ID: 345173
Sample Name: ID4380.htm
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 19:46:36
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report ID4380.htm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Signature Overview 4
Phishing: 5
Compliance: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 9
Private 9
General Information 9
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 45
General 45
Network Behavior 45
Network Port Distribution 45
TCP Packets 46
UDP Packets 47
DNS Queries 49
DNS Answers 50
Code Manipulations 50
Statistics 50
Behavior 50
System Behavior 51
Analysis Process: chrome.exe PID: 5216 Parent PID: 2052 51
General 51

File Activities 51
Registry Activities 51
Analysis Process: chrome.exe PID: 2168 Parent PID: 5216 51
General 51
File Activities 52
Disassembly 52

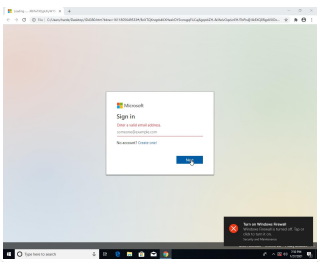
Analysis Report ID4380.htm

Overview

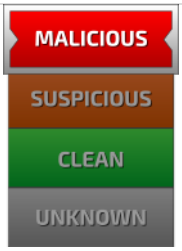
General Information

Sample Name:	ID4380.htm
Analysis ID:	345173
MD5:	09856d61b88443..
SHA1:	099c3616cfb85bf..
SHA256:	586258231081a1..

Most interesting Screenshot:



Detection



HTMLPhisher

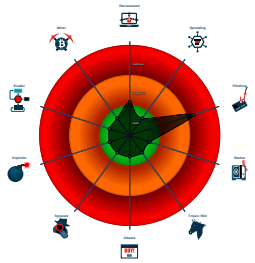
Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Yara detected HtmlPhish_35

IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5216 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\ID4380.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2168 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1504,3014448195932754039,17643246837121573947,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1900 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

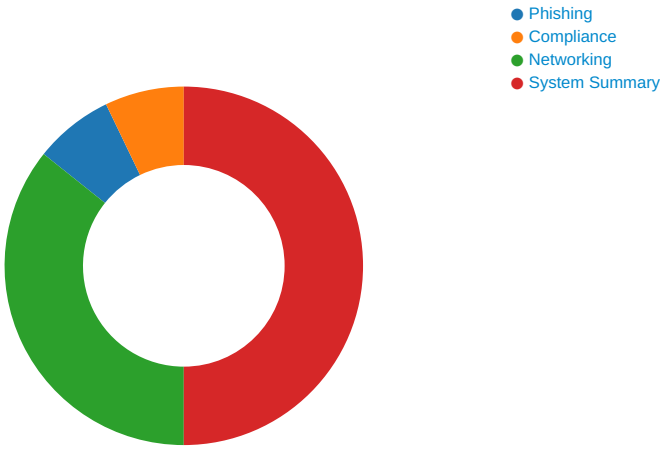
Initial Sample

Source	Rule	Description	Author	Strings
ID4380.htm	JoeSecurity_HtmlPhish_35	Yara detected HtmlPhish_35	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Yara detected HtmlPhish_35

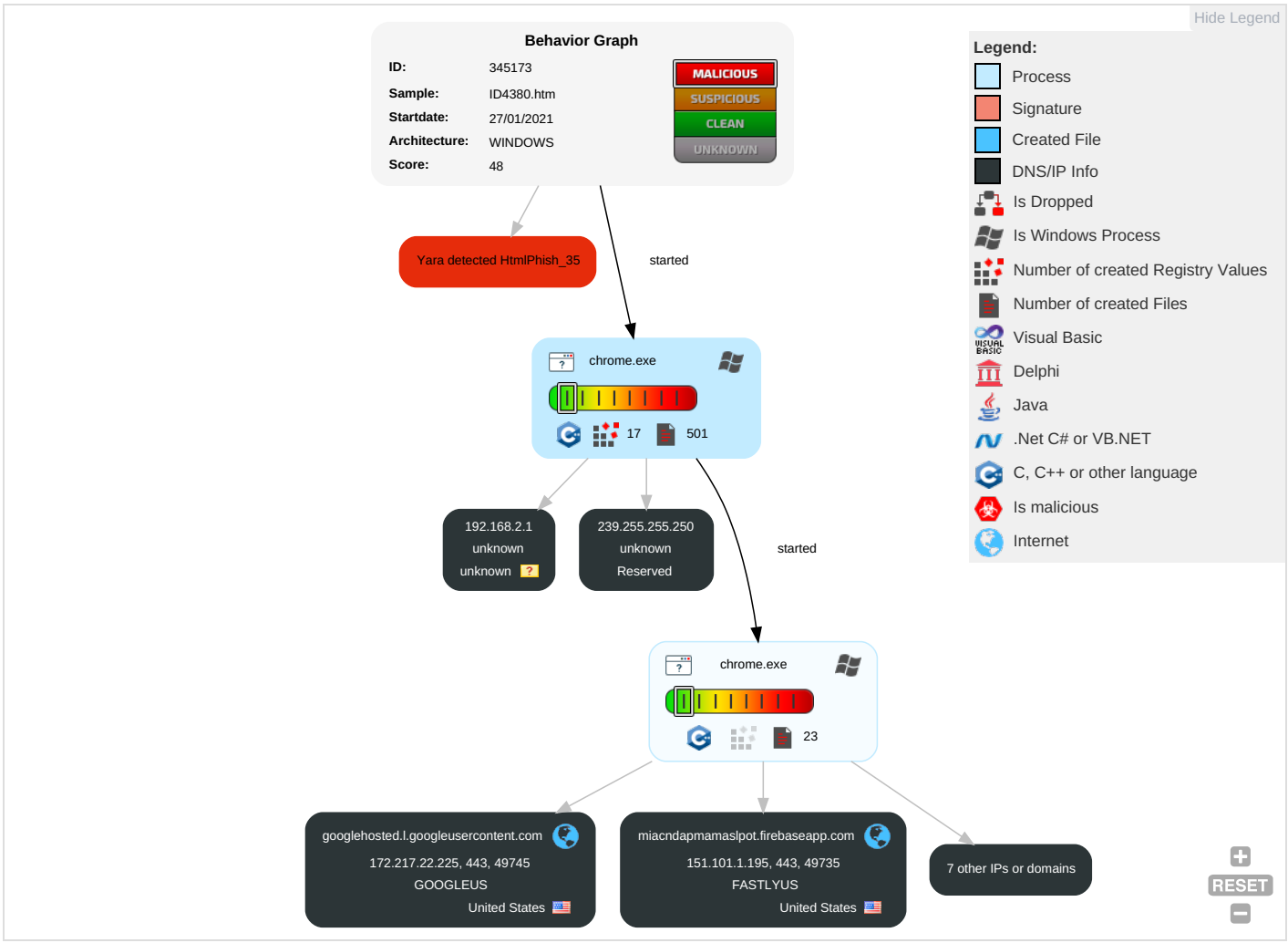
Compliance:

Creates a directory in C:\Program Files

Mitre Att&ck Matrix

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

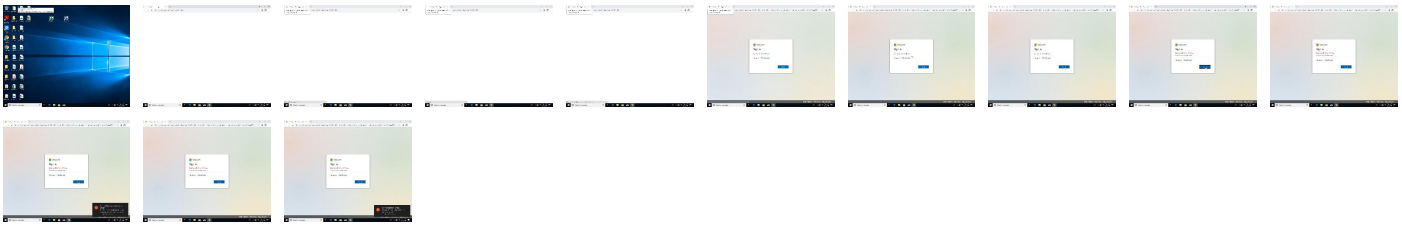
Behavior Graph

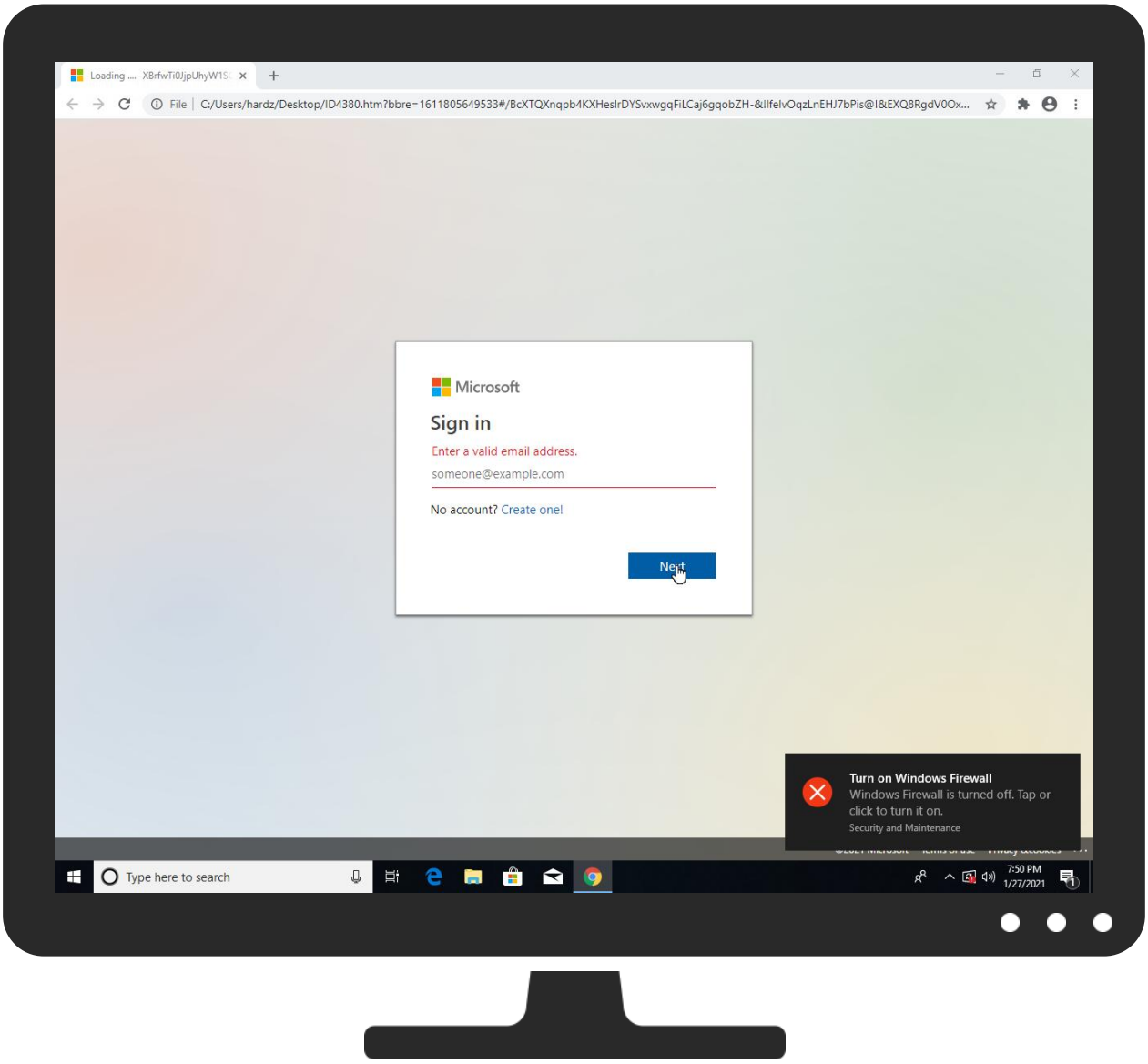


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ID4380.htm	4%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
miacndapmamaslpot.firebaseapp.com	0%	Virustotal		Browse
nodes.smsmail.net	0%	Virustotal		Browse
secure.aadcdn.microsoftonline-p.com	0%	Virustotal		Browse
aadcdn.msauth.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://miacndapmamaslpot.firebaseapp.com	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://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	0%	Avira URL Cloud	safe	
http://https://nodes.smsmail.net	0%	Avira URL Cloud	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

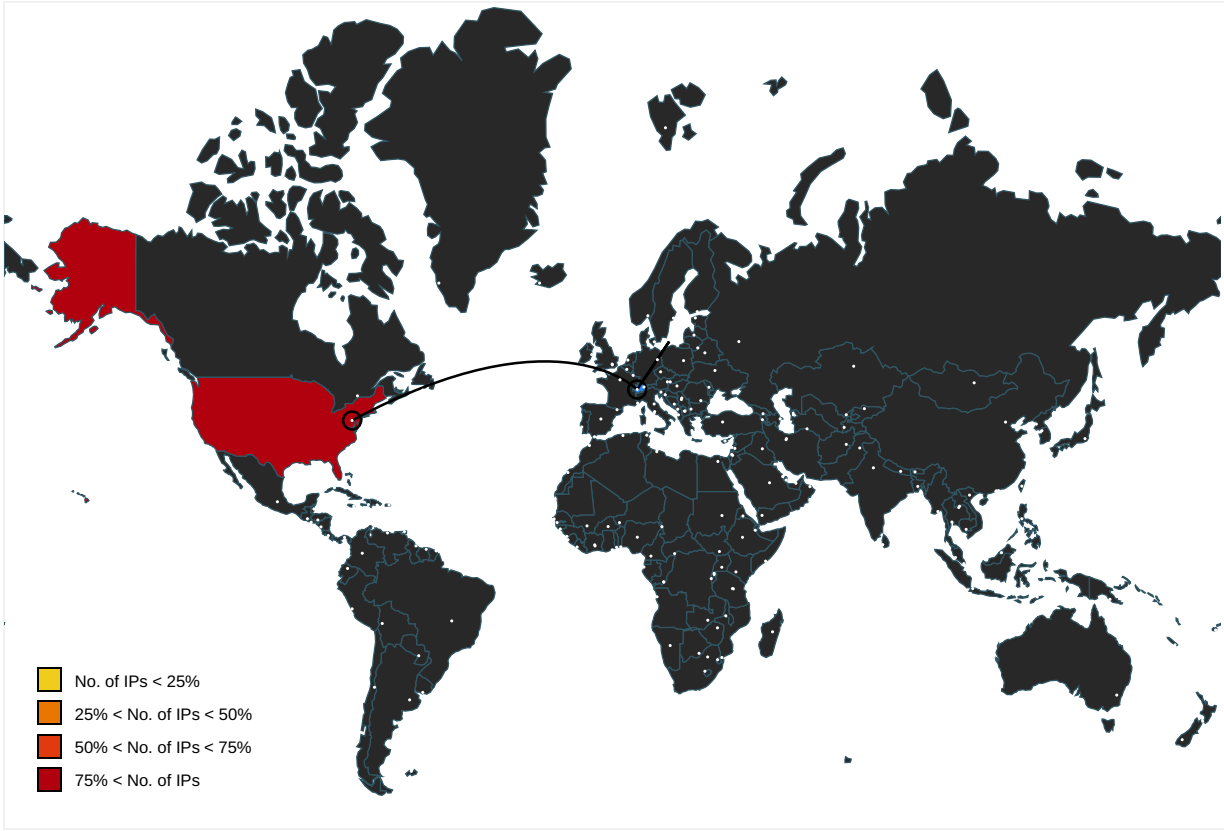
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
miacndapmamaslpot.firebaseapp.com	151.101.1.195	true	false	• 0%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.19.94	true	false		high
nodes.smsmail.net	104.21.19.54	true	false	• 0%, Virustotal, Browse	unknown
unpkg.com	104.16.126.175	true	false		high
googlehosted.l.googleusercontent.com	172.217.22.225	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
aadcdn.msauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://miacndapmamaslpot.firebaseapp.com	db7326a8-6520-4510-92f3-aa0b852234ac.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	db7326a8-6520-4510-92f3-aa0b852234ac.tmp.1.dr, 48dfa693-926f-4504-b052-779723bf4120.tmp.1.dr, 1d56be80-3d24-48ce-b8a7-529d0e360cc1.tmp.1.dr, 029fb286-178e-44a5-b977-daa51b47cc67.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://a.nel.cloudflare.com/report?s=VW8OgCrZ0cKxXrF0vWmxTVJRDMW6K9RyVSr15Qxoex8oWLVMtjBNfO%2FJgKXx	Reporting and NEL.1.dr	false		high
http://https://a.nel.cloudflare.com/report?s=1QkNzY75Rr39mhzYb9VWmcDkFOp8S3ILqnbYjQnL9%2BXjZbXU15guDtWTcXk%	Reporting and NEL.1.dr	false		high
http://https://cdnjs.cloudflare.com	db7326a8-6520-4510-92f3-aa0b852234ac.tmp.1.dr	false		high
http://https://clients2.googleusercontent.com	db7326a8-6520-4510-92f3-aa0b852234ac.tmp.1.dr, 1d56be80-3d24-48ce-b8a7-529d0e360cc1.tmp.1.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.6669.4/content/images/favicon_a.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://nodes.smsmail.net	db7326a8-6520-4510-92f3-aa0b852234ac.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msauth.net	db7326a8-6520-4510-92f3-aa0b852234ac.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://unpkg.com	db7326a8-6520-4510-92f3-aa0b852234ac.tmp.1.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.22.225	unknown	United States		15169	GOOGLEUS	false
151.101.1.195	unknown	United States		54113	FASTLYUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.21.19.54	unknown	United States		13335	CLOUDFLARENETUS	false
104.16.126.175	unknown	United States		13335	CLOUDFLARENETUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345173
Start date:	27.01.2021
Start time:	19:46:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ID4380.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.winHTM@39/233@7/8
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 172.217.20.237, 216.58.207.174, 172.217.23.78, 173.194.187.70, 173.194.187.106, 172.217.23.35, 216.58.207.170, 13.107.246.13, 104.108.36.62, 172.217.20.234, 172.217.23.10, 172.217.23.42, 172.217.22.202, 172.217.22.234, 216.58.207.138, 51.11.168.160, 23.210.248.85, 23.55.110.35, 23.55.110.38, 51.103.5.186, 95.101.22.134, 95.101.22.125, 172.217.23.67, 52.155.217.156, 74.125.13.198, 172.217.22.195, 173.194.151.103, 20.54.26.129, 51.104.139.180, 173.194.164.103, 173.194.182.198, 173.194.188.134 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, r1---sn-4g5e6nsk.gvt1.com, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, wns.notify.windows.com.akadns.net, clients2.google.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, r1.sn-h0jeln7l.gvt1.com, watson.telemetry.microsoft.com, www.gstatic.com, r1---sn-4g5e6ney.gvt1.com, au-bg-shim.trafficmanager.net, r1---sn-4g5ednsz.gvt1.com, fs.microsoft.com, r1---sn-4g5e6nss.gvt1.com, ajax.googleapis.com, aadcdnoriginwus2.azureedge.net, secure.aadcdn.microsoftonline-p.com.edgekey.net, r1---sn-h0jeln7l.gvt1.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, www.googleapis.com, ris.api.iris.microsoft.com, t-0003.t-msedge.net, r1---sn-4g5e6ne6.gvt1.com, blobcollector.events.data.trafficmanager.net, aadcdnoriginwus2.afd.azureedge.net, clients.l.google.com, r1.sn-4g5e6ney.gvt1.com, par02p.wns.notify.trafficmanager.net, au.download.windowsupdate.com.edgesuite.net, r1.sn-4g5ednsz.gvt1.com, r1.sn-4g5e6nss.gvt1.com, r5---sn-4g5e6nsr.gvt1.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, redirector.gvt1.com, emea1.notify.windows.com.akadns.net, r1.sn-4g5e6ne6.gvt1.com, e13761.dscg.akamaiedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, accounts.google.com, r1.sn-4g5e6nsk.gvt1.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, Edge-Prod-FRAr3.ctrl.t-0003.t-msedge.net, a767.dscg3.akamai.net, star-azureedge-prod.trafficmanager.net, r5.sn-4g5e6nsr.gvt1.com, vip2-par02p.wns.notify.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.217.22.225	http://examwriting.blogspot.com/2015/02/describe-person-your-best-friend.html	Get hash	malicious	Browse	• 1.bp.blogspot.com/-tW6bdJ2wjUE/U2FhguGfv0I/AAAAAAAAApY/eoNiqBbrlyI/s1600/essay.png
	http://www.boererate.com	Get hash	malicious	Browse	• 4.bp.blogspot.com/_QXfrrj8yn44/Siuczvogmnl/AAAAAAAABe8/d9uiCWfh0j8/w72-h72-p-k-no-nu/hare.jpg
151.101.1.195	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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	• auto7843878732875879294 7.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=G6fRyfWpf4em3a5PxYoprh6KPSSsHaeEr4x3W3Pvzp31VBrhmksxwaIwF2fZ05EyJsOCg==&rj9L_=qpnTHjlx
	http://Coronavirus.app	Get hash	malicious	Browse	• coronavirus.app/
	http://mime-iz10.web.app	Get hash	malicious	Browse	• mime-iz10.web.app/
	http://payroll-2e393.web.app	Get hash	malicious	Browse	• payroll-2e393.web.app/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
unpkg.com	INVOICES & STATEMENTS_02201.htm	Get hash	malicious	Browse	• 104.16.124.175
	T&S INVC#019.html	Get hash	malicious	Browse	• 104.16.125.175
	4892.htm	Get hash	malicious	Browse	• 104.16.124.175
	4892.htm	Get hash	malicious	Browse	• 104.16.123.175
	VANGUARD PAYMENT ADVICE.htm	Get hash	malicious	Browse	• 104.16.122.175

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PortionPac Chemical Corp..html	Get hash	malicious	Browse	• 104.16.122.175
	COMFAM INVOICE.htm	Get hash	malicious	Browse	• 104.16.125.175
	details.html	Get hash	malicious	Browse	• 104.16.126.175
	Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 104.16.125.175
	details.html	Get hash	malicious	Browse	• 104.16.126.175
	http://https://ddghbbf.r.af.d.sendibt2.com/tr/cl/AZ_fzMJRsE3xIeU_QcnTrJNmrQopncatDd-eovbR7xYq9ypiIqtwKWyrTIIdxNfdZBUhEo89L97BvoqW-m0AK8lpY_G1A0R4-OqWFWF7yqRk6lwWGjYQTbxdkNXIPZafVx__3xwAI7RkCXl8CJrNWoLoVVIyiYf1YWtibYMuXAbvq5KxrlLw-G3RcpVIiID2f-TlZx3vckcUFNx1IBpr5JamUxI3ckvzVYmWJV1yS8ZgSAUq_5FOmOxjsnNrYCXLNFt9Ew	Get hash	malicious	Browse	• 104.16.122.175
	http://login.technion.net	Get hash	malicious	Browse	• 104.16.124.175
	http://https://target-care.webflow.io/	Get hash	malicious	Browse	• 104.16.122.175
	http://https://numisconsult.com/blog/e47c4b8720db7445599988579a03c7c5	Get hash	malicious	Browse	• 104.16.123.175
	http://https://fultonmv.github.io/amanadpsoptodresi/aru.html?bbre=do9348wesid	Get hash	malicious	Browse	• 104.16.125.175
	http://https://rzh09.github.io/kirapzoxda/adiuew.html?bbre=as83wsdcx	Get hash	malicious	Browse	• 104.16.123.175
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fseacoccs.github.io%2fvivapdeltoozx%2fsorirw.html%3fbbre%3dod948reids&c=E,1,vSy_DaxVlhDKTU_DAd4XDQRKFbpEz58IBL3G2ibxtXxy4isfCn6tn5y2D7KvyG8o1RL3a--vpSQ8W1tCBVf3nGFmVP0O8Zl4kUultyRSb1120A,,&typo=1	Get hash	malicious	Browse	• 104.16.126.175
	http://41gq.com/7nosV	Get hash	malicious	Browse	• 104.16.125.175
	http://https://email.tungsten-network.com/K00kzKB00nv60AOP31Bq0G0	Get hash	malicious	Browse	• 104.16.124.175
	http://https://conrad805.github.io/vkiapdeijxzix/uead.html?bbre=ds94refszx	Get hash	malicious	Browse	• 104.16.123.175
cdnjs.cloudflare.com	#B30COPY.htm	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	Monday, January 25, 2021 222135-ATT+72308645308805 6636775.htm	Get hash	malicious	Browse	• 104.16.18.94
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 104.16.19.94
	Payment_[Ref 72630 - joe.blow].html	Get hash	malicious	Browse	• 104.16.19.94
	INVOICES & STATEMENTS_02201.htm	Get hash	malicious	Browse	• 104.16.19.94
	#U03bd#U03bf#U0456#U0441#U0435m#U0430#U0456l202154095982f#U0433#U03bfm+19792193827 19792193827.HTM	Get hash	malicious	Browse	• 104.16.18.94
	T&S INVC#019.html	Get hash	malicious	Browse	• 104.16.19.94
	4892.htm	Get hash	malicious	Browse	• 104.16.19.94
	4892.htm	Get hash	malicious	Browse	• 104.16.19.94
	20202237F.html	Get hash	malicious	Browse	• 104.16.18.94
	Release Pending messages on account.html	Get hash	malicious	Browse	• 104.16.19.94
	Payment Advice.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	Payment Advice.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	ESPP.docx	Get hash	malicious	Browse	• 104.16.19.94
	ESPP.docx	Get hash	malicious	Browse	• 104.16.18.94
googlehosted.l.googleusercontent.com	TT SWIFT COPY.exe	Get hash	malicious	Browse	• 172.217.22.225
	DHL-INVOICE RECEIPT.html	Get hash	malicious	Browse	• 172.217.22.225
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 172.217.22.225
	67654565677.htmL	Get hash	malicious	Browse	• 172.217.22.225
	STJYFHJWQA.dll	Get hash	malicious	Browse	• 172.217.23.1
	MPCAHXYTRX.dll	Get hash	malicious	Browse	• 172.217.23.1
	Cherokeebrick Progress billing(malware).html	Get hash	malicious	Browse	• 172.217.23.1
	fe89833d-6e0a-4916-929d-81ffbd4a244e_ORDER54#0.html	Get hash	malicious	Browse	• 172.217.23.1
	mfpVTSmyz-Fichero.msi	Get hash	malicious	Browse	• 172.217.23.1
	Maersk_BL Draft_copy_Shipping_documents.html	Get hash	malicious	Browse	• 172.217.23.1
	4892.htm	Get hash	malicious	Browse	• 172.217.22.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4892.htm	Get hash	malicious	Browse	• 142.250.180.161
	demo.js	Get hash	malicious	Browse	• 142.250.180.161
	demo.js	Get hash	malicious	Browse	• 142.250.180.161
	Release Pending messages on account.html	Get hash	malicious	Browse	• 142.250.180.161
	vefHXTlef-Fichero-ES.msi	Get hash	malicious	Browse	• 142.250.180.161
	kkToaAZ6Mm.exe	Get hash	malicious	Browse	• 216.58.215.225
	ACH PAYMENT REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 108.177.126.132
	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	• 108.177.126.132
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 108.177.126.132
miacndapmamaslpot.firebaseapp.com	4892.htm	Get hash	malicious	Browse	• 151.101.1.195
	4892.htm	Get hash	malicious	Browse	• 151.101.65.195
nodes.smsmail.net	4892.htm	Get hash	malicious	Browse	• 104.21.19.54
	4892.htm	Get hash	malicious	Browse	• 104.21.19.54

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Order_130577.doc	Get hash	malicious	Browse	• 104.21.19.200
	IMG-79108.doc	Get hash	malicious	Browse	• 172.67.188.154
	IMG-6661.doc	Get hash	malicious	Browse	• 104.21.19.200
	#B30COPY.htm	Get hash	malicious	Browse	• 104.16.19.94
	98.doc	Get hash	malicious	Browse	• 172.67.156.114
	DHL-INVOICE RECEIPT.html	Get hash	malicious	Browse	• 172.67.133.221
	Luminar4 (4.4).exe	Get hash	malicious	Browse	• 104.21.85.23
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	IMG-47901.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	Purchase Order.xlsx	Get hash	malicious	Browse	• 104.21.47.75
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 104.21.27.240
	SecuriteInfo.com.Generic.mg.d82abc4e3bc3179d.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 104.21.27.240
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.Heur.30497.xls	Get hash	malicious	Browse	• 172.67.198.109
	SecuriteInfo.com.Exploit.Siggen3.8790.14645.xls	Get hash	malicious	Browse	• 172.67.200.147
FASTLYUS	SecuriteInfo.com.ArtemisF00BCCFBF4BA.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.f4e794908d8d8093.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Artemis2EB570BBBAA8.dll	Get hash	malicious	Browse	• 151.101.1.44
	33ffr.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.ArtemisCAA9F750565C.dll	Get hash	malicious	Browse	• 151.101.1.44
	smf53wmr.zip.dll	Get hash	malicious	Browse	• 151.101.1.44
	xziu6ib2.zip.dll	Get hash	malicious	Browse	• 151.101.1.44
	cfsuggg.rar.dll	Get hash	malicious	Browse	• 151.101.1.44
	ci0v2ix.rar.dll	Get hash	malicious	Browse	• 151.101.1.44
	ioqjfxnm.dll	Get hash	malicious	Browse	• 151.101.1.44
	ij80czph.dll	Get hash	malicious	Browse	• 151.101.1.44
	ntd7zy47.dll	Get hash	malicious	Browse	• 151.101.1.44
	Quotation.exe	Get hash	malicious	Browse	• 151.101.0.133
	r4bf43.dll	Get hash	malicious	Browse	• 151.101.1.44
	ktyedjx6x.dll	Get hash	malicious	Browse	• 151.101.1.44
	xfagxh61l.dll	Get hash	malicious	Browse	• 151.101.1.44
	ep9n62vf.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.0f80eecd45dc9b78.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.aeca39dc4ac4ba79.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.faa94a7eb8be850d.dll	Get hash	malicious	Browse	• 151.101.1.44
GOOGLEUS	TT SWIFT COPY.exe	Get hash	malicious	Browse	• 172.217.22.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	qGQNEyWr7F.dll	Get hash	malicious	Browse	• 35.198.73.208
	s8mlt68JFA.exe	Get hash	malicious	Browse	• 35.198.73.208
	Order confirmation 64236000000025 26.01.2021.exe	Get hash	malicious	Browse	• 34.102.136.180
	Overdue_invoices.exe	Get hash	malicious	Browse	• 108.177.11 9.109
	DHL-INVOICE RECEIPT.html	Get hash	malicious	Browse	• 172.217.22.225
	SPECIFICATION REQUEST.exe	Get hash	malicious	Browse	• 34.102.136.180
	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	SIT-10295.exe	Get hash	malicious	Browse	• 108.177.11 9.109
	PAYMENT LIST .xlsx	Get hash	malicious	Browse	• 34.102.136.180
	wno5UOP8TJ.exe	Get hash	malicious	Browse	• 8.8.8.8
	quote20210126.exe.exe	Get hash	malicious	Browse	• 34.102.136.180
	org.mozilla.firefox_2015785883.apk	Get hash	malicious	Browse	• 172.217.20.238
	org.mozilla.firefox_2015785883.apk	Get hash	malicious	Browse	• 172.217.23.14
	SecuriteInfo.com.Trojan.Packed2.42783.14936.exe	Get hash	malicious	Browse	• 34.102.136.180
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	4NoiNHCNoU.exe	Get hash	malicious	Browse	• 216.58.207.179
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• 34.102.136.180
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• 34.102.136.180
	eEXZHxdxFE.exe	Get hash	malicious	Browse	• 35.228.108.144
CLOUDFLARENETUS	Order_130577.doc	Get hash	malicious	Browse	• 104.21.19.200
	IMG-79108.doc	Get hash	malicious	Browse	• 172.67.188.154
	IMG-6661.doc	Get hash	malicious	Browse	• 104.21.19.200
	#B30COPY.htm	Get hash	malicious	Browse	• 104.16.19.94
	98.doc	Get hash	malicious	Browse	• 172.67.156.114
	DHL-INVOICE RECEIPT.html	Get hash	malicious	Browse	• 172.67.133.221
	Luminar4 (4.4).exe	Get hash	malicious	Browse	• 104.21.85.23
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	IMG-47901.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	Purchase Order.xlsx	Get hash	malicious	Browse	• 104.21.47.75
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 104.21.27.240
	SecuriteInfo.com.Generic.mg.d82abc4e3bc3179d.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 104.21.27.240
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.Heur.30497.xls	Get hash	malicious	Browse	• 172.67.198.109
	SecuriteInfo.com.Exploit.Siggen3.8790.14645.xls	Get hash	malicious	Browse	• 172.67.200.147

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\39631c89-e300-4172-9fca-99cd5c36456a.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):	155189
Entropy (8bit):	6.0522475432252065
Encrypted:	false
SSDEEP:	3072:x8kRDb0lSBYPycFIs4+w6EoFcbXafIB0u1GOJmA3iuRX:x8l0lS8Gs7tvaqfIlUOoSiuRX
MD5:	184EC87B087D31CB093B3936026D5CC2
SHA1:	3CD27F8AC1DF9668DDA3D460789EFA8898149526
SHA-256:	E4FE0508F565633C70FDD5A0EBFEE7152162AB79A53BBCF7E004F2152B9BD961
SHA-512:	6C378C19D84AA31F0590160DA7F24004159C6988A8D045DE1811E55583D921786C21E1FEF7EBAACFE2A7622C3AF0A1EF2953634415F39D529720D7B84C79011E
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":1.611805651225903e+12,"network":1.611773252e+12,"ticks":101240739.0,"uncertainty":4481293.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016289563"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5a273428-5000-4eb9-9839-983b61482ec4.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):	155085
Entropy (8bit):	6.051930170265883
Encrypted:	false
SSDEEP:	3072:J8kRDb0lSBYPycFIs4+w6EoFcbXafIB0u1GOJmA3iuRX:J8l0lS8Gs7tvaqfIlUOoSiuRX
MD5:	CC2D7DB3D2C65B203D7543F21FB3FE92
SHA1:	83223250708663997612F953EBEBE412801F4D27
SHA-256:	119FA678D3DB521A7B8032F4C64F9795E5D99BF2AD2122C8FA15878CA5A0F4F0
SHA-512:	DB755B5737971B019CBF388F7E94D3481FBBC6BDA7AB279D4C6EB0ECF776F83BDBE316C62EEAFFC5D6DB14E5225E35486EF7C10873A705533C13043762C49C3
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":1.611805651225903e+12,"network":1.611773252e+12,"ticks":101240739.0,"uncertainty":4481293.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016289563"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\654976bb-0b13-49c8-8ce8-22acc61ab2af.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.752120516279205
Encrypted:	false
SSDEEP:	384:df6pNTMijs/fVIu10N9rOvBL3CVn+Hv2GeBrMvVNxy/TvCrwdmIDsLlFVCOT7FNy:9uu5VeTKC8enNvfofrKDKtjpFi
MD5:	5A85195DC203BED732055B3E04210567

C:\Users\user\AppData\Local\Google\Chrome\User Data\654976bb-0b13-49c8-8ce8-22acc61ab2af.tmp	
SHA1:	0BAA766D73C2F8868B587634F2462770B7D7A7CA
SHA-256:	4F0D4076C92D4A7DB006F3E0A085EF8D2DA2835A35E8457EA994369DD6ABBBDA
SHA-512:	2008C96732DE66B1902CD81AC06F21F877C1754879F0FFBDB7034F3B81F6A5DE4682E1961E5EBA4AD60366AD3AB65B007DFF80B0D763F25A9FCD0838AB82969
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..../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\7b2fc8c6-94e7-44bf-81cf-ec1140a62cdb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.751532520194543
Encrypted:	false
SSDEEP:	384:zf6pNTMif/o10N9rOvBL3CVn+Hv2GeBrMvVNxy/TvCrwdmIDsLlFVCOT7FNw19UG:Su5VeTKC8enNvfofrKDKtjpFO
MD5:	F0E2872A1210AB836CCA79A1ACB453B0
SHA1:	A5709D630A53856F5CF9F2898DDB187E3D35C79E
SHA-256:	6FEB5F0F0F1549E8D6F160D966F02FF6377B2EE57DCD5D119FF26793546765C8
SHA-512:	223109334F0C419AF466C284BEA6D133E9F04D34F1DE4EED71E08463D335F27C49D829BBAC52B1952D32A524A3C9D3751CC3748DA8D1A4BB0C9AD3FD2C32FE 3
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n..../8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\9ebdce66-0fd6-47a7-a049-dd21ece1ba90.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):	154991
Entropy (8bit):	6.05164018001793
Encrypted:	false
SSDEEP:	3072:t8kRDb0lSBYPycFls4+w6EoFcbXafIB0u1GOJmA3iuRX:t8l0lS8Gs7tvaqfllUOoSiuRX
MD5:	6DCE7E034DA85B315118E436E2A1ECFC
SHA1:	79EA00CDDE6413EDE279DC7451D20F5FC09668F9
SHA-256:	3B9B8C644D8BBF5F9EF8B2132395E8DF286A972AA2144B5FE448E77F038F9DC7
SHA-512:	3A0BCECDF9CD75C7F8AA5E7FA27963FB59681CFAC831D6600A19A9393961B08D0EDF147AFE6B8FD0E8B0295F5987F22B7059845DDA34DABE7DAB93C561C673 3D
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.611805651225903e+12,"network":1.611773252e+12,"ticks":101240739.0,"uncertainty":4481293.0}},"os_crypt":{"encrypted_key":"RF BBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppN r2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS 1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_man ager":{"os_password_blank":true,"os_password_last_changed":"13245951016289563"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1d56be80-3d24-48ce-b8a7-529d0e360cc1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1da3ac15-65e2-44bc-aae7-24037d7b5877.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):	5.572387852829112
Encrypted:	false
SSDEEP:	48:YLVwU9V6UUhWUo8UoFmseKUewqPeUer2UefMwU9oNwU9ojxUenw:/U98UUoUo8UoU3KUGPeU9UExU9ouU9oE
MD5:	3043C7597EA8DF3E1E9FE4D489A8B600
SHA1:	EB680FE0573A52859CF4570AC4D701E5BFAFA62F
SHA-256:	B1E98F4D0D8D31E6A51E04EBD0E5B3BC8CCF6BE49456E87A61CBD6C6D64E87E4
SHA-512:	C1FD787031D6AF48D9691EF398E7B0D51FD38576838A3980CB325D5FE7EC6B06E8E401087AC6274F915F2323681B772BE5B399FD3E135FA7C56A07FAFC6DF340
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1627585654.712309,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1611805654.712314},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1643341656.719342,"host":"VPmzqbDVkuO8opw7k4VAqApbEStXPXE3j5vzfoygodw=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611805656.719348},{"expiry":1643341654.572801,"host":"e3SziuwfuO2UvuBno+qkR1ObHAzZmSUoJhrc7dbP1Uo=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1611805654.572806},{"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\23e3e224-aac1-411a-98e4-062616380648.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):	22614
Entropy (8bit):	5.535699763500133
Encrypted:	false
SSDEEP:	384:Z2UtgLleYXC1kXqKf/pUZNCgVLH2HfD+rUfHGwnTBaGdS4U:8LltC1kXqKf/pUZNCgVLH2HfKrUPGwnC
MD5:	23D56798931513C669D2C79156C4D257
SHA1:	CCCD5A67FD2F10A304B3E82DC5029EF67E2C2B60
SHA-256:	D3397C9D2B95AAE95C57EE31058A04CBF99440779EC1A4126DF1888DA2F12DB9
SHA-512:	F6A2C11F3B98BFF0F0615DB8484555F369CB31F4DF4434228573905010219284C5EDDA819305D55BB4F0517971CEE3EDA1A047CBF4E22D2AB6F5CF3FFE628B90
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\23e3e224-aac1-411a-98e4-062616380648.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":"13256279248309102","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\3fc6bb5f-53fc-4553-8414-f818f7e4cbe1.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):	19198
Entropy (8bit):	5.570510285178726
Encrypted:	false
SSDEEP:	384:Z2UtRLleYXC1kXqKf/pUZNCgVLH2HfD+rUrHGtaxqdS4E:lLltC1kXqKf/pUZNCgVLH2HfKrU7GAqU
MD5:	49AEBD8A900CF16886760A7EE04D4542
SHA1:	17A418CCCBFE1C19C59432D702C699129DBFF635
SHA-256:	720AD24C2DA273A63478D2E3A14C229259917707FFEAD4043A020636AA5F0991
SHA-512:	2B79BF28EE0F24D26B2D67025C771182E202F71EA34094B46F827023EFD823900418B4A04627BEE198F3A65E45B87CB88CD18963E6DF58554B0476F2FD66FDAB
Malicious:	false
Reputation:	low

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":"13256279248309102","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\5ca3884b-2278-47dc-be3d-fa8694aa3871.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):	4772
Entropy (8bit):	4.9488720220427584
Encrypted:	false
SSDEEP:	48:Yc80UkPklwHjKyUcPqAZRqTlYqlQuoTw0ptGMH3CH3G/s8C1Nfct/9BhUJo3Khmx:nDRFSu4pcVUSok0JCKL8VbOTQVuwn
MD5:	65730F5BF8409ACC901824D3E9BB9362
SHA1:	B4239DD02F5094612493FC07AEB16357F0E020D6
SHA-256:	1CDE75B21FD920E0EB6440F5F54618835DF761200594592DC45AC22BA18C5A35
SHA-512:	52383F066C8CF62A8FD0C494DA4A6AE43C9E27B63A900E73522ACEB884F523A1EB856F7B1E6415F90424CF1D4F0F43933442054B0A43AB9FE110AEAFB1799DD
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13256279248522241","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_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",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5df007a5-d406-4c2c-b2f2-68f0233a09b5.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):	5368
Entropy (8bit):	5.16624226920749
Encrypted:	false
SSDEEP:	48:Yc80UkPklwHjKyUctqAZRqh4HheN4lYqlQuoTw0ptGMH3CH3G/s8C1Nfct/9BhUy:nDRFcu4hohBcVUSok0JCKL8VbOTQVuwn
MD5:	6D60C6EEC8FB742702B0DD6A60FDF0D3
SHA1:	C2B07E370D4C13CF9195843CE113DEFB85320151
SHA-256:	7062E4DC8EB42DB5A977F090AD89E9D69475EB5DE1CE761FA5CEA3696C2095FE
SHA-512:	1A436E5104ACBDB612B77112B66A66E9326FA508D4D20649A630B592E9DBDE5714CAB08E9228618E33E23322522F5C4D74F7E6F671B9A6530F22C7880DFF129F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5df007a5-d406-4c2c-b2f2-68f0233a09b5.tmp

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13256279248522241","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","7355378"],"daily_received_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",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\853d3cb3-1a1a-40fe-a253-b33822e79c4c.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):	5368
Entropy (8bit):	5.16624226920749
Encrypted:	false
SSDEEP:	48:Yc80UkPklwHjKyUctqAZRqh4HheN4lYqlQuoTw0ptGMH3CH3G/s8C1Nfct/9BhUy:nDRFcu4hohBcVUSok0JCKL8VbOTQVuwn
MD5:	6D60C6EEC8FB742702B0DD6A60FDF0D3
SHA1:	C2B07E370D4C13CF9195843CE113DEFB85320151
SHA-256:	7062E4DC8EB42DB5A977F090AD89E9D69475EB5DE1CE761FA5CEA3696C2095FE
SHA-512:	1A436E5104ACBDB612B77112B66A66E9326FA508D4D20649A630B592E9DBDE5714CAB08E9228618E33E23322522F5C4D74F7E6F671B9A6530F22C7880DFF129F
Malicious:	false

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13256279248522241","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","7355378"],"daily_received_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",

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):	5.252369200000472
Encrypted:	false
SSDEEP:	6:mPXM+q2PWXp+N23iKKdK9RXXTZIFUtpe7ZmwPeXLiMVkwOWXp+N23iKKdK9RXX5d:5+va5Kk7XT2FUtp6/PKvV5f5Kk7XVJ
MD5:	03C980C468386A09700CC48365599E03
SHA1:	E7E661C8D161EBAD8A3BBDD6140DC63406D83C4E
SHA-256:	07B50B800AA23F9FD5CB9F16A0B0EE3EBD276160723CDFDAEC0C6DA9B895B080
SHA-512:	7351CCA10A2877F54F8F2FA91CC46F0AC3B9EB577DD4934F426CA05B667FCD2CC570446AE26594DE835AA744A9A604D5C647B7E81C15CA141FEC91411E3F03
Malicious:	false
Preview:	2021/01/27-19:47:36.949 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/01/27-19:47:36.979 1aac Recovering log #3.2021/01/27-19:47:36.980 1aac 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):	5.246655355667976
Encrypted:	false
SSDEEP:	6:mPZM+q2PWXp+N23iKKdKyDZIFUtpe3zZmwPeDMVkwOWXp+N23iKKdKyJLJ:b+va5Kk02FUtpu/PVV5f5KkWJ
MD5:	1049948300C8C6BCAAE828AA7C955F08
SHA1:	FBA49E6B37FF0E2CE62394E98D4F1822B39B6377
SHA-256:	9AD48D92847C7E214F9B09FB56AAE7D788F61D1D941FF88EB6A73F042AFDC5D3
SHA-512:	049DB0C5C46B84857116D12935BA5E3B3FA20063CDBAB4B722FD4B6894CC672C1B35141037162045C8AA13DBD7DB28B549A5410CDD79141F886AED991479188
Malicious:	false
Preview:	2021/01/27-19:47:36.943 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/01/27-19:47:36.944 1aac Recovering log #3.2021/01/27-19:47:36.945 1aac Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	8192

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Entropy (8bit):	1.3510310734779263
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwI6xgAZOZD/i:TekLLOpEO5J/Kn7UL6xNOZi
MD5:	195F9F540391B8CC93843149F6FE7433
SHA1:	E2A336DAD81A8F26D70FF6EE981DA959CE64D90F
SHA-256:	AFD157966E74B364A73C9CF2D5F5C3057C6788C66F68FAD736F7E527A4C0CB29
SHA-512:	94FCE3F87E3DB0C6DBCFA9D18DEDF36F2E362933EF1360FAD8639378CF2E8B2DD2ACAA2BCE549E0EA7C0D795EB44F354396DB389CACF60D267F5D31FE4324 3EA
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):	8732
Entropy (8bit):	1.3123720868542095
Encrypted:	false
SSDEEP:	24:YcLgAZOZD/cqLbJLbXaFpEO5bNmISHn06Uw8t9:Y8NOZcq5LLOpEO5J/Kn7Uvt9
MD5:	A778D4BE99AB22EC8938788E562AFFDD
SHA1:	48E15EA971E20E09031BFCA0482FF1020714B6EF
SHA-256:	FFCA359D505226A407B9BA76605CEEEEF88800C98FBE944C762C0A2EF6CDCE3D
SHA-512:	1825CE09067FB59925388F9A7BD9AC2BAA5664C0EEA42F90E973975E082B4020624279EF31D84F611A1DA0DB9232E769F35CF4B732A3B9FBC42C4151D05BAB04
Malicious:	false
Preview:	.....f..... ....

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):	3593
Entropy (8bit):	4.133162778911566
Encrypted:	false
SSDEEP:	48:343x017jXE4MTyD+8QJRB7H7Um8lWU3glLt+cq54FUO897zAvE+L:34f9WD+8QJs932p+z4idq8O
MD5:	AC8AB16CD76A022BF5330BBC3864C60C
SHA1:	51E17D3F9698B56228884CC5F68302B5C4206816
SHA-256:	6BF1CCBD71C78E4CE9263151D0E8B5E9551D05678BC6971ACD591B7EB24EE3AE
SHA-512:	9C6E32FC1D2542317D75183302798C69D545382DA30F294F49DB3EEFA480543C44E6D7C2F7E6C91F95A5E57B2673B24C9ED0BBAE071FF45202D17C201A4A063I
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...5a8c47a5_a981_4fb5_84a5_1f8f45764bdc.....bW..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....=..8.....<...file:///C:/Users/user/Desktop/ID4380.htm?bbre =1611805649533....D...@.....8.....h.....`.....P.....X.....P.....R./....S./.....<...f.i.l.e.:././.C.:./.U.s.e.r.s./.h.a. r.d.z./.D.e.s.k.t.o.p./.I.D.4.3.8.0...h.t.m.?.b.b.r.e.=.1.6.1.1.8.0.5.6.4.9.5.3.3.....Z...)...f.i.l.e.:././.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.e.s.k.t.o.p./.I.D.4.3.8.0...h.t.m..... .....8.....0.....8..... .....file:

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.258063754615692
Encrypted:	false
SSDEEP:	6:mP/ItVzlL+q2PWXp+N23iKKdK8aPrqIFUtpe/hW1KWZmwPe/hWjLVkwOWXp+N23Q:CYVR+va5KkL3FUtpyhW1KW/PyhW3V5fA
MD5:	2BEEEFBAD6C0F8B464057FAA62FD1D65
SHA1:	BB161E500097F149C5C32333A425B9A323F3FFFA
SHA-256:	A4350B8FA4F28267206161F3506125CE3D0719A16449A420DF484BBC57C8FBDD
SHA-512:	4B57D5AF0131DA616AE95A4678DC885E396606144A18B0DCC7DEAB8937174006B1BDBB820F8BB1920833EEC7826CAB0AE071D42222384DBB8EF4A9437A70D54 8
Malicious:	false
Preview:	2021/01/27-19:47:28.529 103c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/01/27-1 9:47:28.530 103c Recovering log #3.2021/01/27-19:47:28.530 103c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4 C
Malicious:	false
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....f.5.....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):	320
Entropy (8bit):	5.275587289121638
Encrypted:	false
SSDEEP:	6:mPrVlL+q2PWXp+N23iKKdK8NIFUtpeaKWZmwPeMLVkwOWXp+N23iKKdK8+eLJ:UVN+va5KkpFUtpfKW/PhV5f5KkqJ
MD5:	031053516E8EB982F99E8DFA9F0436EA
SHA1:	1D8D6DD170262AAC03B601F5B99190B4F3D3F215
SHA-256:	ECDEA3D08A01EC45175855109A6723CB6B2DDB021E0D3A9A8846B5EA145CD521
SHA-512:	A17EA69A42E4B7A7D0C684200FE1FD1020E2EACC4658DB6708041ACBD563E8118AE647975CFFD0EF954A222DD968137E664172F641F7BF9F095F9A83D525576(
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Preview:	2021/01/27-19:47:30.684 103c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/01/27-19:47:30.685 103c Recovering log #3.2021/01/27-19:47:30.685 103c 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\1.0.0.5_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):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49C
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2l/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.5_2_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):	17938
Entropy (8bit):	6.061511031838911
Encrypted:	false
SSDEEP:	384:ahlZ97TC4hNLFkQF/4H/vo3c93yaM5ZAVGnLMeP3rrBsuzfccHyfXRH0MVEPT:ahlvS2Fk5ooNM5Zg+YePRgpXRHLVA
MD5:	58E0F46E53B12F255C9DCFD2FC198362
SHA1:	24E3904DED013ED70FFC033CFA4855FBB6C41C19
SHA-256:	F82EEF4F80D86F5DEF0F40F91FFB6453E1706CA5FD8A7172EDB19C4B17E2F330
SHA-512:	1AC83CDFF124E4C0281FBBFC0A919AA177F1524AB85434D82E5A87DDDF7CAC26A761C5E6249566626054C62D6B0F46A51AAC1F6E64C260F50832AE1D5F0A49C
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["vyABSKu1ssLnoQtj8Nqw6CjEthL33alh0QYBLzRg9+E=","DGWrOFQ2mF53Fk3FM5jLCV5sKg1DgRTF750mXhpKaoM=","f8vmSL13lL5/sEk/UBo2z9BTE1au+kMnftvxebWlLfQ=","g6BagkGM3fYVfhX6pe9v+WIhrxb6KJyr1H8KEdf3iQc=","6GdjKPovCi9TAL74Kj/R6GzGC1RVsWCb0lMtrG41ElU=","vttVT0ok78296FZBpoJgEIMmZmATBpKLrC5wr6RiPIg=","5dwwmOMAg6GXh2x6hn99MsZgiXJCxgTnwFdiMmcl2/0=","lQFxytI8i5cYLqNLbSnc45XXd/jEIuKwO1nAvNh5/WE=","qETF6aAOXwVcduPggf/FGrY8l2ALwdIswKxFJWG2JpQ=","+fjs95t/ESSgtcK9SzZOIcY/aemUr2l/yYI07esfjbk=","H+r4m51qI4G0z8YtAibc3/AGYvPK9qT14BbGvmM4/y4=","Qz4vtomAqVrAeKIcJ/zbVi5yDpFiY+F7tP/FTdoAKwU=","k110zqa69JMO5T4RH/nBdkCVX9I/98Gd7K2dnRuyFyg=","+QrRx4Pz8wbz4ef9ch1Q2aAQDZbv0r64NMyj9z0qaaE=","6q/tcYekY7TN66ZdPx4ALLcteRLQJqFy0wgcIqL6fFU=","djipPPtOAFsToDpKDbadLJLGQiCzTkN2qsRbzvKijBo=","uHEm1DVxHADroGNWHjmdfpdNUgtHXDQ0zfTmdqtJgYo=","1C2E0Gz2nqKFG3ghcQEVyiTYI4rTYNnrpsHQY9J7BfI=","swYZ8T85/4tzx26dfC0RKxMiHwnjqJoxtn0Mb8NdcjI=","AuXwavx8SOtkgFhnRlnM4rolw243Ryh2ktL0QZRDLoE=","oG0S5XUkjBtAHts9X+uQt5MTsf

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.807609660559822
Encrypted:	false
SSDEEP:	48:yBmw6fUbyD+8S8slxtjI90R4mG7yD+8LLmslXd:yBCfD+8S8slj090xD+8L6slXd
MD5:	021E61BDBFFF21B927C1A86A79BA71EE
SHA1:	F0B4BC0FBCEE378D90C83BC767BB3DA485A127D7
SHA-256:	5AC0B54586D3C89DD89660335D078D58BF5DBCB0D9DFBBB25F367E3A6D7B65FC
SHA-512:	9D920266456E167A10EBC47B4B319DA4BBA1C0A0FA7BAE2B06B48D3B58E6F65C1B68D6892C1C49DD7CF886EEC065D9849BCE79655BFAE64E7AB96156DC4F9 35
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7774498587493992
Encrypted:	false
SSDEEP:	24:+cce5u7BoU2yLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwY3n:KjadBmw6fU/3n
MD5:	EB16046BEBB487F986B530B205855A5D
SHA1:	3E71DF2E4810BE06A7B73EF657AAD89D750280B4
SHA-256:	438DF9BE5BFABCCD249D646A48FEE771FB70E82D40BC53F680643D94DB27B430
SHA-512:	4148F960D574045CC7E469D15743BC5D65C2B3EA8390E2FA40DBDC56E784BE5DCFE130C550AFB200079BDBFA4CA40C8A93A59D293100D0EE08A35DD7F6C24 4
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.273538577922803
Encrypted:	false
SSDEEP:	6:mPAF4M+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpe5FU0XZmwPehMVkwOWXp+N23ib:fj+va5KkTXfchI3FUtpmFU0X/PjV5f5G
MD5:	69DA7DF2980D6EDA961A7510CD8F43BC
SHA1:	E4B54AB23343CBF6B70E410CE9AC50A884F62C2A
SHA-256:	CDF4F85D030A390A902D683CC96DDDFA30376AE7DF9818C6D42FD92F0678C415
SHA-512:	CE81FDDDCC3E5624BAC6C9A670F87B30A1B0E58BF4746A83708ADB47768885F8D47A1CC2CC6270CD44DF3A9838659EFE87A42C58BF0EEB331A41C91664FB4E2
Malicious:	false
Preview:	2021/01/27-19:47:36.891 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/01/27-19:47:36.906 1aac Recovering log #3.2021/01/27-19:47:36.907 1aac 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):	5.254111404349072
Encrypted:	false
SSDEEP:	6:mPBM+q2PWXp+N23iKKdK25+XuoIFUtpeQQZmwPeFiMVkwOWXp+N23iKKdK25+Xu6:v+va5KkTXYFUtpLQ/PAV5f5KkTXHJ
MD5:	AF7B422872252CDF9437BBAFCBC4A995
SHA1:	064C7FE6A7D4C220D2D719C446D4BDD6A1FFB525
SHA-256:	BC1ACB14B820DDC79C62C80071BB17867EEE0FD4DC47463C7CB04ED4E88ABE6E
SHA-512:	7C9DA6097D39B81745C7B5B66507B557E50A47D624A276F2F8457917894A0F51BE800741D34D84BFFBF2015032F42789351F3C1A81E95837D356A9919EDDFADC
Malicious:	false
Preview:	2021/01/27-19:47:36.828 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/01/27-19:47:36.829 1aac Recovering log #3.2021/01/27-19:47:36.869 1aac 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):	5.261838232317268
Encrypted:	false
SSDEEP:	6:mPdM+q2PWXp+N23iKKdKWT5g1IdqIFUtpeKXZmwPe3UTMVkwOWXp+N23iKKdKWTk:D+va5Kkg5gSRFUtpL/PaUAV5f5Kkg5gZ
MD5:	638A82EDA9C34ADC1253045150347243
SHA1:	177022A4D5307B955B205008E4BB5E10AB7F7247
SHA-256:	F055AB86F73D26D611E13C6B55070F8F29D47C283A2AC3C25BBB47135EBE085D
SHA-512:	859DCD1129BDA50A7D7AED3FB81F5D910D3676513BFEE839ACE2EFD779B4A5A92DF4D77D6DEA45595D5B46A784938A33580858AF0E080DDB0CCD08AC6AE0A7BA
Malicious:	false
Preview:	2021/01/27-19:47:36.060 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/01/27-19:47:36.068 1aac Recovering log #3.2021/01/27-19:47:36.069 1aac Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8Efl9hol:8gOl
MD5:	F6203802DED2C9702E5F51A1B69DFF01
SHA1:	FFB1550B64F6AAE36B72A5B894E1CC8B9245AF40
SHA-256:	5B0EDE7CFF7B306C4DA5D22858D6367BB431AFF664338E8626C31E752A604A0C
SHA-512:	DE14F68316701E26B4F89FE87D65FB61C2A5B1D53AF893C783ABFF1E474B63D378320A83DD8B2A2594846A3A6AA8B8E89940603768C19BDF7F337792DFDBE712
Malicious:	false

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.6203292570305754
Encrypted:	false
SSDEEP:	24:TLxxZfyyDTdNnC8HALGWRFjbDhZfmbDAJuZDblZf4bll0BBpRlNyhftZfyyDTdNp:TUyD+8yDcDCgieIBpRGkyD+8LLD
MD5:	3532FD34E7F1A15B078B9B82C1CDA38B
SHA1:	5A13F3940A420EBE7191231F47EBF65404E299FD
SHA-256:	ED6081D2AAE4D1C70DBAA856D393D2A11A940754DF4FA8CB9ED5767286D101C4
SHA-512:	D6606C563625EA99BD730E5539F131D414A18D1495F50EE9EBC7A4AC5BDA2D64D0B1FEA511940F8E18686287652D2DDD56DDF0FCD93C36AB024E53FF561908/ 2
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1223
Entropy (8bit):	5.881468239221713
Encrypted:	false
SSDEEP:	24:YkBna8sRGQE3frrm2irA6s6l6/sgz+2b0rlYZfRbHZfrb5hZcbi4F9y0x:YkBawrmpAp6gB5Ki4Wa
MD5:	CD247A8EFD446C3E6C0023702E69F6E0
SHA1:	24096980765F18ADC88EF329B73BC2FF92EDD718
SHA-256:	33F46941EBB627115C7F4C03CF3A3BD8D75A88BDD1CDD2CCAF3AB583252EADE7
SHA-512:	5EC89044E60DF73927CD9339B1CD553380D10BEE291C8529154D6CE149C83C55336C73693F6B86C8C84742D07D3675D39D292E7A9C7F0F7B7D2013DA6DD4696
Malicious:	false
Preview:	....."l....1611805649533..bbre..c..desktop..file..user..htm..id4380..loading..users..xbrfwti0jjpuhyw1sc7ota2ldzk9z*.....1611805649533.....bbre.....c.....desktop..... file.....user.....htm.....id4380.....loading.....users...!..xbrfwti0jjpuhyw1sc7ota2ldzk9z..2..."....0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....a..... ....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....w.....x.....y.....z....y..... .....B..... .....*>file:///C:/Users/user/Desktop/ID4380.htm?bbre=1611805649533#/2+Loading .... - XBrfwTi0JjpUhyW1SC7otA2ldZk9z:..... .....*<file:///C:/Users/user/Desktop/ID4380.htm?bbre=16118056495332+Loading .... -XBrf

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11656199446418389
Encrypted:	false
SSDEEP:	12:LwCuqLBj/D77M3l/4nMWQA9L0BQZ8fOyn:yqLBD77M3GbN0TfLn
MD5:	1EE5EBFF8087ED05562E212029219B73
SHA1:	45989E4C3010FE288A8ED083337583C4CD50DDB8
SHA-256:	D46DFCD5A614FB2941A78CA5A8D3E126550C134C9B6EF36D71EF3104FBAF197E
SHA-512:	84D0457FBD2A752026BE7E74943B33ABFEFF602384DCC0522C1526F6C38CBD0D640DA982D3B71290C6DE024157478DDA7304B82D17D45EA43A1CB61CF34CB2 4
Malicious:	false
Preview:	.....LM..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Entropy (8bit):	5.540223829184991
Encrypted:	false
SSDEEP:	48:0DPp/mmlllf5XwZwGdDa74MoD8dbAWk0jbQSefgGBNrS0U9RdiN94:01932Ha74MoQdbAWk0jbQ5fgG7rS0W
MD5:	B49868FB9D098206280EC9645B2BE5D7
SHA1:	13946BF484B23F2A292005F546190AA41E917011
SHA-256:	180870540CA7FAD00B6C8A0B92166E4212E65E4EAA263D7D27A87A566ED2A2F1
SHA-512:	82CA0345D1DB20A21625153FED455BF53BF15DF268A4DE6FB7F3D4C1670F229A5265F65F5EB993DC515BCE9E44C6BA43F754D5D81F3DC937BEBF7F892D7FAA7
Malicious:	false
Preview:	E9.._..*.....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://..nbrteststA4..../.....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..645356000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-01-27 19:47:38.57][INFO][mr.Init] MR instance ID: 710fdcb9-c7f9-4a9c-8d28-b6f007347690\n","[2021-01-27 19:47:38.57][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-01-27 19:47:38.57][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
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.2224217430927276
Encrypted:	false
SSDEEP:	6:mP/+Wuyyq2PWXp+N23iKKdK8a2jMGIFUtpe/+jUk1ZmwPe/+QaMjRkwOWXp+N23c:C+Wuyyva5Kk8EFUtpy+jf/Py+IjR5f5i
MD5:	D35226175EBB4A52F91CC662ED2A7737
SHA1:	DC7FCC9475B2A3B483FF888B6F7679B4379CB5B5
SHA-256:	DB43FDD148D2AEB8E684D9927AB4EA3970F5CB16B95C34603C89D5D94DADAFB6
SHA-512:	8BADEF89B736AA588FB1A6B877940F4EBB7BB0862DD520E7DB5A6CDDFD3D8C36B60D88386B0720D62141FD09DD68B0D3D6E7AE1A580BFF010B3755F89F4A891
Malicious:	false
Preview:	2021/01/27-19:47:28.363 1010 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/01/27-19:47:28.364 1010 Recovering log #3.2021/01/27-19:47:28.365 1010 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.294803403229483
Encrypted:	false
SSDEEP:	6:mP/OJO+q2PWXp+N23iKKdKgXz4rRIFUtpe/OzDZmwPe/OHUzVkwOWXp+N23iKKdA:COJ/va5KkgXiuFUtpyO//PyO0Z5f5Kkt
MD5:	0E4C0F04BCE4173630E9CE9B28A3CFF3
SHA1:	EC0BDBFE47D7BE7A7CB1076C48CA5B0351C6D1CB
SHA-256:	7BD66A19D64ECEFE1BAD3552D9EEEA01D09C87FB0DCF1F0D2CF44D7F580C2264
SHA-512:	6CA548F28E0B47614F08455563E130B9DAC345C7F3BEC4CE4A017CBD125D6B82753D762A83EBDD6AF83A6752C196EDD0BC8DE6BE285FB070B43501DB6A1602E
Malicious:	false
Preview:	2021/01/27-19:47:28.546 1608 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/01/27-19:47:28.547 1608 Recovering log #3.2021/01/27-19:47:28.548 1608 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):	1.0741916837767933
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGU4vQK03fBuJAb1:wIElwQF8mpcSEEkQPEIb9
MD5:	1196562A41F5678CC39FDF76E9748067
SHA1:	50453B2799F4B8360733797A4FB767B2F100ACF1
SHA-256:	8AB270036484021C6CD91E4E931D57EAA11CB72E2D7BE9930F1977D7123DDC46
SHA-512:	684B5225C92A35659BD9CCAF783FEA7B978E376BF1D2BFE94975CBEA49A29EBD4B2CC72CCFA0FEC9889F04F89B379E6C8E6A5F7EE17288EC98F26D0EAE39E6C1

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6287240511176662
Encrypted:	false
SSDEEP:	48:iZ2qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUG64:i0hIElwQF8mpcSq
MD5:	2D13E2BE979B97CC741986ED97FD818C
SHA1:	23BC644AAEB805A76F2DFC065D1A8B7C75B5CEA8
SHA-256:	0B4D6D2C79CC51BB850F39362777E5872F97658DDDC56E9368E65B515BB8E4DE
SHA-512:	CF66A53BDA8AECC76A7A4C28F84F516B5210F79CDFAB8E9F949EBBF0764CD6A8D44817454AE46563E17424732F04471484B50D0FFA6BE15B5E6238426C3F897
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	265
Entropy (8bit):	4.320418106765339
Encrypted:	false
SSDEEP:	6:5lk/lllaHzZvtjAJef3ul1kAl1kAl1kAl1kAl1:5lMlYz1tjAJKmkAvkAvkAvkAv
MD5:	7DC2D992419965B0F707DBC365FFDED4
SHA1:	ED44C6F41E446204F4F1A92BB75C7DBF5CF0545D
SHA-256:	98BA7114E861BFD29A6DDE9AC3D1578E60A447A948D3FE6D1F8C4EE8B1BE7BB0
SHA-512:	948B5A0407E79AA80C2F51FCD8529D487BFFB23B7E678D2071868E9936D929358F91C833FDC7A7ABA8D38695D01E1436E796F788655F7125786D73A53B09DF96
Malicious:	false
Preview:	..&f.....7..V.....next-map-id.1.7namespace-5a8c47a5_a981_4fb5_84a5_1f8f45764bdc-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):	320
Entropy (8bit):	5.2237428708669285
Encrypted:	false
SSDEEP:	6:mP/K+q2PWXp+N23iKKdKrQMxIFUtpe/YwZmwPe/bVkwOWXp+N23iKKdKrQMFLJ:Crva5KkCFUtpyYw/PyB5f5KktJ
MD5:	C8FB74A7FFAB9604B60B4657D80EA191
SHA1:	A6020A6D57FD0ED2AAB4F439CA439BB1D6F53B1A
SHA-256:	1BF84F8E8AA51087234D3824FA272A43500D4CB3CFF9DA8D61DD7B6F254AF4D2
SHA-512:	AFCCA2ACED038F0AB797CDF5E1548EEE31505236A114B8DF8469201140766788813C105ED09C92E169423FDC234A96F8C80342F5C1EFFC174E01E9BBC1CF555
Malicious:	false
Preview:	2021/01/27-19:47:28.468 1608 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/01/27-19:47:28.469 1608 Recovering log #3.2021/01/27-19:47:28.470 1608 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.163400579676575
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SSDEEP:	6:mP/1GMM+q2PWXp+N23iKKdK7Uh2ghZIFUtpe/0YXZmwPe/PGMMVkwOWXp+N23iKm:C1GN+va5KkIhHh2FUtpyxX/Py+NV5f5m
MD5:	3E78149D150997D0F8BD61187A71D586
SHA1:	0EF81DC5BD8D7C3157D590A5B9E739B0E17B96E9
SHA-256:	31367B898C1748A7DADB33D0DF736433305A3E32B7A6A9613A7CE9735A3DC169
SHA-512:	41CEBC1C14CC806034BCE6A3DA8BE5CDD3309EDFB710D8ACF7A458065D80C362E1A5FEF84C305C86A59A2AEE0D057A350B60C40929CE68ADA7F1DFBF6CB0ACF9
Malicious:	false
Preview:	2021/01/27-19:47:28.291 121c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/01/27-19:47:28.292 121c Recovering log #3.2021/01/27-19:47:28.293 121c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\48dfa693-926f-4504-b052-779723bf4120.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.303060733179088
Encrypted:	false
SSDEEP:	6:mP/G+q2PWXp+N23iKKdKusNpV/2jMGIFUtpe/KMDZmwPe/KJnVkwOWXp+N23iKKZ:CHva5KkFFUtpyKMD/PyKH5f5KkOJ
MD5:	086766C8956CD51C26D85E0E66A89B76
SHA1:	B2EEE98BED5D12FA73661DFD983A4CD1C0BD0DD2
SHA-256:	29E9844B70A12C2CA8604732B25CEE4111B773CC6ACB0AF3FD04EB363190DAA1
SHA-512:	0D9E011E4AE8DD333FB5FB466ED922B6BF8DF3587AC8263E30FD741D77AD6ECC7B8DCE90AB465F1E7FCB578F0D99508317D18F06EDCC12E132A7C31DAA584F0
Malicious:	false
Preview:	2021/01/27-19:47:28.499 1608 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/01/27-19:47:28.500 1608 Recovering log #3.2021/01/27-19:47:28.501 1608 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.327830968237057
Encrypted:	false
SSDEEP:	12:CO0H+va5KkmiuFUtpyOPKW/PyiV5f5Kkm2J:fDa5KkSghPlf5Kkr
MD5:	1B04C8300135EF22375E2A9987704285
SHA1:	A71A1217580A43E0440FF64CF015AF4A9BB9EC3A
SHA-256:	EC8B324EF5CB65B946B4D88BC376AD9E94EE5BB9B3B913BE73EC09DD4AFF677D
SHA-512:	0012625E8E9047EDC655ECDBD3157D296566079E260649180017DA43A07CA5D7592F74ADB4754B4C681BE07742947780C2DBEBBF64883F069322A17938456332
Malicious:	false
Preview:	2021/01/27-19:47:28.548 103c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/01/27-19:47:28.549 103c Recovering log #3.2021/01/27-19:47:28.550 103c Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.296936458957273
Encrypted:	false
SSDEEP:	6:mP5SSuGH39+q2PWXp+N23iKKdKusNpZQMxIFUtpe5SHUKNJZmwPe5Scv9VkwOWXJ:tzGova5KkMFUtp9HDX/P9c75f5KkTJ
MD5:	FBC51FACB9CED4AADD4456BE7DCF3966
SHA1:	332A796EAE5B42F2BFE521822DDCC61867E301FC
SHA-256:	8281163E1C74CB66327B636B4D76F3A4EA081D14441F13248083D6A6F328795B
SHA-512:	540EBA836ED362B7CC34D4F9F9DDF31AC381C2E5C48237D918BBB33888B63C14DBF6402CBEBB8BB5E657D1C5905937E5DBFFAC67F8E55F8D97C6B2D669355E2
Malicious:	false
Preview:	2021/01/27-19:47:44.727 13d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/01/27-19:47:44.728 13d8 Recovering log #3.2021/01/27-19:47:44.729 13d8 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\029fb286-178e-44a5-b977-daa51b47cc67.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\029fb286-178e-44a5-b977-daa51b47cc67.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.2646936120855665
Encrypted:	false
SSDEEP:	12:3Kva5KkkGHArBFUtppH/Pr5f5KkkGHAryJ:Aa5KkkGgPgtf5KkkGga
MD5:	9E388392322BBCE1ADC01E09BC26756C
SHA1:	84EFE5209FD9D44EA01E762F7250A01BF2DC3FF3
SHA-256:	31EA2F4A6B0B440BCA219FCF3F55123BBAF64A469D69A1857B59A2543CE0B71A
SHA-512:	1A664C136E5D5D89EC14EDA3BC0DDAF341246709CA9606A1070A7C98883025FED3BB830E3BA930896822170189F12580C89E696433ECA345CFE0057971D9AD52
Malicious:	false
Preview:	2021/01/27-19:47:36.384 1608 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/01/27-19:47:36.391 1608 Recovering log #3.2021/01/27-19:47:36.395 1608 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):	5.229688091450901
Encrypted:	false
SSDEEP:	12:lg3+va5KkkGHArqiuFUtpxs/P3V5f5KkkGHArq2J:Xa5KkkGgCg7af5KkkGg7
MD5:	2458289E5B26AFBDDF4C6CE727BCC978
SHA1:	B921A31BF3D3C09CC0C4C20CD1D8112B24A0C695
SHA-256:	41725F4408D04CE47A0067759DF72300EA1E8DD6CC2A5A45BB0AE12C9021B9CC
SHA-512:	261553BA0668613D5B3A125E21319F787B79231409D6E9EFB72F95B1FB7DC850F9726AA6ACDDECBA8571851B39100DA37743A02726A13CACCC8CA488DC3331D
Malicious:	false
Preview:	2021/01/27-19:47:36.400 d0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/01/27-19:47:36.404 d0c Recovering log #3.2021/01/27-19:47:36.405 d0c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Preview:	..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.242563868248969
Encrypted:	false
SSDEEP:	12:Qva5KkkGHArAFUtpm/PG+5f5KkkGHArfJ:ia5KkkGgkgvof5KkkGgV
MD5:	43BFD73C4418ADA0CDEEB3117CF9A9C3
SHA1:	F42F5CB9ECD722D10BBDA8717C2B88EC8AB6A1B4
SHA-256:	DEA81E2A84B021CB65A75A85D490119A66B88921AB4D691ADE4D3A838A2DB216
SHA-512:	12F4658D23FE12B6CC65F37A68D8498573BDC38A1D4A3C2E8B4870E0DCC782DE355DB54C745F97576A0FD6DA2A1CA7C7DF3032D651BD00EC93F398A2146B95 1
Malicious:	false
Preview:	2021/01/27-19:47:51.804 1608 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/01/27-19:47:51.805 1608 Recovering log #3.2021/01/27-19:47:51.806 1608 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.237415186441372
Encrypted:	false
SSDEEP:	6:mP/QM+q2PWXp+N23iKKdKpIFUtpe/6UuXtZZmwPe/6cPMVkwOWXp+N23iKKdKa/o:CZ+va5KkmFUtpy6lXtZ/Py6JV5f5KkaQ
MD5:	13640C403BC7C47DCA5D2014FEFE66DA
SHA1:	AFE0E159E9ECD3EAB6EE1E3BD5DA3A188857C8CB
SHA-256:	D9915EF8D494BCBBD1CB748EB3D0315EBCCE4FD744F54AD7198FEE7B11B000A7
SHA-512:	74C03FB56A665779EA051135ECBBE31447144335F37550A9975BBF9D0E18F7ECBD0E7D28CEE421E4D4794364F673480600D5A819DEA0F12465EA9ECE81920EB/
Malicious:	false
Preview:	2021/01/27-19:47:28.317 121c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/01/27- 19:47:28.321 121c Recovering log #3.2021/01/27-19:47:28.329 121c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Size (bytes):	402
Entropy (8bit):	5.401439434108915
Encrypted:	false
SSDEEP:	6:mPn9+q2PWXp+N23iKKdKks8Y5JKKhdIFUtpeBKJZmwPeBXF5H39VkwOWXp+N23iC:Vva5KkkOrsFUtp3/PaHz5f5KkkOrzJ
MD5:	FD8B9BD708918066518ACFB529C5AB99
SHA1:	EB61B3B639D012E55F7A402C92556B21ED340B59
SHA-256:	C9EC0DE75E70BF04CDBDE1C20BBA80D06DF5EEAF026A5127C4702044C6D2DD49
SHA-512:	F78CB721A0C9F64F1C42FC85974FAD81AFE670E48431DC92438153238A1D773CC3CB279833A508F14A4B543398B5294070236D3BB2145D8906653F4693B31654
Malicious:	false
Preview:	2021/01/27-19:47:38.559 13d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/01/27-19:47:38.561 13d8 Recovering log #3.2021/01/27-19:47:38.562 13d8 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):	4.647055208874201
Encrypted:	false
SSDEEP:	3:93ZtxallzJ/o3fuv:93Txuovg
MD5:	6BAC7162A83B81A4FDBE98E984D2FFA9
SHA1:	E7B9E79EB7890CFC3E1DED43FE8AC192EB39AF32
SHA-256:	80E95196ABDE64C6218D1652F59984F9B5A9D453BCAB2A70BF339D9CB53493FF
SHA-512:	83CCCEC438771ACB1DDD9447EA7B86A2DAE1AB381651677D09A8BCDC5EC45E4A1717305027CB443950EE7755CEB4124022AE30FCF136A91480FE41DD36D928BF
Malicious:	false
Preview:	....Y./ .-.....^.\....'*D6..7.....<z...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\49771840-21ff-4832-8c4b-a81d2169028a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 13 icons, 8x8, 32 bits/pixel, 10x10, 32 bits/pixel
Category:	dropped
Size (bytes):	175509
Entropy (8bit):	5.489440694064333
Encrypted:	false
SSDEEP:	1536:rKbsLAR2A4VBQV1111111111111Nr366R6faFR+up0y0y2im1OsFcgYzQNL9X:rKbsLAR2fe/FZntrslfX
MD5:	33EABC19FDF40F3D36B6870EF5861957
SHA1:	CF3EF59C3940B58C314E9F6A1616751553F2D9A2
SHA-256:	647D07F37554672865902B2CEE80864B5A5283C372C7263BB1497D5582054E57
SHA-512:	47CFEDB1FDBC9BC09905C70F69A5114C64A8FC791BCA480D24972275276F00CEB230C579B4217337F9C69ECB2AB3221A3B549F06E8074D76BCE2F31773FB69F
Malicious:	false
Preview:	..... .H..... ..... .p..... .h...n..... ....n...((.... .h.....00.... ..%..~H..@@.... .(B..&n..``.... .....N..... .(....D..... .w`...M..(..... .....+.O-8&]P>/^Q?-^&:?I.1;<....qye.f.%.....X...E.....I...k}....{.m.t.CP.....E...\.....=H..,A..,J..;P.....nnp}nnp}.....~~~.....!...!---2---2... .....(..... .....!...7.#.:3,";3,!<.&'/.....NPLYt.F.K.%.....L..C.....1...`...KOPVutz}..A.BxX.....P..Q.....1...x...tqpyxuux...0D..DP.....G.....uojuppnw....t|..9F..-=..+:..5:..rr.....llkrkkmw.....ggitllkv.....hhgssss~.....YY\eYY[e.....nnnzXXXa.....RRR\.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Applications_crx_nmmhkkegccagdldgiimedpiccmgmieda\Chrome Web Store Payments.ico.md5	
Preview:	F.....r...(R..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a2e71e33-a612-46ea-a458-931f3bff73de.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):	22613
Entropy (8bit):	5.535734616530891
Encrypted:	false
SSDEEP:	384:Z2UtgLleYXC1kXqKf/pUZNCgVLH2HfD+rUfHGTnTBajdS4N:8LltC1kXqKf/pUZNCgVLH2HfKrUPGTnQ
MD5:	312F5FE9ED9D445E59D68840CC3643F0
SHA1:	C1F8AD4B19FD1FD2F4577F1E2A7E81A7D4F58F2D
SHA-256:	EFECD57383C4DF657F909DCD775920CA54043E67FC17FA22A8DF49EA66B7F58E
SHA-512:	3F1F609E19FAF4EC82EDC2F0CDB85C8EDAAFFDC48ACFB07A3D343B9F5D2577A3D60A03A4803EF4F02785050A90778161AEA022A84AE546B98523CD48A31092 9
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13256279248309102","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c6d06dd7-1647-4703-916b-05db089a2ace.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\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.653676757250244
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
SSDEEP:	3:tUKbMfWU2dESZZmwv3dMfWQjmV8sdMfWQjmWGv:mP9ovZmwPe5KVve5Ktv
MD5:	9CFCB03C2CDE64647EAD2FA2C5134CA0
SHA1:	112A96247057B6A7577C2E69E2183E6348E1F670
SHA-256:	F4F7DD708F7C3F9D4ADAF27FBF59D8C4B1CFB739B743440D00DD8C451966D22D
SHA-512:	17470E400FE4033E31415B26B9582ADAC8F168298BCAEFD0B76B4D89C369C437C06BDBDE6C4437910ED6FF251A4EECB2A4FD8B34ACF7100854189ADB9F606C1
Malicious:	false
Preview:	2021/01/27-19:47:35.607 1aac Recovering log #3.2021/01/27-19:47:35.649 1aac Delete type=0 #3.2021/01/27-19:47:35.649 1aac 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/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\db6a75f1-40ef-47b9-aa79-cd833f68218a.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):	24073
Entropy (8bit):	5.533514200227994
Encrypted:	false
SSDEEP:	384:Z2UtgLleYXC1kXqKf/pUZNCgVLH2HfD+rUaHGXHGenTBaMdS4s:8LltC1kXqKf/pUZNCgVLH2HfKrUqG3Gr
MD5:	D5B815187CA3EAD6EFE2CA416D347CF5
SHA1:	F40991B6FCE416E77FF64361FB37C504698AF9C0
SHA-256:	E672C4AF48A6A1C2D06A1DE9C6085477F023369EC9801EDA9240BB033DBD2E59
SHA-512:	12C6C15EE68D3CE8672868F5123FE13611E60342737D053737848FBA26EEC19D196C103329BCCDD265D2F99D668FFAB65DAF8119D1CE46882BE9213C1B254AD
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":"13256279248309102","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\db7326a8-6520-4510-92f3-aa0b852234ac.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):	2655
Entropy (8bit):	4.876730946556595
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHzMzsDzRLsFTsGogspX8qO6Ms8yveNsV3zsqMHXYhbD:JTnOCXGDHzMuqwBXrO6g+eOjGIhH
MD5:	5B956F99B4E52D52CE94EB27108F7EA4
SHA1:	CE2AFDBE16C91303EEFB11AEB7DC5454A1BF54DE
SHA-256:	7F8A8DB2CBD22511625E289A2348F665CF4FE06EBF0AC4FD79A05575B5D8FB35
SHA-512:	5F8FA9F887526E325FF461236C28A97A8FAD97909098CD708A9F56DC83B7A12ED477DC5C33F63884B280F8D9BC9649863800406EF6CE83567F1A06FC5CE8338A
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://nodes.smsmail.net","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13258871251212488","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13258871251228638","port":443,"protocol

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ee445f44-00dd-4d1a-830b-fce2dde17a19.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):	5394
Entropy (8bit):	5.168862591127933
Encrypted:	false
SSDEEP:	96:nDRFVu4hohBcVUSok0JCKL8/DgbOTQVuwn:nDR24KhBcON4KgO
MD5:	1E128AABA65D1E652F36914BAC961B21
SHA1:	1DC127598B0A13B74A45336A284EDB86D82628A1
SHA-256:	F56465E70D2C016D5F110DA80E65D2398D5B9F094B34D6818973946471C310D7
SHA-512:	C94F79CD81F204FDA4BDA0D5B29BDA6F85F004490430A3E692E0497BCF28D3CAF91CBE5D6EA902DE8A33F43958B5C351C302D29EA372B12B5D1DB2A0ED963 B9
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256279248522241","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

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):	5.247483415982857
Encrypted:	false
SSDEEP:	6:mPa+q2PWXp+N23iKKdKfrzAdIFUtpe15ZmwPe1tVkwOWXp+N23iKKdKfrzILJ:Sva5Kk9FUtpu5/PuT5f5Kk2J
MD5:	3B98D7CC2B4932D6097A482228C97BE1
SHA1:	FA6061AB5488DBA2FBB77062C2E9491A985241F3
SHA-256:	486D84BF6A615F0913E960A533BD18181538CA69B80562D965B12D60F7C48516
SHA-512:	A1167EE23D1C55D3CAFE45A953FAE4AEEE8DBAC63A305B9F08C75B2B16BFF04E37EAF2FC02F69160740770A018BDDD5863A0C87C81812796B7845F0678B9037 2
Malicious:	false
Preview:	2021/01/27-19:47:38.214 1608 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/01/27-19:47:38.217 1608 Recovering log #3.2021/01/27-19:47:38.217 1608 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:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
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:	3:8EflZ99u:8w9u
MD5:	F04113D0B0DFA080C46867756342BDA3
SHA1:	3F2EE13357DFD8D894E2BBFB04331E5FFB1F6267
SHA-256:	460BE57550B8361B7F1718C2173A1603C67663DC041CD8500BEDC81AE8DB0E7B
SHA-512:	74455BA1EBC8E76AF407F75E71CD98BA24033C04F3CD8055BA651EE84A643F90AC8F5DD9A1F1CE9C11035EF10076197A5C602B7543030676F655DF71949A279E
Malicious:	false
Preview:	.'..(.....k... /.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.18.0\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_dir5216_1502180960\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235624
Entropy (8bit):	4.967847153665615
Encrypted:	false
SSDEEP:	3072:EtV4WVaR1c58AVLz5LTmUbHqrzpxmHBoET2N42aq5tETVoQ6MGnr9/ipKiao5u9V:WL8lVZT2+85tThEKl
MD5:	4AFE0BFD28E65161E164F53178A96836
SHA1:	498E6448FAC9E2901F65124C8A3D79077B5256BF
SHA-256:	3F8EA1BE3A593F8309C89B6A59249EFF593EF90911FED8205D9C964594BC112B
SHA-512:	1FD7BC2FC2114A9D1CA79CFD730D19BEF72159D54DBF962D6E3BFDB39F7F2E13833B236C6C9B8A5C9AABD7822820E42D28C9E7310F98CD74C2F371C75D1CF75
Malicious:	false
Preview:	.....<)..... .....`...D.....|.....t...p.....h...d...`.....t...L...T...8...@...<...8...4.....,...(...p.....uocca.....l.....ozama.....`.. .....0iupb.....@.....g.bat.....onwod.....ennab.....`.....nozam.....geips.....|...0.....rekoj.....H.....lgoog.....q..`.....uotpo.....D..... ..lreko.....t...+.....t.....l...P.....,.....h.....H.....|...$...t...p...l...h.....`.....X.....P.....\|...D...@...<...8...4...L..,...,..$... ... .d.....D.....l.....|...x...@...p... .....\.....T...P.....H...h...L...0...8.....0..,...(...$... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\d3236fd2-59cf-4e3c-9662-807081e36f4f.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):	154991
Entropy (8bit):	6.05164018001793
Encrypted:	false
SSDEEP:	3072:t8kRDb0lSBYPycFIs4+w6EoFcbXafIB0u1GOJmA3iuRX:t8l0lS8Gs7tvaqfIlUOoSiuRX
MD5:	6DCE7E034DA85B315118E436E2A1ECFC

C:\Users\user\AppData\Local\Google\Chrome\User Data\d3236fd2-59cf-4e3c-9662-807081e36f4f.tmp	
SHA1:	79EA00CDDE6413EDE279DC7451D20F5FC09668F9
SHA-256:	3B9B8C644D8BBF5F9EF8B2132395E8DF286A972AA2144B5FE448E77F038F9DC7
SHA-512:	3A0BCECDF9CD75C7F8AA5E7FA27963FB59681CFAC831D6600A19A9393961B08D0EDF147AFE6B8FD0E8B0295F5987F22B7059845DDA34DABE7DAB93C561C673D
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":1.611805651225903e+12,"network":1.611773252e+12,"ticks":101240739.0,"uncertainty":4481293.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016289563"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\d7b90c53-c9b5-4d0d-bf67-52718dc53869.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):	155189
Entropy (8bit):	6.0522475432252065
Encrypted:	false
SSDEEP:	3072:x8kRDb0lSBYPycFIs4+w6EoFcbXafIB0u1GOJmA3iuRX:x8l0lS8Gs7tvaqfIlUOoSiuRX
MD5:	184EC87B087D31CB093B3936026D5CC2
SHA1:	3CD27F8AC1DF9668DDA3D460789EFA8898149526
SHA-256:	E4FE0508F565633C70FDD5A0EBFEE7152162AB79A53BBCF7E004F2152B9BD961
SHA-512:	6C378C19D84AA31F0590160DA7F24004159C6988A8D045DE1811E55583D921786C21E1FEF7EBAACFE2A7622C3AF0A1EF2953634415F39D529720D7B84C79011E
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":1.611805651225903e+12,"network":1.611773252e+12,"ticks":101240739.0,"uncertainty":4481293.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016289563"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\d92610ba-41d8-4e8c-8d36-3a3d687e3ea0.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):	163463
Entropy (8bit):	6.082290232736345
Encrypted:	false
SSDEEP:	3072:OVv8kRDb0lSBYPycFIs4+w6EoFcbXafIB0u1GOJmA3iuRX:Qv8l0lS8Gs7tvaqfIlUOoSiuRX
MD5:	D91C7D00AE8E44FFB30464478DC1CB6A
SHA1:	3A65C624AA80EBE7959AAF21C12C314CDC79C571
SHA-256:	FB8240EFC5485113D19357023CAD47DA613A8DDE3A8FB9FC21B9B73463D7D9B3
SHA-512:	6C58FD71E0681CA7A7778DE6A43DBB70D91C6CD4A283D948B6E7BCC4AFAB28D0D0307E98582380AFE7FCB1A34C3B6C84816C4F46691D1DB135F3ECFFFB4C2AF
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":1.611805651225903e+12,"network":1.611773252e+12,"ticks":101240739.0,"uncertainty":4481293.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\dcbd6191-17b4-433b-977b-72904ce1f9ac.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):	155085
Entropy (8bit):	6.051930170265883
Encrypted:	false
SSDEEP:	3072:J8kRDb0lSBYPycFIs4+w6EoFcbXafIB0u1GOJmA3iuRX:J8l0lS8Gs7tvaqfIlUOoSiuRX
MD5:	CC2D7DB3D2C65B203D7543F21FB3FE92
SHA1:	83223250708663997612F953EBEBE412801F4D27
SHA-256:	119FA678D3DB521A7B8032F4C64F9795E5D99BF2AD2122C8FA15878CA5A0F4F0

C:\Users\user\AppData\Local\Google\Chrome\User Data\dcbd6191-17b4-433b-977b-72904ce1f9ac.tmp	
SHA-512:	DB755B5737971B019CBF388F7E94D3481FBBC6BDA7AB279D4C6EB0ECF776F83BDBE316C62EEAFFC5D6DB14E5225E35486EF7C10873A705533C13043762C49C3
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":1.611805651225903e+12,"network":1.611773252e+12,"ticks":101240739.0,"uncertainty":4481293.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016289563"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\e51a915c-9471-4f27-85a2-64fed10f53ef.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):	163463
Entropy (8bit):	6.082289319783923
Encrypted:	false
SSDEEP:	3072:O4Q8kRDb0lSBYPycFIs4+w6EoFcbXafIB0u1GOJmA3iuRX:tQ8l0lS8Gs7tvaqfIlUOoSiuRX
MD5:	5360B92439CED168B13F80DDAF56F2BE
SHA1:	04B06688E6EF8DCDE537BC712018802F7B34949E
SHA-256:	F072FA41821669F4372D88E5915DE411DE2CE7E720E206371060AF0E48E9A09E
SHA-512:	588305CEBD27A6B5AA7D4F6B10EBCC49F7B99A6463B7789CCEE4D4A02D9454147743B61CD2BB2E5EC61532EC5C9C9EE22636AA2B9A04D5011918022DADBCB25
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":1.611805651225903e+12,"network":1.611773252e+12,"ticks":101240739.0,"uncertainty":4481293.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\e766af71-ed0c-4544-bbb4-7e93439bf7e5.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):	163463
Entropy (8bit):	6.082290442873002
Encrypted:	false
SSDEEP:	3072:ORA8kRDb0lSBYPycFIs4+w6EoFcbXafIB0u1GOJmA3iuRX:0A8l0lS8Gs7tvaqfIlUOoSiuRX
MD5:	1D390C8FCDB41100BF3B6A4CB16F5595
SHA1:	2FCB3B0A87963F00A671C33B5E7CDAB8DED03357
SHA-256:	0CF06CFC5E8F91FE1D37BFD4468728BECB07EF65E51C75F5AC78561FCE02FB6B
SHA-512:	2C9F29548CD3B5EA4E2AD2871DDDD317AEEA9061A7B2EC34121EBEB60D30BAC5FC63415ABA5DE6B4090F4BDDB188D03600690B10B779A7F3FC471E5A86797AE6
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":1.611805651225903e+12,"network":1.611773252e+12,"ticks":101240739.0,"uncertainty":4481293.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\e8f6b7a8-6121-4105-85d8-45b8eac88391.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7521419303352332
Encrypted:	false
SSDEEP:	384:Nf6pNTMijs/fVIu10N9rOvBL3CVn+Hv2GeBrMvVNxy/TvCrwdmI8WsLlFVCOT7Fu:Nuu5VeTMC8enNvfofrKDKtjpFU
MD5:	49FFC06C44D0BF1FF10A98FC3109FC70
SHA1:	DAC7F6E7368C42FFF984645C89118E4B576A44D0
SHA-256:	7EC4D2FBA2B071CEEF65B1E8A9560252C16DB54962A3B18D2C5939EC1E47CB76
SHA-512:	52B1123E59881212AA1F1E33E2E704E80C70F714D1305E4675874301FDB31A77A0CF0D480707DAF4ABE637CCA0682AFFB82DCF339857A437595E3E8861B83D1C
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\e8f6b7a8-6121-4105-85d8-45b8eac88391.tmp	
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n..../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\e95cc890-0493-4922-8747-d4e923db214c.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):	163463
Entropy (8bit):	6.082290395971981
Encrypted:	false
SSDEEP:	3072:U4Q8kRDb0lSBYPycFIs4+w6EoFcbXafIB0u1GOJmA3iuRX:nQ8l0lS8Gs7tvaqfIlUOoSiuRX
MD5:	3EB4AD2E3F2ED94BA6F4081C35F01843
SHA1:	5E301A39AB120F0D75D40955105E40040888BDD4
SHA-256:	B447A36E9549FCE7B3DD135EEAC2FA6902A951E9C885F2C10B09F46332DD021A
SHA-512:	E57100BC3D380DDEA1D8FF1F859846C063C976073276243CE3FAEC77514807A80F770900B8BC32ACD3700368BF96DA0482F3E844A7D102296927603F67B21717
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":1.611805651225903e+12,"network":1.611773252e+12,"ticks":101240739.0,"uncertainty":4481293.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016289563"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\5216_1502325624\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\5216_2980606\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.914285309904654
Encrypted:	false
SSDEEP:	3:SWuUJmHlgdGc1DVdCHDb87TkcRx:SWbJmHlLHsXkcRx
MD5:	DA2751277B14FF42373DF15E27B9CE19
SHA1:	20823DAF8755A7DAB983726C460DA55C634BFA49
SHA-256:	63B01D3AC2258EC441F20182A4C3FCBE5F47E09C14D4A511CB83EB447C7F0EDA
SHA-512:	0D99F79F4D6D3DF2C177CC3F4CE84CD76489C0A652C9455FA5322793F25C3B2910F7537851086AF6775B944F72E487893665C26EBD26F65C4BBE712803BEF818
Malicious:	false
Preview:	1.3c7a41cee94e225a40d1158c97cf08f3039bfc9b1c9102745eca434c6f6994db

C:\Users\user\AppData\Local\Temp\5216_518535266\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	66
Entropy (8bit):	3.866533712632772

C:\Users\user\AppData\Local\Temp\5216_518535266\manifest.fingerprint	
Encrypted:	false
SSDEEP:	3:SpUCQEd2dq8ebEJW2GnnHR:SXQ5Y88EJeR
MD5:	423CB83A2A3B602B0AA82B51B3DA2869
SHA1:	58BC924AF90A89CE87807919F228FE6C915AD854
SHA-256:	0047059C732D70AF8C2F407089237F745838A0FE4F75710ABF1E669B81243E9C
SHA-512:	F80E9B5D544894A667F74CFD0A4D784311299DB080CA6793AABD93B95CF1E2870F74AD38A6386D862580220047F828457240577335C565B7F38B0C6677811660
Malicious:	false
Preview:	1.ffd1d2d75a8183b0a1081bd03a7ce1d140fded7a9fb52cf3ae864cd4d408ceb4

C:\Users\user\AppData\Local\Temp\6769b3d1-a356-492c-975b-dfb28feda020.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U .KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F ....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\b8d073ee-4f8d-4db1-b8d9-eb04b0fed1b0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	300953
Entropy (8bit):	7.973503294353402
Encrypted:	false
SSDEEP:	6144:0sb1v/4nxPbqqBbWbFsw+wh3bC5NFv++S/hup0XcaxlnJ9:7l/4nxPZbOFsw+y3d+S6WnX
MD5:	1FE8E0AEB768437A23CEEAE6053E5822
SHA1:	5529A275644B729009E22035F6125879450F4ABB
SHA-256:	25A2F515CEC98CF2ACF11B34C59723D76820A4B5734E223D7EBEA55E5A851468
SHA-512:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA56812320
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....L.18..Y.~..%...~._.....O\..p,...eY.0=.!..+.SoZA7...:t.G...VZ<..d....MN.....T..{1\.T...P, ...i...NrD...e.2..u....5.....1.n.Zu.E...!..XR..j.:.E.gUw.-s7:T.c_...(.i..iU.).M=yF<..`.....F...@)..IK.. b.4.o..mC'...N.*@OtT...`.&|.8.M;.....0..0...*.H.....0.....).'..b.*$w\ $.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....R l.G.,2.....[..T'.....".ct.).s#.(/.D..C..4..RKf.W....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...H0F.!...L..\.j.1.d.....==v.....-

C:\Users\user\AppData\Local\Temp\c10c471c-5147-4e97-9199-bbc831511d31.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\Temp\df766ec6-7fb1-469e-a2fc-6eefe1fa8989.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\e5f7a061-8c56-4c1a-bb3b-38354f0f11ff.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\ed1c3b82-bd56-4e87-988a-bd40cb764229.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	300953
Entropy (8bit):	7.973503294353402
Encrypted:	false
SSDEEP:	6144:0sb1v/4nxPbqqBbWbFsw+wh3bC5NFv++S/hup0XcaxlnJ9:7l/4nxPZbOFsw+y3d+S6WnX
MD5:	1FE8E0AEB768437A23CEEAE6053E5822
SHA1:	5529A275644B729009E22035F6125879450F4ABB
SHA-256:	25A2F515CEC98CF2ACF11B34C59723D76820A4B5734E223D7EBEA55E5A851468
SHA-512:	45C8EEC35301495EB9DCE36B32F1CA2E9A7B167CAB52D3E026E2617134067C38CCE1463DEC18C1657A6984FBB8F342336E29E8BF6280C0533CB67CA56812320
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....L.18..Y.~..%...~._.....O\..p,...eY.0=.!..+.SoZA7...:t.G...VZ<..d....MN.....T..{1\.T...P,...i...NrD...e.2..u....5.....1.n.Zu.E...!..XR..j.:.E.gUw.-s7:T.c_...(.i..iU.).M=yF<..`.....F...@)..IK.. b.4.o..mC'...N.*@OtT...`.&|.8.M;.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....e..;.<LQ0{^....=m.V.#....a.NL.....%...p.@.4....Q.Fw...dUoCq....R I.G.,2.....[..T'.....''ct.).s#.(/.D..C..4..RKf.W....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...H0F.!...L..\.j.1.d.....==v.....-

C:\Users\user\AppData\Local\Temp\scoped_dir5216_1444961248\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	886
Entropy (8bit):	4.799570700992651
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyIDEK:1HE7n4gn8WYpYrbhz8ZpotHOPjsrdaD
MD5:	0F604F138A921EE7270C45E520621C30
SHA1:	E2BA940AF44609BEAC49B603EB1C379E43F4AAEB
SHA-256:	A149D52858570C9544E33B183915556230B7F66CF4ABAD4DDB00B1409476FBE1
SHA-512:	D87C8C7D0C998B37E34B7E4E6F5212FF4A0588C15F1273A55CD36B4A6FB13B7FDAE4F3B23EA469E7ACAF22B8BF53EB67476D897B96CA5C15C113EC078071A6D
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir5216_1444961248\CRX_INSTALL_locales\bg\messages.json	
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "..... .. .., ...-.....".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5216_1444961248\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	705
Entropy (8bit):	4.576619033098666
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyFJKtOi2V2Te:1HE5baib6WYpm31Lt0Z8Zp8pxOaKtwVl
MD5:	DDD77BA67108D8D88D66E35AA72A8048
SHA1:	F9C217728E756728B788C969F5101484D0557065
SHA-256:	3DB4D2B1586C020EC679C09148DB226DBB23857D326BECBB6CC48976036C391F
SHA-512:	6CA88083CECF6166503A1441BE8BB726CF08DEA8CFD61F1E81A970FE623284039FB9A530990E8E2008A4B1128399022AFE4F517E85CC7B069B670F5BA659F4F6
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "No s'ha pogut completar la transacci.. Torneu-ho a provar m.s tard.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5216_1444961248\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	4.771803710371731
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyN+/sFfmSYWc:1HEl4G8WYpdt8Zpq5TOT0FfmR
MD5:	B587AF92ECD087AAE3EF210364960844
SHA1:	AD78B31888863D3F0EC0D8CDCA316EDE9EBD7543
SHA-256:	9796A230BA459EF31E3D102B02575B73D6F1C812BF11F4D1E55B17C17891D2C5
SHA-512:	D2771ABB1174C3B6AF70BA1640837DE1B28137319307841B12A7D03C0A605AAECFC93069026A3906B289BAE12D33F4457FB54D7D27ABC5DC674C5C4C1E9F7CE 1
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "Transakci nebylo mo.n. dokon.it. Zkuste to znovu pozd.ji.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5216_1444961248\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	642
Entropy (8bit):	4.533570611298554
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyNz31m8tbYzD:1HErMKfqMKVWYpM6lL8ZpDNOOQ84D
MD5:	639CEF5231701AE13F81DBB67730BB95
SHA1:	E249FE0C70B0F85B033730719B6D1B30F0B04431
SHA-256:	6C71F9D37006245D0E2E956D6D2C1815FFEB43236DD3D427A02F8DD348AC93C5
SHA-512:	D040D25ADD9666050544F9173EF61E044F7EBBAE8C528FC4077880734141205AAE60566668E6854D0B9C8D59924E22D1665D2C93085ED7F7E1F4DA91B951F09E
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "Transaktionen kunne ikke gennemf.res. Pr.v igen senere.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5216_1444961248\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	701

C:\Users\user\AppData\Local\Temp\scoped_dir5216_1444961248\CRX_INSTALL_locales\de\messages.json	
Entropy (8bit):	4.598783840405771
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603Oy91Lj8SYJ6K:1HEzWWYp3Bewv8Zp7k4OALIhj
MD5:	6E1B49ABC0AA5C1E2764E48EB1EA256A
SHA1:	604E76C89D4763C002C51908CEFE8C11AF7CBBE5
SHA-256:	B692DB1A249223E62E62DE9725334039419B5942AF715669F0F0F4BDEDAC5733
SHA-512:	EE527D48178D09D66120C0D1EA2584A7397404109A074AC09487D6AE8507A593193B31D3197C2418A162BB3E7DCC46FA5844D4951BB09650FC2A4AA10EAB811(
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "Die Trans aktion konnte nicht abgeschlossen werden. Bitte versuchen Sie es sp.ter erneut.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5216_1444961248\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	875
Entropy (8bit):	4.920210350678433
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOBINZXD:WguYpCZnpEZb6fD
MD5:	41BB0DB6EC99E4664C6E2247EC704151
SHA1:	BF2268F9A77218384F1F73951F98829296318452
SHA-256:	90FC75C419D7359C2241F54562177252655526F3074E7E419E36F5C473843842
SHA-512:	738F7C254825E0D00D4BDF909FA6957D5A6027BCBCDF76F1385210FA5F908C2C94C038B6DF4309C68774C96B84447079AAF514F46519E60876BE4A8F4ABC9E6(
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "... ....".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

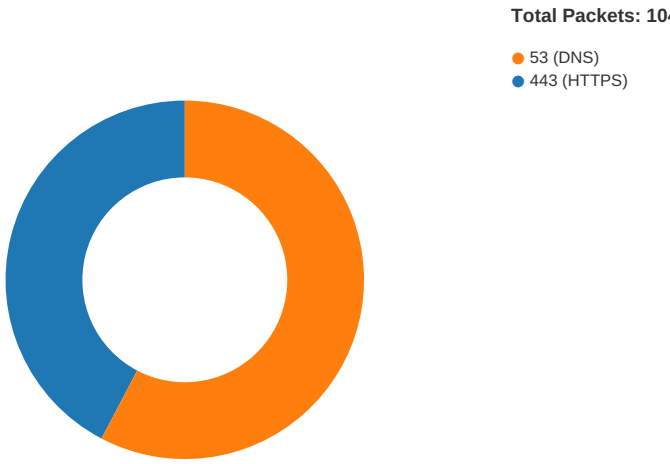
Static File Info

General

File type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Entropy (8bit):	5.993525367498149
TrID:	• HyperText Markup Language (15015/1) 20.56% • HyperText Markup Language (12001/1) 16.44% • HyperText Markup Language (12001/1) 16.44% • HyperText Markup Language (11501/1) 15.75% • HyperText Markup Language (11501/1) 15.75%
File name:	ID4380.htm
File size:	5695
MD5:	09856d61b88443692497e1d9d564c43e
SHA1:	099c3616cfb85bf601875d70f468bccec6d3354d
SHA256:	586258231081a1dbe0f78e8e2c3a93c144524a3c36038a a4ac202af9fc1ad848
SHA512:	0db764318445f4f3906604c9a4c44c83e5afa7180f7cec1f a4282fd1028e8c26803de2c33a63d4b202310c085610ab e08b2c51036db691fcb6e814fe5109fafa
SSDEEP:	96:kjtJA3emV6tS/PDfvMUv4EDvigxXTiiu7EcbLlVPg2eZ LAu2XU1/A2aVxAK:At7lt8fvMgbFxjiiu7Euhg8u+6/XUP
File Content Preview:	<!DOCTYPE html><html><head><script>console.log(wi ndow.location.href);if(window.location.href.indexOf("bbr e=")==-1)window.location.href = document.location.path name+"?bbre="+Date.now();</script><meta http-equiv= "Content-Type" content="text/html;charset=utf

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:47:30.704135895 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:30.750730038 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:30.750843048 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:30.751241922 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:30.799369097 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:30.804251909 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:30.804290056 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:30.804430962 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:31.026489973 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:31.026989937 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:31.027334929 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:31.072557926 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.072817087 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.072832108 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.073185921 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.073200941 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.073283911 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:31.113061905 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:31.121236086 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.611469030 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.611515045 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.611576080 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:31.611591101 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.611655951 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.611697912 CET	443	49726	104.21.19.54	192.168.2.3
Jan 27, 2021 19:47:31.611706018 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:31.651104927 CET	49726	443	192.168.2.3	104.21.19.54
Jan 27, 2021 19:47:31.735025883 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:31.777481079 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:31.777633905 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:31.777869940 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:31.820586920 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:31.822350979 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:31.822395086 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:31.822429895 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:31.822515011 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:31.841474056 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:31.841722965 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:31.841861010 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:31.884404898 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:31.884448051 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:31.884820938 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:31.926687956 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:31.929738998 CET	443	49735	151.101.1.195	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:47:32.204210043 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.240184069 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:32.282668114 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.647625923 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.647679090 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.647717953 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.647746086 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:32.647754908 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.647794008 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.647804022 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:32.647830009 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.647871971 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:32.647876978 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.647918940 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.647963047 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:32.649466038 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.649504900 CET	443	49735	151.101.1.195	192.168.2.3
Jan 27, 2021 19:47:32.649559021 CET	49735	443	192.168.2.3	151.101.1.195
Jan 27, 2021 19:47:32.738045931 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.778060913 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.778178930 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.778757095 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.818814039 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.822490931 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.822544098 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.822626114 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.834543943 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.834692955 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.834813118 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.874907970 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.874948025 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.874974012 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.875610113 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.875880957 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.898128986 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898173094 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898209095 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898216009 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.898241997 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.898246050 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898263931 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.898273945 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898305893 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.898310900 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898349047 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898369074 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.898386002 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898407936 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.898428917 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898469925 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898487091 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.898507118 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898525000 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.898535967 CET	443	49741	104.16.126.175	192.168.2.3
Jan 27, 2021 19:47:32.898562908 CET	49741	443	192.168.2.3	104.16.126.175
Jan 27, 2021 19:47:32.898581028 CET	49741	443	192.168.2.3	104.16.126.175

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:47:21.976315975 CET	60831	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:22.028677940 CET	53	60831	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:22.939910889 CET	60100	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:22.990775108 CET	53	60100	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:47:23.948967934 CET	53195	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:23.996879101 CET	53	53195	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:25.050247908 CET	50141	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:25.111639023 CET	53	50141	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:26.115879059 CET	53023	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:26.166889906 CET	53	53023	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:27.256735086 CET	49563	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:27.306660891 CET	53	49563	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:28.878331900 CET	51352	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:28.926213026 CET	53	51352	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:30.524794102 CET	58823	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:30.575351954 CET	53	58823	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:30.623920918 CET	57568	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:30.624138117 CET	50540	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:30.628294945 CET	54366	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:30.628612041 CET	53034	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:30.689516068 CET	53	50540	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:30.693150997 CET	53	54366	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:30.693430901 CET	53	57568	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:30.705569029 CET	53	53034	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:31.115874052 CET	57762	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:31.181266069 CET	53	57762	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:31.307795048 CET	55435	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:31.379225016 CET	53	55435	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:31.490367889 CET	56132	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:31.543423891 CET	53	56132	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:31.663701057 CET	58987	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:31.728101969 CET	53	58987	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:32.435656071 CET	56579	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:32.442946911 CET	60633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:32.499241114 CET	53	60633	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:32.513282061 CET	53	56579	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:32.687589884 CET	61292	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:32.735769987 CET	53	61292	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:33.438821077 CET	63619	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:33.486563921 CET	53	63619	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:33.595076084 CET	64938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:33.643166065 CET	53	64938	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:33.869086981 CET	61946	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:33.928261042 CET	53	61946	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:35.585814953 CET	56338	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:35.650738001 CET	53	56338	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:36.144079924 CET	59420	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:36.202025890 CET	53	59420	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:36.756105900 CET	58784	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:36.814399004 CET	53	58784	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:38.190459013 CET	63978	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:38.248106956 CET	53	63978	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:51.665954113 CET	57145	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:51.713953018 CET	53	57145	8.8.8.8	192.168.2.3
Jan 27, 2021 19:47:53.522362947 CET	55359	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:54.527858973 CET	55359	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:55.550522089 CET	55359	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:47:55.611095905 CET	53	55359	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:10.672348022 CET	58306	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:10.730530024 CET	53	58306	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:11.786562920 CET	64124	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:11.836229086 CET	53	64124	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:19.791271925 CET	49361	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:19.852200031 CET	53	49361	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:28.457508087 CET	63150	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:28.524290085 CET	53	63150	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:28.562215090 CET	56881	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:28.622013092 CET	53	56881	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:48:28.994220972 CET	53642	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:29.050826073 CET	53	53642	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:29.199470997 CET	55667	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:29.203681946 CET	54833	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:29.260183096 CET	53	54833	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:29.266525984 CET	53	55667	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:29.400106907 CET	62476	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:29.437880039 CET	49705	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:29.460211992 CET	53	62476	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:29.494297981 CET	53	49705	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:29.527295113 CET	61477	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:29.595665932 CET	53	61477	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:29.841162920 CET	61633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:29.899817944 CET	53	61633	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:30.350339890 CET	55949	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:30.410562992 CET	53	55949	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:31.153475046 CET	57601	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:31.205676079 CET	53	57601	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:31.932194948 CET	49342	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:31.985415936 CET	53	49342	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:33.056596041 CET	56253	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:33.118138075 CET	53	56253	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:33.784943104 CET	49667	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:33.856787920 CET	53	49667	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:33.877764940 CET	55439	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:33.939102888 CET	53	55439	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:34.793088913 CET	57069	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:34.854268074 CET	53	57069	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:35.277106047 CET	57659	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:35.333488941 CET	53	57659	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:51.996031046 CET	54717	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:52.069792986 CET	53	54717	8.8.8.8	192.168.2.3
Jan 27, 2021 19:48:55.319896936 CET	63975	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:48:55.367944002 CET	53	63975	8.8.8.8	192.168.2.3
Jan 27, 2021 19:49:16.210984945 CET	56639	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:49:16.263638973 CET	53	56639	8.8.8.8	192.168.2.3
Jan 27, 2021 19:49:26.334052086 CET	51856	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:49:26.398202896 CET	53	51856	8.8.8.8	192.168.2.3
Jan 27, 2021 19:49:26.824150085 CET	56546	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:49:26.891480923 CET	53	56546	8.8.8.8	192.168.2.3
Jan 27, 2021 19:49:30.351928949 CET	62152	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:49:30.413022041 CET	53	62152	8.8.8.8	192.168.2.3
Jan 27, 2021 19:50:03.488518953 CET	53470	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:50:03.555599928 CET	53	53470	8.8.8.8	192.168.2.3
Jan 27, 2021 19:50:03.680880070 CET	56446	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:50:03.737467051 CET	53	56446	8.8.8.8	192.168.2.3
Jan 27, 2021 19:50:07.555345058 CET	59631	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:50:07.619725943 CET	53	59631	8.8.8.8	192.168.2.3
Jan 27, 2021 19:50:07.755954981 CET	55515	53	192.168.2.3	8.8.8.8
Jan 27, 2021 19:50:07.812408924 CET	53	55515	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 19:47:30.623920918 CET	192.168.2.3	8.8.8.8	0x6319	Standard query (0)	nodes.smsmail.net	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:31.663701057 CET	192.168.2.3	8.8.8.8	0x5e2e	Standard query (0)	miacndapmamaslpot.firebaseapp.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:32.687589884 CET	192.168.2.3	8.8.8.8	0xa561	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:33.595076084 CET	192.168.2.3	8.8.8.8	0x9cff	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:35.585814953 CET	192.168.2.3	8.8.8.8	0xbeca	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 19:47:36.144079924 CET	192.168.2.3	8.8.8.8	0xd464	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:36.756105900 CET	192.168.2.3	8.8.8.8	0xc22b	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 19:47:30.693430901 CET	8.8.8.8	192.168.2.3	0x6319	No error (0)	nodes.smsmail.net		104.21.19.54	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:30.693430901 CET	8.8.8.8	192.168.2.3	0x6319	No error (0)	nodes.smsmail.net		172.67.185.66	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:31.728101969 CET	8.8.8.8	192.168.2.3	0x5e2e	No error (0)	miacndapmamaslpot.firebaseapp.com		151.101.1.195	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:31.728101969 CET	8.8.8.8	192.168.2.3	0x5e2e	No error (0)	miacndapmamaslpot.firebaseapp.com		151.101.65.195	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:32.735769987 CET	8.8.8.8	192.168.2.3	0xa561	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:32.735769987 CET	8.8.8.8	192.168.2.3	0xa561	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:32.735769987 CET	8.8.8.8	192.168.2.3	0xa561	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:32.735769987 CET	8.8.8.8	192.168.2.3	0xa561	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:32.735769987 CET	8.8.8.8	192.168.2.3	0xa561	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:33.643166065 CET	8.8.8.8	192.168.2.3	0x9cff	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:33.643166065 CET	8.8.8.8	192.168.2.3	0x9cff	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:35.650738001 CET	8.8.8.8	192.168.2.3	0xbeca	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:47:35.650738001 CET	8.8.8.8	192.168.2.3	0xbeca	No error (0)	googlehosted.l.googleusercontent.com		172.217.22.225	A (IP address)	IN (0x0001)
Jan 27, 2021 19:47:36.202025890 CET	8.8.8.8	192.168.2.3	0xd464	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:47:36.814399004 CET	8.8.8.8	192.168.2.3	0xc22b	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5216 Parent PID: 2052

General

Start time:	19:47:27
Start date:	27/01/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\ID4380.htm'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 2168 Parent PID: 5216

General

Start time:	19:47:28
Start date:	27/01/2021
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=1504,3014448195932754039,17643246837121573947,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1900 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly