E63272B3E86D01EB932A669
SHA-256:	50EF5479457EF08593368F3D77528B1D843A48DE0515F19B32413EC2BD2472E6
SHA-512:	FDFD826BF4E1B7DCEE6D317FD5BFD8D965F1B06086DDDD9E32F3C4568DCC8D5967F580F00096C271992943F7C71B7CE71FA705DC8F5461E2FFE4C05AB7D88 5
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":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016772232"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\dadb1716-9259-4092-b8cf-f1b8cd5be034.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174421
Entropy (8bit):	6.0795258650680895
Encrypted:	false
SSDEEP:	3072:mUN5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:JN5hnrszc0fZl/xKmaqfIlUOoSiuRY
MD5:	3453DC5E0E08F60066938D7099ADE767
SHA1:	2D5BF3957EED58C56F628C0241718F8E3D5269EA
SHA-256:	02CB79AB937257D26C504323AFEA2DAA7D34884E8AB6EEF0ECAEDD07914F3D6D
SHA-512:	13AC1F9E5D547BB0650E7FDE30AE66F001550BEC081E14E4D9F130EDD1C500EEE9E76515FEBDB807F624CE08E96E6F4C250E73AF0F2CC463EAAF47A8A79DA6 8C
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":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\de762af8-2e3d-499a-b79b-7c4f6b79a410.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174420
Entropy (8bit):	6.079526235961799
Encrypted:	false
SSDEEP:	3072:mUR5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:JR5hnrszc0fZl/xKmaqfIlUOoSiuRY
MD5:	968D58726AD3EBCDA6DD1A5A9F364C6F
SHA1:	5CE3CE3A86B6BBA8CA214A908FA9A82DFDC63C07
SHA-256:	F6855C507CFC7AFFC37F7EB6C62F43FFE20C7A564E8A8AE618BD8D4BE9FD6AFD
SHA-512:	A4ACDC4F73AAEDD555B7BC1C5B122C610C55324F8CA3148DB59B7AB63B9D266FD13261A869CCD488A573090D8F3CEB2F3A124E6A4B44EC28E684BE0BF574A 20
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":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\e278d02e-572f-473e-b399-a28098695b37.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\e278d02e-572f-473e-b399-a28098695b37.tmp	
Category:	dropped
Size (bytes):	166497
Entropy (8bit):	6.051082650528982
Encrypted:	false
SSDEEP:	3072:JX5phUtGnrszca1FLtEnNwi2rIhJxKnNSdTFcbXafIB0u1GOJmA3iuRJ+:t5hnrszc0fZI/xKmaqfIlUOoSiuRY
MD5:	D6A84E882BC49289529EDCB598569A6D
SHA1:	EBB04D104C627FB79FAEA39E12CB05EF379C7F4C
SHA-256:	1817BE001CAC4E90CB0EE5F80C5FD3B46683C9A2320836072028692285B109CC
SHA-512:	FE5986330772059F7F8D45C1D419FA87BE5A07593B3E7E27969906FC60248C98FD118D9B9E0A0BD723D2ADF0396BEE977F8C804F8428DAC8B8EB2738FA00977A
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":1.626976602457574e+12,"network":1.626944203e+12,"ticks":6262844305.0,"uncertainty":3602195.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAA AAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRh NbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyX OajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1

C:\Users\user\AppData\Local\Temp\2cf10051-368b-4a63-9187-52a96724d6ab.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:	.

Static File Info

General

File type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Entropy (8bit):	6.031952994077906
TrID:	• HyperText Markup Language (15004/1) 83.32% • Text - UTF-8 encoded (3003/1) 16.68%
File name:	#U00e2_#U00e2_Play _to _Listen.htm
File size:	3836
MD5:	59bcd893624173dbb0ae81eb3019974f
SHA1:	995c8ee3b0810659468fbc216e1d8c0d1f2fa1f6
SHA256:	51cb67fbe8cc07001310c8b8c9c78f9b117f8efb03f31ed41dd2432b38639a8b
SHA512:	5a95030326ab98ea9257f851d4248df2068819f99809eb3a07e416e4ee02ea74137fc79e984289d63005c25c1c522ebf4fa442b51b9bd2e05c7b0a2c51779b0a
SSDEEP:	96:OMtt33ZwaJfIaA6nEaMz55crIUqcJ+w1Ict:OKt3XJfnydCrIUqg+CN
File Content Preview:	...<!DOCTYPE html><html><head><script>var fdgfhx="erika.lontoc@enbridge.com"</script>..<script>var hjtyfgcx="@!&EfQBIjex4nAvaSN&@!QtCJrXmE3YnhHsy5VU2ow!&@";if(window.location.href.indexOf("bbre=")==-1) window.location.href = document.location.pathname+"?b

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 10:56:42.054318905 CEST	192.168.2.3	8.8.8.8	0xd5f9	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:42.065114975 CEST	192.168.2.3	8.8.8.8	0xbbb9	Standard query (0)	titko.wancdnapp.page	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:42.068073034 CEST	192.168.2.3	8.8.8.8	0x17fc	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:43.542026997 CEST	192.168.2.3	8.8.8.8	0x44f2	Standard query (0)	manaapdpemtri.fireba seapp.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:43.861809015 CEST	192.168.2.3	8.8.8.8	0xd6e1	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:44.314798117 CEST	192.168.2.3	8.8.8.8	0x43fa	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:45.132850885 CEST	192.168.2.3	8.8.8.8	0x7f9a	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:45.532155037 CEST	192.168.2.3	8.8.8.8	0xa58d	Standard query (0)	noem.urll.pw	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:45.553618908 CEST	192.168.2.3	8.8.8.8	0x2c6a	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:45.857445955 CEST	192.168.2.3	8.8.8.8	0x3abd	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:46.754698992 CEST	192.168.2.3	8.8.8.8	0xe6e8	Standard query (0)	manaapdpemtri.fireba seapp.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:48.273484945 CEST	192.168.2.3	8.8.8.8	0x5285	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:50.952675104 CEST	192.168.2.3	8.8.8.8	0x6e24	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:04.189244032 CEST	192.168.2.3	8.8.8.8	0xf645	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:04.788737059 CEST	192.168.2.3	8.8.8.8	0x190	Standard query (0)	account.live.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:05.369440079 CEST	192.168.2.3	8.8.8.8	0x3f7a	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:05.456235886 CEST	192.168.2.3	8.8.8.8	0xe388	Standard query (0)	acctcdn.msftauth.net	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:06.936080933 CEST	192.168.2.3	8.8.8.8	0x6ea0	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 10:56:42.114475012 CEST	8.8.8.8	192.168.2.3	0xd5f9	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:42.119982004 CEST	8.8.8.8	192.168.2.3	0x17fc	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:56:42.119982004 CEST	8.8.8.8	192.168.2.3	0x17fc	No error (0)	clients.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:42.146527052 CEST	8.8.8.8	192.168.2.3	0xbbb9	No error (0)	titko.wancdnapp.page		104.21.47.62	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:42.146527052 CEST	8.8.8.8	192.168.2.3	0xbbb9	No error (0)	titko.wancdnapp.page		172.67.145.59	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:43.609144926 CEST	8.8.8.8	192.168.2.3	0x44f2	No error (0)	manaapdpemtri.fireba seapp.com		151.101.1.195	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 10:56:43.609144926 CEST	8.8.8.8	192.168.2.3	0x44f2	No error (0)	manaapdpemtri.firebaseapp.com		151.101.65.195	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:43.921243906 CEST	8.8.8.8	192.168.2.3	0xd6e1	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:43.921243906 CEST	8.8.8.8	192.168.2.3	0xd6e1	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:43.921243906 CEST	8.8.8.8	192.168.2.3	0xd6e1	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:43.921243906 CEST	8.8.8.8	192.168.2.3	0xd6e1	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:43.921243906 CEST	8.8.8.8	192.168.2.3	0xd6e1	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:44.375262976 CEST	8.8.8.8	192.168.2.3	0x43fa	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:44.375262976 CEST	8.8.8.8	192.168.2.3	0x43fa	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:45.191451073 CEST	8.8.8.8	192.168.2.3	0x7f9a	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:56:45.191451073 CEST	8.8.8.8	192.168.2.3	0x7f9a	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:45.597732067 CEST	8.8.8.8	192.168.2.3	0xa58d	No error (0)	noem.urll.pw		104.21.72.95	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:45.597732067 CEST	8.8.8.8	192.168.2.3	0xa58d	No error (0)	noem.urll.pw		172.67.179.200	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:45.618743896 CEST	8.8.8.8	192.168.2.3	0x2c6a	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:56:45.916515112 CEST	8.8.8.8	192.168.2.3	0x3abd	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:56:46.824213028 CEST	8.8.8.8	192.168.2.3	0xe6e8	No error (0)	manaapdpemtri.firebaseapp.com		151.101.1.195	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:46.824213028 CEST	8.8.8.8	192.168.2.3	0xe6e8	No error (0)	manaapdpemtri.firebaseapp.com		151.101.65.195	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:48.335957050 CEST	8.8.8.8	192.168.2.3	0x5285	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:56:48.335957050 CEST	8.8.8.8	192.168.2.3	0x5285	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)
Jul 22, 2021 10:56:51.014240980 CEST	8.8.8.8	192.168.2.3	0x6e24	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:56:51.014240980 CEST	8.8.8.8	192.168.2.3	0x6e24	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:04.239505053 CEST	8.8.8.8	192.168.2.3	0xf645	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:04.239505053 CEST	8.8.8.8	192.168.2.3	0xf645	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:04.839123964 CEST	8.8.8.8	192.168.2.3	0x190	No error (0)	account.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:57:04.839123964 CEST	8.8.8.8	192.168.2.3	0x190	No error (0)	account.msa.msidentity.com	account.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:57:05.436543941 CEST	8.8.8.8	192.168.2.3	0x3f7a	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:57:05.436543941 CEST	8.8.8.8	192.168.2.3	0x3f7a	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 10:57:05.436543941 CEST	8.8.8.8	192.168.2.3	0x3f7a	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:05.517136097 CEST	8.8.8.8	192.168.2.3	0xae3c	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:57:05.517136097 CEST	8.8.8.8	192.168.2.3	0xae3c	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:05.524457932 CEST	8.8.8.8	192.168.2.3	0xe388	No error (0)	acctcdn.msftauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:57:05.524457932 CEST	8.8.8.8	192.168.2.3	0xe388	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:57:05.524457932 CEST	8.8.8.8	192.168.2.3	0xe388	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Jul 22, 2021 10:57:06.994554043 CEST	8.8.8.8	192.168.2.3	0x6ea0	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:57:06.994554043 CEST	8.8.8.8	192.168.2.3	0x6ea0	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:57:06.994554043 CEST	8.8.8.8	192.168.2.3	0x6ea0	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 10:56:47.002006054 CEST	151.101.1.195	443	192.168.2.3	49747	CN=firebaseapp.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Wed Oct 21 19:55:39 CEST 2020 Thu Jun 15 02:00:42 CEST 2017	Wed Oct 20 19:55:39 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 22, 2021 10:56:47.003556013 CEST	151.101.1.195	443	192.168.2.3	49748	CN=firebaseapp.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Wed Oct 21 19:55:39 CEST 2020 Thu Jun 15 02:00:42 CEST 2017	Wed Oct 20 19:55:39 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 22, 2021 10:56:51.098153114 CEST	152.199.23.72	443	192.168.2.3	49758	CN=aadcdn.msauthimages.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 02, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Microsoft Azure TLS Issuing CA 02, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 08 23:55:38 CEST 2021 Wed Jul 29 14:30:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013	Fri Jun 03 23:55:38 CEST 2022 Fri Jun 28 01:59:59 CEST 2024 Fri Jan 15 13:00:00 CET 2038	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Microsoft Azure TLS Issuing CA 02, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Fri Jan 15 13:00:00 CET 2038		
Jul 22, 2021 10:57:07.079384089 CEST	152.199.21.175	443	192.168.2.3	49804	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jun 06 01:52:36 CEST 2021 Wed Jul 29 14:30:00 CEST 2020	Wed Jun 01 01:52:36 CEST 2022 Fri Jun 28 01:59:59 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		
Jul 22, 2021 10:57:07.079554081 CEST	152.199.21.175	443	192.168.2.3	49805	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jun 06 01:52:36 CEST 2021 Wed Jul 29 14:30:00 CEST 2020	Wed Jun 01 01:52:36 CEST 2022 Fri Jun 28 01:59:59 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		
Jul 22, 2021 10:57:07.260319948 CEST	152.199.21.175	443	192.168.2.3	49806	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jun 06 01:52:36 CEST 2021 Wed Jul 29 14:30:00 CEST 2020	Wed Jun 01 01:52:36 CEST 2022 Fri Jun 28 01:59:59 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4088 Parent PID: 2308

General

Start time:	10:56:38
Start date:	22/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\#U00e2_#U00e2_Play _to _Listen.htm'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: chrome.exe PID: 5700 Parent PID: 4088

General

Start time:	10:56:40
Start date:	22/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1640,14482809985186982011,5593868377781062687,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Disassembly