ID: 364051
Sample Name:
audio_cheri.riley@treetop.com_file.htm
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 19:04:57
Date: 05/03/2021
Version: 31.0.0 Emerald

Table of Contents

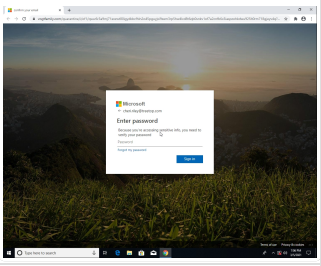
Analysis Report audio_cheri.riley@treetop.com_file.htm

Overview

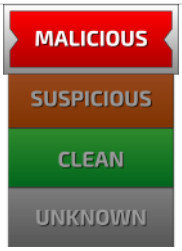
General Information

Sample Name:	audio_cheri.riley@treetop.com_file.htm
Analysis ID:	364051
MD5:	ce5eab4d11db52..
SHA1:	973c43de204871..
SHA256:	bae99731991ee7..
Infos:	

Most interesting Screenshot:



Detection



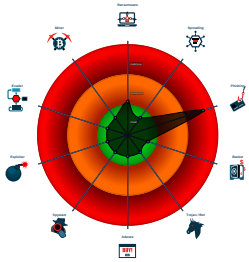
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Yara detected HtmlPhish_3
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6868 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\audio_cheri.riley@treetop.com_file.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7116 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1504,3313749393455400725,13859779750281236468,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1852 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

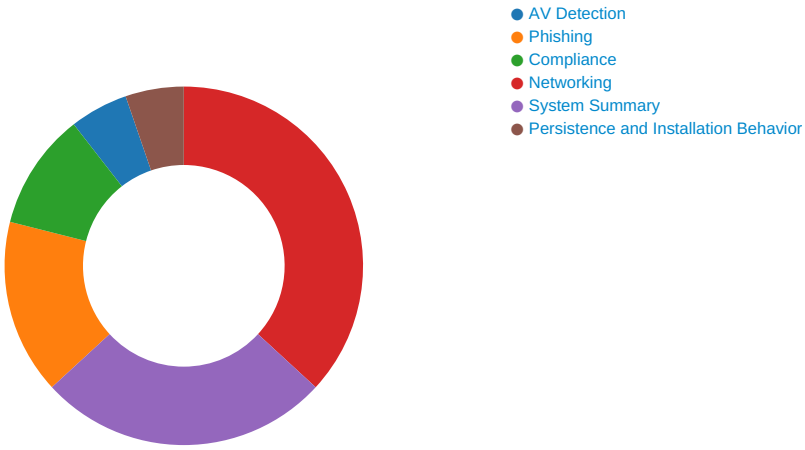
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Yara detected HtmlPhish_3

Compliance:

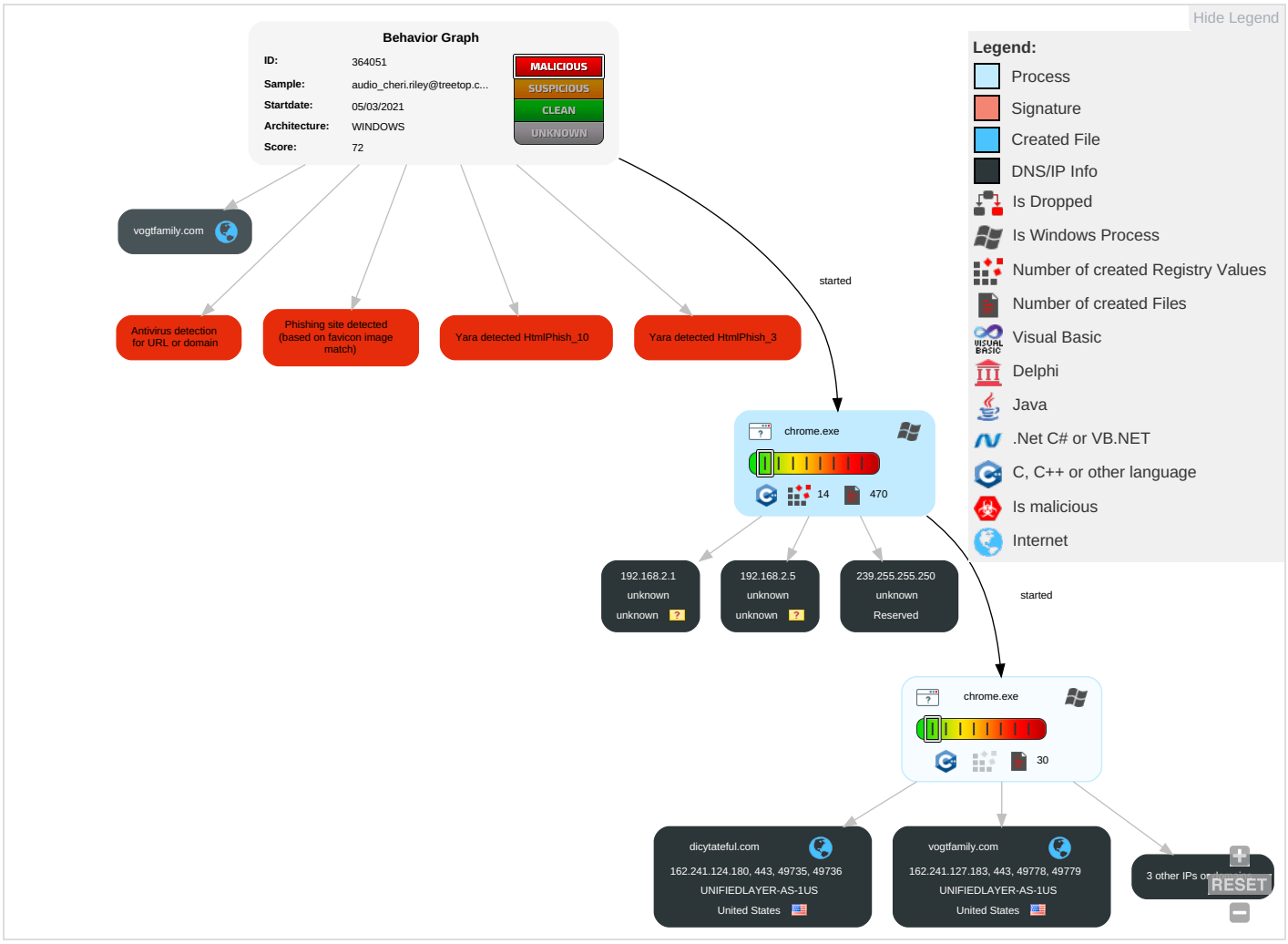
Creates license or readme file

Uses secure TLS version for HTTPS connections

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 1	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

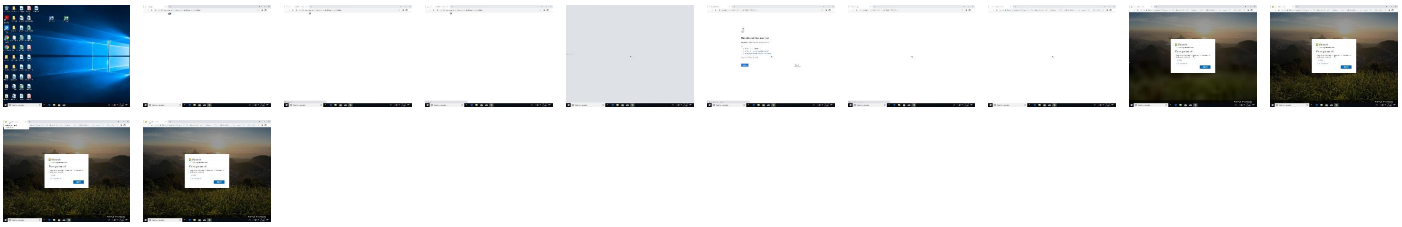
Behavior Graph

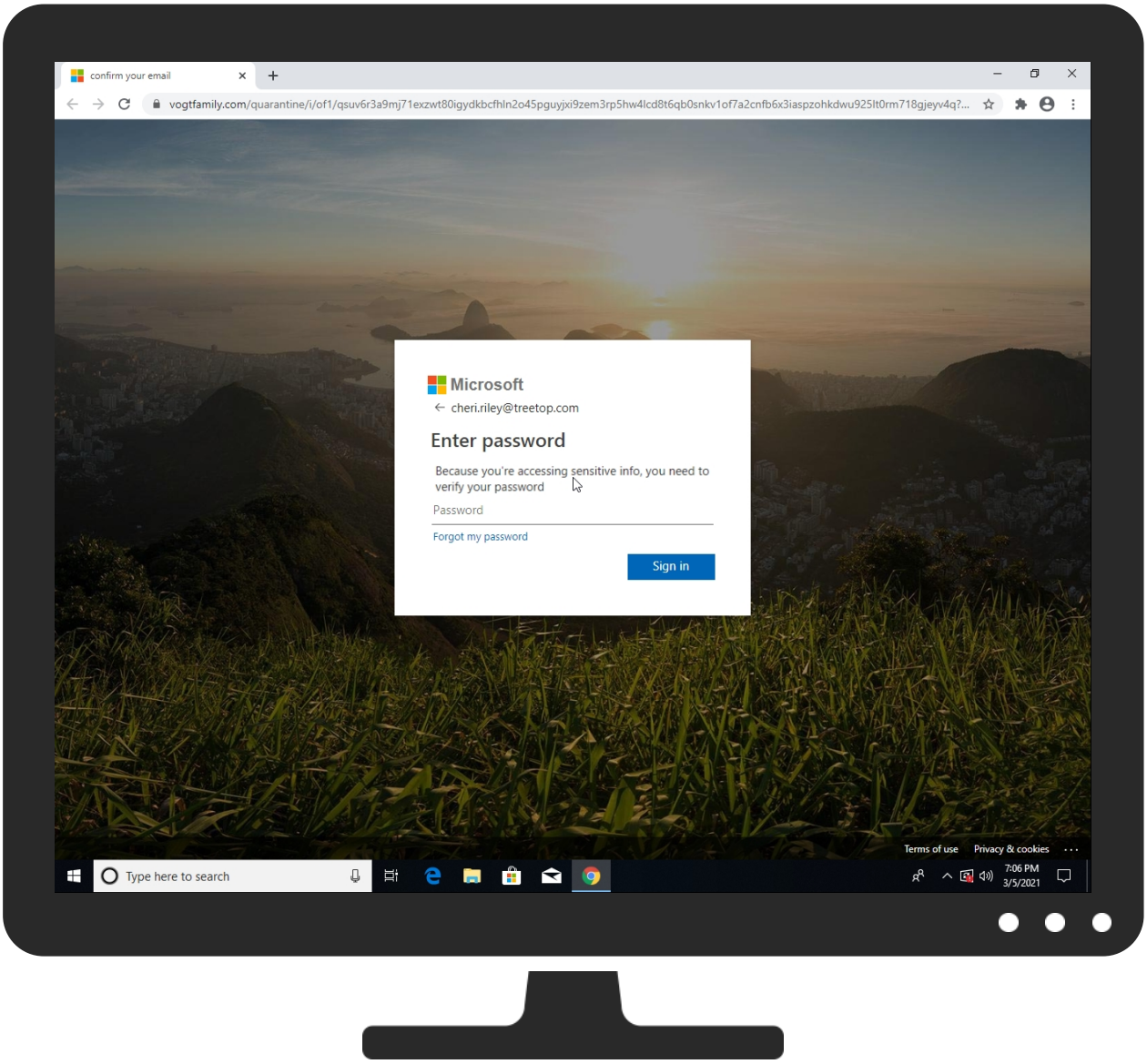


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
vogtfamily.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://vogtfamily.com/quarantine/i/of1/qsuv6r3a9mj71exzwt80igydkbcfhln2o45pguyjxi9zem3rp5hw4lcd8t6qb0snkv1of7a2cnfb6x3iaspzohkdwu925lt0rm718gjeyv4q?data=Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://dns.google	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dicytateful.com/l.html#Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=	0%	Avira URL Cloud	safe	
http://https://vogtfamily.com/quarantine/i/of1/?Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=D	0%	Avira URL Cloud	safe	
http://https://dicytateful.com/l.html#Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=confirm	0%	Avira URL Cloud	safe	
http://https://vogtfamily.com/quarantine/i/of1/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://vogtfamily.com/quarantine/i/of1?Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=	0%	Avira URL Cloud	safe	
http://https://vogtfamily.com/	0%	Avira URL Cloud	safe	
http://https://vogtfamily.com/quarantine/i/of1/qsuv6r3a9mj71exzwt80igydkbcfhln2o45pguyjxi9zem3rp5hw4lcd8t6q	0%	Avira URL Cloud	safe	
http://https://vogtfamily.com/quarantine/i/of1?Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=confirm	0%	Avira URL Cloud	safe	
http://https://vogtfamily.com/quarantine/i/of1/?Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=confirm	0%	Avira URL Cloud	safe	
http://https://vogtfamily.com/quarantine/i/of1/?Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=	0%	Avira URL Cloud	safe	
http://https://dicytateful.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vogtfamily.com	162.241.127.183	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.23.33	true	false		high
dicytateful.com	162.241.124.180	true	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

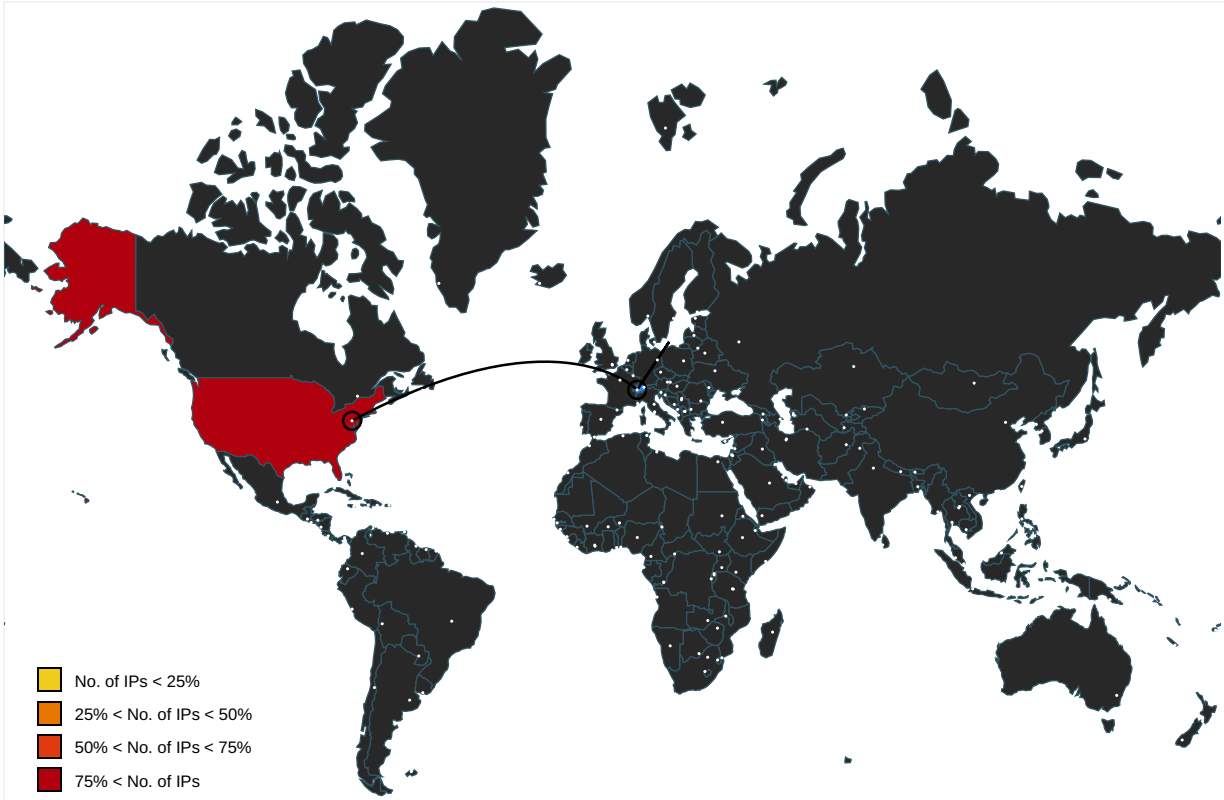
Name	Malicious	Antivirus Detection	Reputation
http://https://vogtfamily.com/quarantine/i/of1/qsuv6r3a9mj71exzwt80igydkbcfhln2o45pguyjxi9zem3rp5hw4lcd8t6qb0snkv1of7a2cnfb6x3iaspzohkdwu925lt0rm718gjeyv4q?data=Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	df837a08-30f9-4c60-8265-aa263f6953ee.tmp.2.dr, afefa4c5-16a6-4350-a4d8-b69a1dfc878d.tmp.2.dr, f9608479-6dc8-4552-aa92-e0e24261c17f.tmp.2.dr, 2222edd6-a419-4dee-b830-adedae1c0abc.tmp.2.dr, d7cf1098-11e2-443c-996f-03c8a71426e7.tmp.2.dr, 946eb2dc-2451-4e87-b2fe-abfded2a8b72.tmp.2.dr, 21e667a9-1214-4ca0-9a39-2ebabc452c46.tmp.2.dr, 58943f74-7189-4396-8315-607374d71848.tmp.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dicytateful.com/l.html#Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=	Current Session.0.dr, Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://vogtfamily.com/quarantine/i/of1/?Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=D	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dicytateful.com/l.html#Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=confirm	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://vogtfamily.com/quarantine/i/of1/images/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://vogtfamily.com/quarantine/i/of1?Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://vogtfamily.com/	Network Action Predictor.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://vogtfamily.com/quarantine/i/of1/qsuv6r3a9mj71exzwt80igydkbcfhln2o45pguyjxi9zem3rp5hw4lcd8t6q	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://vogtfamily.com/quarantine/i/of1?Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=confirm	History.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients2.googleusercontent.com	afefa4c5-16a6-4350-a4d8-b69a1d fc878d.tmp.2.dr, 2222edd6-a419-4dee-b830-adedae1c0abc.tmp.2.dr, d7cf1098-11e2-443c-996f-03c8a71426e7.tmp.2.dr, 946eb2dc-2451-4e87-b2fe-abfde d2a8b72.tmp.2.dr	false		high
http://https://vogtfamily.com/quarantine/i/of1/?Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=confirm	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://vogtfamily.com/quarantine/i/of1/?Y2hlcmkucmlsZXlAdHJlZXRvcC5jb20=	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dicytateful.com	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.127.183	vogtfamily.com	United States		46606	UNIFIEDLAYER-AS-1US	false
162.241.124.180	dicytateful.com	United States		46606	UNIFIEDLAYER-AS-1US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.23.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	364051

Start date:	05.03.2021
Start time:	19:04:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	audio_cheri.riley@treetop.com_file.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:	17
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:	mal72.phis.winHTM@42/191@4/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 168.61.161.212, 104.42.151.234, 172.217.20.238, 172.217.22.237, 172.217.22.206, 74.125.173.39, 216.58.207.163, 172.217.23.42, 172.217.23.74, 172.217.22.202, 172.217.22.234, 216.58.207.138, 216.58.207.170, 104.43.139.144, 40.88.32.150, 13.88.21.125, 104.43.193.48, 172.217.20.227, 51.104.139.180, 205.185.216.42, 205.185.216.10, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 74.125.173.28, 74.125.173.232, 173.194.163.75, 20.82.209.183, 173.194.187.103, 173.194.187.198, 173.194.188.6, 74.125.173.55, 173.194.163.76 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, r1---sn-4g5e6nze.gvt1.com, clientservices.googleapis.com, r2.sn-4g5e6nsr.gvt1.com, r1.sn-4g5ednll.gvt1.com, skypedataprdcoleus15.cloudapp.net, r1---sn-4g5e6nlk.gvt1.com, clients2.google.com, r3.sn-4g5ednz7.gvt1.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, r6.sn-4g5ednls.gvt1.com, r1.sn-4g5e6nze.gvt1.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, www.googleapis.com, r2---sn-4g5e6nsr.gvt1.com, r6---sn-4g5ednls.gvt1.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, r3---sn-4g5ednz7.gvt1.com, r1---sn-4g5edns7.gvt1.com, r6.sn-4g5e6nld.gvt1.com, r5---sn-4g5ednls.gvt1.com, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, redirector.gvt1.com, r5.sn-4g5ednls.gvt1.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, accounts.google.com, r1.sn-4g5edns7.gvt1.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, r1.sn-4g5e6nlk.gvt1.com, r1---sn-4g5ednll.gvt1.com, skypedataprdcoleus17.cloudapp.net, r6---sn-4g5e6nld.gvt1.com, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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

Time	Type	Description
19:06:12	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
239.255.255.250	March 4, 2021, 055038 PM.HTM	Get hash	malicious	Browse	
	MRS.exe	Get hash	malicious	Browse	
	equinitiTicket#51347303511505986.htm	Get hash	malicious	Browse	
	_evm5437345.htm	Get hash	malicious	Browse	
	March 4, 2021, 021638 PM.HTM	Get hash	malicious	Browse	
	PaymentConfirmation_9QE1-NSSB8U-CHF3.htm	Get hash	malicious	Browse	
	New Invoice.PDF.htm	Get hash	malicious	Browse	
	Intruder.exe	Get hash	malicious	Browse	
	Invoice 76221 Secured_Pdf_brianc@johnstoncompanies .com.html	Get hash	malicious	Browse	
	holla.htm	Get hash	malicious	Browse	
	UPS Delivery Notification, Receiver susiej@johnsto ncompanies.com.html	Get hash	malicious	Browse	
	wzdu53.exe	Get hash	malicious	Browse	
	wzdu53.exe	Get hash	malicious	Browse	
	remit726498.htm	Get hash	malicious	Browse	
	Xero from wellbeingsoftware.htm	Get hash	malicious	Browse	
	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKe ep.htm	Get hash	malicious	Browse	
	#Ud83d#UdcdeMichelle.bloxham.htm	Get hash	malicious	Browse	
	selfassessment.doc	Get hash	malicious	Browse	
	Xeros from ecommpay.htm	Get hash	malicious	Browse	
	BL.html	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	73uhuBCLi6.exe	Get hash	malicious	Browse	• 192.185.19 6.170
	ParcelDL7593462.doc	Get hash	malicious	Browse	• 192.185.11 3.122
	Huda Company Profile.doc	Get hash	malicious	Browse	• 192.185.19 6.170
	eeb4BBNsTR.exe	Get hash	malicious	Browse	• 50.116.93.102
	igw7oUEmTY.dll	Get hash	malicious	Browse	• 162.241.20 4.234
	new order.exe	Get hash	malicious	Browse	• 192.254.18 0.165
	hb4XWZKUGa.dll	Get hash	malicious	Browse	• 162.241.20 4.234
	ixyuzTLo3J.dll	Get hash	malicious	Browse	• 162.241.20 4.234
	9Vg3FVqP9b.dll	Get hash	malicious	Browse	• 162.241.20 4.234
	Datos factura.doc	Get hash	malicious	Browse	• 162.241.15 5.200
	PO.41000055885.exe	Get hash	malicious	Browse	• 74.220.219.171
	ryBnPtMPIR.dll	Get hash	malicious	Browse	• 162.241.20 4.234
	CBIMcKSkQR.dll	Get hash	malicious	Browse	• 162.241.20 4.234
	cQJzHE4wYW.dll	Get hash	malicious	Browse	• 162.241.20 4.234
	777qAhQFJq.dll	Get hash	malicious	Browse	• 162.241.20 4.234
	K69VT3tcaL.dll	Get hash	malicious	Browse	• 162.241.20 4.234
	YBkyjD4N0E.dll	Get hash	malicious	Browse	• 162.241.20 4.234

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TAG5TYzh37.dll	Get hash	malicious	Browse	• 162.241.204.234
	overdue_account.exe	Get hash	malicious	Browse	• 192.185.226.148
	9voSrqd0o4.dll	Get hash	malicious	Browse	• 162.241.204.234
UNIFIEDLAYER-AS-1US	73uhuBCLi6.exe	Get hash	malicious	Browse	• 192.185.196.170
	ParcelDL7593462.doc	Get hash	malicious	Browse	• 192.185.113.122
	Huda Company Profile.doc	Get hash	malicious	Browse	• 192.185.196.170
	eeb4BBNsTR.exe	Get hash	malicious	Browse	• 50.116.93.102
	igw7oUEmTY.dll	Get hash	malicious	Browse	• 162.241.204.234
	new order.exe	Get hash	malicious	Browse	• 192.254.180.165
	hb4XWZKUGa.dll	Get hash	malicious	Browse	• 162.241.204.234
	ixyuzTLo3J.dll	Get hash	malicious	Browse	• 162.241.204.234
	9Vg3FVqP9b.dll	Get hash	malicious	Browse	• 162.241.204.234
	Datos factura.doc	Get hash	malicious	Browse	• 162.241.155.200
	PO.41000055885.exe	Get hash	malicious	Browse	• 74.220.219.171
	ryBnPtMPIR.dll	Get hash	malicious	Browse	• 162.241.204.234
	CBIMcKSkQR.dll	Get hash	malicious	Browse	• 162.241.204.234
	cQJzHE4wYW.dll	Get hash	malicious	Browse	• 162.241.204.234
	777qAhQFJq.dll	Get hash	malicious	Browse	• 162.241.204.234
	K69VT3tcaL.dll	Get hash	malicious	Browse	• 162.241.204.234
	YBkyjD4N0E.dll	Get hash	malicious	Browse	• 162.241.204.234
	TAG5TYzh37.dll	Get hash	malicious	Browse	• 162.241.204.234
	overdue_account.exe	Get hash	malicious	Browse	• 192.185.226.148
	9voSrqd0o4.dll	Get hash	malicious	Browse	• 162.241.204.234

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Amazon_Order_Confirmation#OR54389L4GT.exe	Get hash	malicious	Browse	• 162.241.127.183
	tsyv3x6l9x.doc	Get hash	malicious	Browse	• 162.241.127.183
	aHPAHpmYmy.doc	Get hash	malicious	Browse	• 162.241.127.183
	hdFITQcUNH.doc	Get hash	malicious	Browse	• 162.241.127.183
	POCS1570.xlsx	Get hash	malicious	Browse	• 162.241.127.183
	P18gSPEiT7.exe	Get hash	malicious	Browse	• 162.241.127.183
	nhiZa1aKSi.exe	Get hash	malicious	Browse	• 162.241.127.183
	s2qBa23HqR.exe	Get hash	malicious	Browse	• 162.241.127.183
	Paid561571.htm	Get hash	malicious	Browse	• 162.241.127.183
	midterm_problem1.exe	Get hash	malicious	Browse	• 162.241.127.183
	midterm_problem1.exe	Get hash	malicious	Browse	• 162.241.127.183
	PDC_156280_5635_ALF.xlsx	Get hash	malicious	Browse	• 162.241.127.183
	equinitiTicket#51347303511505986.htm	Get hash	malicious	Browse	• 162.241.127.183

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	condiz_03.21.doc	Get hash	malicious	Browse	• 162.241.127.183
	pago de documento de pedido.exe	Get hash	malicious	Browse	• 162.241.127.183
	remmittance859405__.htm	Get hash	malicious	Browse	• 162.241.127.183
	SecuriteInfo.com.Variant.Midie.79660.31247.exe	Get hash	malicious	Browse	• 162.241.127.183
	WinRAR_1845561462.exe	Get hash	malicious	Browse	• 162.241.127.183
	annualreport.xlsx	Get hash	malicious	Browse	• 162.241.127.183
	Weekly Vacancy Status Report.xlsm	Get hash	malicious	Browse	• 162.241.127.183

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.11466556781601
Encrypted:	false
SSDEEP:	6:kK1tbwTJ6YN+SkQlPlEGYRMY9z+4KlDA3RUe0ht:XbwTJ6HkPlE99SNxAhUe0ht
MD5:	5C1860CF4522993905D5C424F7787008
SHA1:	6E83CF85CFAF8808A5D562B66A7A014FDB96C47C
SHA-256:	881F9028D3FD83F3DF8E9EAD9BC73ED037607DC5BF190EF2CD4A03CFA7B5E6E5
SHA-512:	62670ABC75D713FD0C6A592B3E226EBFDEA525463C76D07C49527670499F3811EF40A27A860AA6EE2F10A95C749D8F65E7EFA78E44DDEB01E3D87AAC18FD2C0
Malicious:	false
Reputation:	low
Preview:	p..... .....:....(..... .....$.....h.t.t.p.:.//./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\1ebbde17-9a82-41c3-a7bb-289361c56cfa.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428

C:\Users\user\AppData\Local\Google\Chrome\User Data\1ebbde17-9a82-41c3-a7bb-289361c56cfa.tmp	
Entropy (8bit):	3.744654124319603
Encrypted:	false
SSDEEP:	384:tbhCG4fdwn8CV3pGFN6rvvuW3lugRH8xGhIrjgqwxNEYALrzGm/L9DQa+GFOEoW3:92CVBSQQpMebQSoEXv2SK4Gap5
MD5:	2983CD3D4924F9E1580CACD26B4F2340
SHA1:	5BD07B41F63169E4A99D073442E3EA52957AEE29
SHA-256:	BEC9DE814FE6B04CB549C50B5AD0EB04F63736459B8F60EEBBBC1D678A42F2B8
SHA-512:	21B4805769AB2D14D9AD558477B4F7FA70630789A839F74F4992757A2E73D14E8EFB205F0967BD9391749B8A727B96BD4C02935250212CD0233C63C0DB17DBF4
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...j38.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\1ec7e948-9292-4d08-a74d-07e932d3320d.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):	157072
Entropy (8bit):	6.05280046983719
Encrypted:	false
SSDEEP:	3072:cwe9QSr571ljD6v2CcDPvZaerlibFcbXafIB0u1GOJmA3iuRN:1AQwh1xFTJ4kaqfIlUOoSiuRN
MD5:	48A707B450295362C62AB6F59BF28BBF
SHA1:	6A7BCE14531AE557B4CADC8BC14DED29B3A20814
SHA-256:	AAC7966DD0EC637BF1F3BAF9AA4066257419E12CD5F189154E9E27C19851089C
SHA-512:	F453CD5EA3BF027130A9042AB2D8EF03AC137CABB4D1AADB23AFD1374035C075E78D0E3536FFD62720A72CB7480CF0E578B73EDBF775FF5BAC5A31DB163F67 EB
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxA AAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Os h5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2P KkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":

C:\Users\user\AppData\Local\Google\Chrome\User Data\36b7f1ac-a990-4327-ab64-286194a43c79.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):	165130
Entropy (8bit):	6.081772181624107
Encrypted:	false
SSDEEP:	3072:+lawe9QSr571ljD6v2CcDPvZaerlibFcbXafIB0u1GOJmA3iuRN:QTAQwh1xFTJ4kaqfIlUOoSiuRN
MD5:	D414DB0B49E365E80E76C3AAE3BBA9C4
SHA1:	A7DA157BED3D72EC6DD53BABEB8DA8A51291E3F6
SHA-256:	2BC0B43051C39112FF29FE3A5FFCE1DD871E587A1786F19E0B4ED1A65D554DD1
SHA-512:	531C70F6B4EDC6168D435BA2D6FC0DA379BC189842CBCFA5DBF53E7427A8453C4094765F83824C41C1522424EEB9E7C901160814015BE5C93099321CE283380A
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"os_crypt":{"encrypted_key": "RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiL GeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwR gUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_ manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\4871bfac-8d01-4056-83f8-87c710154a8a.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):	165130
Entropy (8bit):	6.08177135859063

C:\Users\user\AppData\Local\Google\Chrome\User Data\4871bfac-8d01-4056-83f8-87c710154a8a.tmp	
Encrypted:	false
SSDEEP:	3072:+n9we9QSr571ljD6v2CcDPvZaerIibFcbXafIB0u1GOJmA3iuRN:qeAQwh1xFTJ4kaqfIlUOoSiuRN
MD5:	A24C93FEAE623BE408A88C4FD3A86420
SHA1:	2C573EE7B8E635EF682C132C038B0F9B4928B870
SHA-256:	A80B9A3A7B36404953A3512D6CB8BC63DCE99F347FFC6394DC2E8F68264F1889
SHA-512:	308672E8518883A2C73B6E809A3250D304EB409B9D0DDB72CAB23BCC9E8D249092F52248F503226AA373789CDEB4A3269CAE6EE8E21DA3A667B77820A203744
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6bkTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\4a772cdf-1c2f-4ef7-8441-d1edaed9138a.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):	157342
Entropy (8bit):	6.053464927070266
Encrypted:	false
SSDEEP:	3072:dwe9QSr571ljD6v2CcDPvZaerIibFcbXafIB0u1GOJmA3iuRN:+AQwh1xFTJ4kaqfIlUOoSiuRN
MD5:	C6287FED4D0F8B3CAD8B4835AE4368CD
SHA1:	C931FC38E1505D7252D0121F7D8D05266244299F
SHA-256:	70BF6C985A19F50F2BCA7F275478561C73121847102F8F3718B9AD6AA3FAFBA3
SHA-512:	F9B222A5E1F912427A3E2940FB5098AA4853881BB73220E2568428B18B9AA610EB2826B2439E34670EEBFAFD931E134070184974D39996FA8AB637509DC94875
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6bkTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":

C:\Users\user\AppData\Local\Google\Chrome\User Data\4c790279-8e8d-4147-bfab-d8b940e1477d.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):	157250
Entropy (8bit):	6.053212213706335
Encrypted:	false
SSDEEP:	3072:owe9QSr571ljD6v2CcDPvZaerIibFcbXafIB0u1GOJmA3iuRN:pAQwh1xFTJ4kaqfIlUOoSiuRN
MD5:	7564F4924BB29D6EEF85ED3FFA20E8E3
SHA1:	F2761961852B3823E03510FA969FE3E935C27F67
SHA-256:	39381BF71432CD16E81C4E55CE71556C34EC5CE01A650609ABD2E3DF234C0566
SHA-512:	5BF0FD1E7568056719D0DEAB645B1210CC5AF34CE4255D924AC192299FC139420A230A89A6A15AEC91B6AA7BB8AC383D43952DE2A10FF0CA42157FAE1CCB1A66
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6bkTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":

C:\Users\user\AppData\Local\Google\Chrome\User Data\634d9193-9bbc-40af-bd93-d9aace816ec8.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):	165130
Entropy (8bit):	6.081772579614283
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\634d9193-9bbc-40af-bd93-d9aace816ec8.tmp	
SSDEEP:	3072:ylrwe9QSr571ljD6v2CcDPvZaerlibFcbXafIB0u1GOJmA3iuRN:EcAQwh1xFTJ4kaqfIlUOoSiuRN
MD5:	1DEBDF86049654537A18A0DACB02E67B
SHA1:	306A44FB486A548362950AEE621F014E9F2A184F
SHA-256:	DE693ED0D6A3AE5AD4570943D5D36E16C8FC370E9D7A3BDCD3C18C0ADD95AFE5
SHA-512:	FCC6F4767103499813DC4AD26FB95B3848296DA48DDEFF4892D7044C512D22A787175FE7FE9A55082FA501C2C092D072884A199481415B68481914A210FFC713
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715593430"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\6bce22a0-9319-48be-8603-6c1a8032c41f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.74487704256072
Encrypted:	false
SSDEEP:	384:9bhCG4fdwn8CV3pGFN6rvvuW3lugRH8xGhIrjgqwxNEYALrzGm/kDQa+GFOEoWNf:t2CVBSQtpMebQSoEXv2SK4GapP
MD5:	B71794CE2AA37BB3E5AB1C35CF003ED1
SHA1:	C9A0506CEC4C316BDDF37DD6D87A07FD0FF52A46
SHA-256:	33F702A5627AB84BCC573FAA492DCF3EFE392BFB0D36C9B4F6075A16B25DE0CD
SHA-512:	05B27DF4A5F5697BDA494722FA022CF47BE8044DF9D3F5CBD0B6950E10FAE58DB814A624E6D1BD91FCCE173CFD89ACE0C42A3CB3ED8ACF4B3C3019840969395
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...j38.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\8d3b3211-a131-49e7-b213-955f15092e5a.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):	156746
Entropy (8bit):	6.051943257994218
Encrypted:	false
SSDEEP:	3072:rwe9QSr571ljD6v2CcDPvZaerlibFcbXafIB0u1GOJmA3iuRN:cAQwh1xFTJ4kaqfIlUOoSiuRN
MD5:	D0857239E887D6A81699695DBBBBF0ED
SHA1:	FC4AAC94A04E853D90E17D58DB53A8E02F107112
SHA-256:	DEA270DE89C211DA50BE339024ED233459F7EEEB5361FF9E365395FB3DEDAF6B
SHA-512:	94DC6D3AFD0C631527D050A10E4298AA1158D49412F011882711331A8C28C75D572EC14D887BD649500E0539F7ADF1246D233B4529B650B5A26DFBA5A745686E
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715593430"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\91b738a5-14ed-4e5d-8c5c-54f6da51cbd7.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):	165130
Entropy (8bit):	6.081772459842341
Encrypted:	false
SSDEEP:	3072:+lrwe9QSr571ljD6v2CcDPvZaerlibFcbXafIB0u1GOJmA3iuRN:QcAQwh1xFTJ4kaqfIlUOoSiuRN

C:\Users\user\AppData\Local\Google\Chrome\User Data\91b738a5-14ed-4e5d-8c5c-54f6da51cbd7.tmp	
MD5:	8CED04ACC5EB848929E537134CC5AB40
SHA1:	22004BE05D30FF51FA7815ED67587566DE1F7A55
SHA-256:	4530A3E707C0D2A0FC0E0D819B7C69E25098277FFED44F04AB4FE8A0773D3776
SHA-512:	BA167CF6CA7A6CA742250EEBA47EA85E9E6284AE1ACDFB80526727086336987BA54AFFB9332B6BA754DCEC8059044320B4C32070A89C2487FA4B112344BABDA E
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\92919595-9f76-42a6-bfcb-f55dd999a1ae.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):	157156
Entropy (8bit):	6.052950942244401
Encrypted:	false
SSDEEP:	3072:8we9QSr571ljD6v2CcDPvZaerIibFcbXafIB0u1GOJmA3iuRN:VAQwh1xFTJ4kaqfIlUOoSiuRN
MD5:	0A2BF490C15D345CAD4BAAE484BA4623
SHA1:	20E47CB9542F4080769CE9FECD4D7BAA71181CC3
SHA-256:	DBE28829F08CB5CEA5983231D03E974BD844F256339C3E01F333D37D558C3DF7
SHA-512:	AAD185581DFC8194BB0A03CE3C9830CD384F9E6973D49C21A03E267EDBB6CE0E45B7E8D4BA1BDF2897C1D5EECD471B8643766E815445D737595D5D5F07DCF FB
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":

C:\Users\user\AppData\Local\Google\Chrome\User Data\9c689873-e577-4a73-95dc-40852c18fb6a.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):	156642
Entropy (8bit):	6.051627714261319
Encrypted:	false
SSDEEP:	3072:iwe9QSr571ljD6v2CcDPvZaerIibFcbXafIB0u1GOJmA3iuRN:bAQwh1xFTJ4kaqfIlUOoSiuRN
MD5:	EE54F4D14B12161C68766AC77413F6D7
SHA1:	0EA404FF4AE8A5A96E228E92EDE5ADAA10B32BD5
SHA-256:	4409B0510B4810CA1F7378C1CFC0C2BD6A75024DB84CA1E57FC9993E166EA845
SHA-512:	BD75FB65430D74C03A52A52D055D4232AE2DCD519DCA528135D464D3ED8D1AF95528D0A5320E29D06F4B6CAF2857DBFCC5938E016C1210A9AEB19BEF8B1CA 86
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715593430"},"plugins":{"metadata":{"adobe-flash-player":{"d

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):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2222edd6-a419-4dee-b830-adedae1c0abc.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):	3473
Entropy (8bit):	4.884897250513757
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhd:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSa
MD5:	A1CDBC88F8B4CC8D10212775766B42CF
SHA1:	895505AE442DC20942D1D7A5094B01E3DCE208F4
SHA-256:	AFB41143BF853D6784565FA685200B22EC79DFE2A846E8C774C1D4CBD5A9C82D
SHA-512:	E12E2260702115347A053A6A323732901D440C5D391041AFD7920FCEF6AC53BF2C6376E0651F4A6BBB2A6F8DFED7C56BAD8EA7131C85A8B5B676C9CAA71F1D2F
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\946eb2dc-2451-4e87-b2fe-abfded2a8b72.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):	1725
Entropy (8bit):	4.848754647780584
Encrypted:	false
SSDEEP:	48:Y2nzMK6qDHGXCtwWshmRLsh0DshuyKshK3gYhbp:JnzMKxDHGXCOe15Vxhd
MD5:	0A4686136E3560B4C82191AFE821EF0C
SHA1:	988E8EC2ED39255E81A9505EFD31DE8A8CE7E2C4
SHA-256:	4F52F8F93E0A0DE68B0F758BFB909CAED78882A8CBD5973FA285E58995EE2A10
SHA-512:	6A08D1E76C1DAFCA572BCFE8D48AB347A10F4E8C85845F1E74995BCEC0F833A0A4537CF5D250478303CC8BC93B5DE7440366279D7F428DCE6CDB704DC804113
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13262033147506011","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{

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):	5.2757277380796355
Encrypted:	false
SSDEEP:	6:mn5sh39+q2Pwkn23iKKdK9RXXTZIFUtpW5ehJZmwPW5eh9VkwOwkn23iKKdK9RX3:mc9+vYf5Kk7XT2FUtpWMhJ/PWMh9V5J3
MD5:	037A0E9EF192AABC979A6DCCC40C233E
SHA1:	107F030551A18760B12C7C89EDB5FB0E1294DC49
SHA-256:	86DB8F59CA15E75D5CAD975C72C0E709CD49F417DD831265BE66BF6053FABA0A
SHA-512:	3F18878A03F15B1872992D3B703E773AE941FF629ACA21257CF129B82D8C7E2C7564788820F8D7777C70177303BB95FBB9416BE1199C7B91B3A0FCE012BE7130
Malicious:	false
Preview:	2021/03/05-19:05:46.926 18dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/03/05-19:05:46.928 18dc Recovering log #3.2021/03/05-19:05:46.928 18dc 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):	5.2600779709217775
Encrypted:	false
SSDEEP:	6:mn5EN9+q2Pwkn23iKKdKyDZIFUtpW5jS3JZmwPW5DSC9VkwOwkn23iKKdKyJLJ:mWN9+vYf5Kk02FUtpWpS3J/PWtSC9V5E
MD5:	5F28896DFB95F11E172E0AF9C3F512F4
SHA1:	F9A6511A2BC9A300625E721863509F8E73AC4711
SHA-256:	6B6226F397862567EDD562C0BE2989C35A21F50FCFDB5EA89B04D43F4C01107D
SHA-512:	C00B55D27CDB9F1A9C67CAF7FEFF75BB22DECAFDB137B7955A1610AB7C6C9E667C4562F315C78F85D2C63959DDDC29319F35F1C3A6C8A17172DEB81E14FB78D
Malicious:	false
Preview:	2021/03/05-19:05:46.917 18dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/03/05-19:05:46.919 18dc Recovering log #3.2021/03/05-19:05:46.921 18dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	1.1250123155435594
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwgEWogDqRUe98s6pf1H1oNJ7K6P:TekLLOpEO5J/Kn7UoWTmexfvoNo6P
MD5:	711118666289DACFD98785578758D56D
SHA1:	68237E545863CB622A53243A51A05B275C02CDBB
SHA-256:	B5C7380E47EDB56DDC28063B510983C29D4A102A73B19095FB7122630D63347A
SHA-512:	264E167B30C76DEE9A46812B364C8636A62EDC58E339C5A4DA63377493A1F0F206ED6D4E0BE0B6B2AD226AD65364588EE413B3C39B7E86D34A83E6AB3082F54
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9719743404579627
Encrypted:	false
SSDEEP:	24:5e9H6pf1H1oNQqLbJLbXaFpEO5bNmISHn06UwnY8:5bfvoNQq5LLOpEO5J/Kn7UD8
MD5:	9BD449DBF4AD872601512BC05934B97E
SHA1:	674803D04F2C905A61CFFD7FECD31F487E5C2316
SHA-256:	E134504F94080DE0C5E303B01A9556964F7673D76DA7ADB6A076FD331F21AFB2
SHA-512:	943A764E82FDF7FF87E0666E28EE5BFDFE1C88ACD33783B352782EABA5FED9FEEEF65B327E6698FA7A9575B3A708356A862722A415455E2C4B21883512FB6A7E
Malicious:	false
Preview:	.....gt..... ....

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):	2853
Entropy (8bit):	3.7053190029283734
Encrypted:	false
SSDEEP:	48:34JxMMPuF7MPbmAQIvXwj7ANuz15WaF1w4T:34FPqAPaAnAvANuK4T
MD5:	2A483E5F8A54736B1935D5E2C8101556
SHA1:	2C8F2D36027E781487B7EA93330D269F3036189C
SHA-256:	7DB035C5DAE3446D19E46D42963D4E75DD28731337152AEF1F7671140A5F16D2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
SHA-512:	F629ED8AD711DB60996CC3BC1EB651AA28764B1444D8D1BED46E3C3D7CF2515420B0E0BE11507D61ABCCBEA8969FB6A1E4B55522878A582C87219B603FB84C4
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...30fc8b4e_3a91_44fa_b56d_cce3ce639a8e.....).....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....E...file:///C:/Users/user/Desktop/audio_cheri.riley@treetop.com_file.htm.....h.....`.....:.....:....8.....P.....E...f.i.l.e.:././.C.:./.U.s.e.r.s./.j.o.n.e.s./.D.e.s.k.t.o.p./.a.u.d.i.o._.c.h.e.r.i...r.i.l.e.y.@.t.r.e.e.t.o.p...c.o.m._f.i.l.e...h.t.m.....8.....0.....8.....E...file:///C:/Users/user/Desktop/audio_cheri.riley@treetop.com_file.htm.....:i7

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):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.212112405503772
Encrypted:	false
SSDEEP:	6:mn5mQ+q2Pwkn23iKKdK8aPrqIFUtpW5GXgZmwPW5GXQVkwOwkn23iKKdK8amLJ:msvYf5KkL3FUtpWYw/PWY45Jf5KkQJ
MD5:	988426F83A910F19BFE69FD657875895
SHA1:	AEE16ECBFA8BD4881DA13C81F231F35E643BDB61
SHA-256:	2AA4E5774D413C876EF0FE4EF7279267BDBD37A893BA555453CC911C402B60E1
SHA-512:	5BA5A459B82EC467E60706EDCA48606D3E14618358359E05D9D1692236A4B96ED61CBC12CC4A3AAC8223C230E1EBFD4E01E203CF5B0A8A06CD98A3E3B48D2D7A
Malicious:	false
Preview:	2021/03/05-19:05:44.799 1828 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/03/05-19:05:44.801 1828 Recovering log #3.2021/03/05-19:05:44.801 1828 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

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):	5.2277883057406695
Encrypted:	false
SSDEEP:	6:mn5YTvUdjq2Pwkn23iKKdK8NIFUtpW5YT2XZmwPW5YTV/PkwOwkn23iKKdK8+eLJ:mOQdjvYf5KkpFUtpWOq/PWOh/P5Jf5Kb
MD5:	66F6968A75D31D0613147066DBF57012
SHA1:	0CD95051B6D4604CEDF62558497D5F5307F558D5
SHA-256:	9B9BDDE53B5BB532A99A11C6D9A6B302899F444B54F91EB2DC0DA77566409FC1
SHA-512:	B4914CE0DEA6F47A3199390AA742A136D1E35A3535514DB6F0B3BA04BA9B90FD528E19DD965E6DEBA84F95CEF41F48CF0D558389D2DA86AF725D8C22F1F2EF B6
Malicious:	false
Preview:	2021/03/05-19:05:47.060 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/03/05-1 9:05:47.061 1834 Recovering log #3.2021/03/05-19:05:47.062 1834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5 n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","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):	1.933402555740488
Encrypted:	false
SSDEEP:	48:tBmw6fUYuzubcA9Bnw1Ok0+TXUBdsxxyeriuz2Av:tBCLuubcA9Bwsn+Tkvuyeriu2Av
MD5:	CC14E7FA2EA09972CB6D1B0E785BF377
SHA1:	B86D14CB663BB56E6EDDA6211158E1B121297F9D
SHA-256:	5C5673EF20DCDC7FC2178C774D38D022F5F41BF30A20ECF2C5CA1D34BD144C0B
SHA-512:	6A385990ABD185B3A33CDB9B053BD4F2BF494D167AD7ADA58AD9B64942FB543F558038009ACFF4D50EE72B614C256F14FF9DFF8DE0D48A3FD9B6F5A746014F0
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):	0.8134783180010473
Encrypted:	false
SSDEEP:	24:05Sq4lnaQDhyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6UwR3n:Va6CBmw6fUO3n
MD5:	8B99C57E13833451AF389D79E26468B2
SHA1:	230E62E19E212E06EDA67E6E81F0B33BD87F8B77
SHA-256:	0DE6B381EED8E1D510C4BA67B16F8FF60A7018EF0CAB288FD6560C87F6798E43
SHA-512:	DE2672D8E4BB288AE34F343FF4AB71E521D4F75219F11F7D6B40457DE0653C7DDF341D023A59A7C1E74994D1F7F27BEFF1BA53EC60FB985269B44A27484678D
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):	5.2963393766602875
Encrypted:	false
SSDEEP:	6:mn54N9+q2Pwkn23iKKdK25+Xqx8chI+IFUtpW5ZJZmwPW5lO39VkwOwkn23iKKdP:m2N9+vYf5KkTXfchI3FUtpWjJ/PWa39y
MD5:	5076220A61380F9BF7929B0DFD12B30C
SHA1:	892500A3F0C8E0CC7C602A3297FC82027EC0BB52
SHA-256:	563E31FD65F7057B806D9B9117946D2EB89D05BB709216FDB812F631E72A2945
SHA-512:	707D86E293DA9172F97760D80FE30ABE25B263AB06F4EEFF8701C68DAEACF582B68021E8AE078272650792A1C1EFBD81174D5EA4319A0051A76F873101485F36
Malicious:	false
Preview:	2021/03/05-19:05:46.881 18dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/03/05-19:05:46.888 18dc Recovering log #3.2021/03/05-19:05:46.889 18dc 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):	5.251804753574146
Encrypted:	false
SSDEEP:	6:mn50QN9+q2Pwkn23iKKdK25+XuoIFUtpW50dyEJZmwPW5yQh9VkwOwkn23iKKdKl:mX9+vYf5KkTXYFUtpWmyEJ/PWsQh9V5j
MD5:	EB4A46FCE81619D5C24C937B55110ADF
SHA1:	83A92E07CD5426D4ABABF3581D3A4D963C5354B7
SHA-256:	36255F7B8DC4785000C6D2AD6AB3AD8EED2D7CE27DD7449C0785094887B1432D
SHA-512:	FEF0726F0B7AF34A0C012D97871553C04C058354CA2CDAD0349DC65376CAA80749DB29BA0AB447AC3E1355084D651286FCC0E381233E652CD5F5578969A67DA
Malicious:	false
Preview:	2021/03/05-19:05:46.831 18dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/03/05-19:05:46.838 18dc Recovering log #3.2021/03/05-19:05:46.855 18dc 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):	5.3226484783379755
Encrypted:	false
SSDEEP:	6:mn5cUa+q2Pwkn23iKKdKWT5g1ldqIFUtpW5w4+ZmwPW5wKVkwOwkn23iKKdKWT5i:mPvYf5Kkg5gSRFUtpW4/PWx5Jf5Kkg5i
MD5:	5207975CE602E4C6E3E2F727778EF1C1
SHA1:	F05A9D7BBBC27FB05A06B6F6BB24E38CBB5ADF8A
SHA-256:	45FA24373E0EC14451DCA4A6A904E7C59F04DF0DA724CE99837FBA171DA7AA0E
SHA-512:	B2FD8A2DFB01561C786E9876BAF291FB40302F7E00229E91EDACC2679671438257F0DFFDB2AF8FC018A3F127879765430CDC29F39E33E13FF35A2C6494BB7F90
Malicious:	false
Preview:	2021/03/05-19:05:46.687 1b78 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/03/05-19:05:46.692 1b78 Recovering log #3.2021/03/05-19:05:46.693 1b78 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\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	0.354130424939154
Encrypted:	false
SSDEEP:	48:TL5MPkDMPWwA0qWuzFTWd5MPnIKcjqySfUyuzoAIMPZ:iPkYPpA0qWuFTWkPnIKcFByuoABPZ
MD5:	8A6489E2529F6A3AFE1603575C76DA5A
SHA1:	A9486DAE355EED7DE4AA41956155611D408CB59C
SHA-256:	C793AC96B6E50C811DC3589D7F81707C9AEA305E937E73F95F70B7DA2203C5CA
SHA-512:	BC9E745D0E09BBB2E298329F87246B09CEA15615E6E9E807D2E9700419C7AAD6C5202A72C1D54A1399B6B5B3D9A234897989961AD7E95C82935F2BB9931302A8
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	649
Entropy (8bit):	5.197501919603076
Encrypted:	false
SSDEEP:	12:8qb3mVYiegDKj2ZBRD66YFAxeT2cxP1tndq36nItiwu1TBk778B/xgskZBa9sNi9:nmVY/gE2pXOxP1tdqIlwY78BJgskfa9D
MD5:	37FB5F5B0A57303A9D81FE073E71D5A6
SHA1:	1A59A87CB15D833C05074E7F1C7576667F184F82
SHA-256:	15973CF529B8D368D6889E2E2DF04BD34650537DBFB12BE51C5B9E73D0E18EC2
SHA-512:	BC2D2687D988BCD7C66740DF78599861F80C6F87352B3BC203274DB67098A7A21BA573D9FDCE00E51C728463A0FF63460C9F08A180B689FB9592B7C1F04E2931
Malicious:	false
Preview:	....."J....audio..c..cheri..com..desktop..file..htm..user..riley..treetop..users*v.....audio.....c.....cheri.....com.....desktop.....file.....htm.....user.....riley.....treetop.....u sers..2.....a.....c.....d.....e.....f.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....y...:e..... .....Bm...i..... .....*Efile:///C:/Users/user/Desktop/audio_cheri.riley@treetop.com_file.htm2.:.....J.....%+19=B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	71328
Entropy (8bit):	0.12941989634774098
Encrypted:	false
SSDEEP:	24:eqLBD2M3ApMP6W3pMPyMh+Cu6tf1NQTfT:eqT3wMP6W5MP8Z61j4T
MD5:	14E2C7EA0D5671A0F24A940C79D2F54D
SHA1:	16BB1EC68D4B618ECFD5AD444EC91C7FD2649DEB
SHA-256:	1BB9685B9FB739467DB6AFE490247196B28AFD9B6179DCDE1F954F19CEF20842
SHA-512:	F05A660F37EDBF2A23231D4DE5CE434974041885252A1461808B4CCBAA6629400B8B0600E8ADA982F4951CF7A0B39AB6A762B414FBD6B856C7817BB23BA16596
Malicious:	false
Preview:	.....H."Q..... ....

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):	2955
Entropy (8bit):	5.467480026151995
Encrypted:	false
SSDEEP:	48:lZ7WGjDa76MB8dbc7Lx5bQSefgGxYi4NrS0U9RdiN9Wx:lZla76MCdbc7LLbQ5fgGxYZrS0a
MD5:	B7910B1C9D136ABA77F19CB4F2A73B91
SHA1:	2F853F69AF2B700CEA0E5A6EB16C236277CF435F
SHA-256:	6172E6471111520D359843E07EAB401173220ED8E37DFEF0220791FC7EA5F2A9
SHA-512:	2580FBEB290C5E166945F31FE33E9924CA49CD709828D8B6645F53E3FDBB015ACF9DA294EA525DCB0B77B3B3F1EBCA4815A71950775C615E7C08645070CCCC 9
Malicious:	false
Preview:	..r....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.Hangout SinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast .RequestIdGenerator..105942000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-03-05 19:05:51.18][INFO][mr.Init] MR instance ID: 7401927b-8f80-4a86-ad92-61cfca1e8bf1\n","[2021-03-05 19:05:51.18][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-03-05 19:05:51.18][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-03-05 19:05:51.18][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-03-05 19:0 5:51.18][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-03-05 19:05:51.18][INFO][mr.CastProvider] Query enabled: true\n","[2021- 03-05 19:05:51.18][INFO][mr.CloudProvider]

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Size (bytes):	332
Entropy (8bit):	5.168271366004618
Encrypted:	false
SSDEEP:	6:mn5t+q2Pwkn23iKKdK8a2jMGIFUtpW5fFfWZmwPW5vzVkwOwkn23iKKdK8a2jMmd:mT+vYf5Kk8EFUtpWXW/PWNzV5Jf5Kk8N
MD5:	4ED20615FC49251B59A12E74C0C1EF2D
SHA1:	DFE96FEE33EEF10FF40D7B926EA992B3BFBDCD00
SHA-256:	06F215E1F7CCB7AEF92050F82F0DCB22560D70D9CF94617100602AF785052661
SHA-512:	95E38532882B5C06026DCE0901414F7495D5FB39D8F17DF454C54B0FCC98D68477D8CC8CD8B5A3A7E02F0B1B922EFF48FA98F718A25389D32F53D2193BB823A
Malicious:	false
Preview:	2021/03/05-19:05:44.591 1bec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/03/05-19:05:44.592 1bec Recovering log #3.2021/03/05-19:05:44.593 1bec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	1.1157221051119153
Encrypted:	false
SSDEEP:	48:Trw/qALihje9kqL42WOT/xO7rCfibw/qALihje9kqL42WOT/xaWu:vOqAuhjspnWOs7GMOqAuhjspnWO9u
MD5:	E56D5F75F10DB7F210021F6D9F056FE7
SHA1:	52A562AAF13443D20F972218899D42E00B5F7E46
SHA-256:	9DE1618C63050248A105EFF1C8F14265DB4E50735C340FBA2649BAE7781B76A8
SHA-512:	A63A603A1669DD7A542D4DE2F1890070B950BA4A3C804082AB26DE6BD3FEAEB8A86D778E1B822870E7D85B487284E05198CAF5C0D9A0B24CFC3F68732C14EAF
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>...,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.0203281623978284
Encrypted:	false
SSDEEP:	48:U4q7w/qALihje9kqL42WOT/mkqrw/qALihje9kqL42WOT/C8:U4UOqAuhjspnWOLkOqAuhjspnWOd
MD5:	5DE002517557D7189A86B803D9E0F015
SHA1:	6790C77A1BA99BD2697F8E9443E4E3FC22BF5D2A
SHA-256:	8A9903C4E2E25AC3CCE495F430ED80FD6F79693A3307E58223022E64C9FE9B0A
SHA-512:	33F29A61105214D37F29F5984311C39F8B4B3DE5BE367B326942E4B8F715583B661688BF272BFD555473A16F0551E35C267B735C226D44C4DA49A21FDAF11758
Malicious:	false
Preview:	.....5E..... ....

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):	5.232704429832544
Encrypted:	false
SSDEEP:	6:mn5qSq2Pwkn23iKKdKgXz4rRIFUtpW5B1ZmwPW5bZFkwOwkn23iKKdKgXz4q8LJ:m0SvYf5KkgXiuFUtpWJ/PWZn5Jf5Kkgi
MD5:	0E833CA5CC101F18B2961E1D58F4E8E0
SHA1:	6BC7CD01D3EF2DAAF4DBD8608275B6A9328A4F16
SHA-256:	81F2487C5889B22A2B701295AC0DED86480F46B9645C88E3D9A1183C914E495A
SHA-512:	90DF1C89CA54BECC42FC6C26580D229F28ACE49DD9DA78CB9FF57FF101428E1905831160B1AD34CABF8808CAF255125ACEFAEBDF70D37693F120EDD61E1F0729
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Preview:	2021/03/05-19:05:44.827 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/03/05-19:05:44.831 1834 Recovering log #3.2021/03/05-19:05:44.833 1834 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\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	133
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljljl
MD5:	2D264D9C84A987914AFF523B33A657BF
SHA1:	2673ADCD9295F0A9965C72379499337B98114CCC
SHA-256:	ED239EE0B51A309EF10DC617685639BBE298D489C94AC5662BFF78079334F946
SHA-512:	48ADD9AC76C4A7B5F5D6A47ADDD833352314CC95EB3CBD33407B2076856AF21BDEE6F1BD26AB950BE18D13E5BAC9D34FE4AB46833E93D826EEBDF7B09659D48A
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.213288120131204
Encrypted:	false
SSDEEP:	6:mn5pQ+q2Pwkn23iKKdKrQMxIFUtpW5zAgZmwPW5zAQVkwOwkn23iKKdKrQMFLJ:mhvYf5KkCFUtpWpJ/PWpD5Jf5KktJ
MD5:	AFF071940B4E48C0AD5C83346A5C93FA
SHA1:	9B8A9E94D170F44A849449E07F034B843E546193
SHA-256:	0DC045FDD6B24FB168028CD558960C5FC3D502FA32B3838F5BCC309330B50E3C
SHA-512:	50E43384753A4B70BFAD7E25F640854F63380DF39E1E5766E83DC7A129EF0697ED6788B64CBBD6480BF870DBBC09F3D9D08A6897722A5D8E39191E72AD0D593
Malicious:	false
Preview:	2021/03/05-19:05:44.756 1828 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/03/05-19:05:44.757 1828 Recovering log #3.2021/03/05-19:05:44.757 1828 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\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.320671207545618
Encrypted:	false
SSDEEP:	3:uXl9p+WwKWlkAj4detv:Anc5kAcds
MD5:	705EA780771300C6ABE8E29DD0CE6C08
SHA1:	06641F5AA14AEF0A0E6120778CC9B92F2E6618D5
SHA-256:	60B0FBAB9AD7662272FF0C967FAB9B4DE12A564388A095BA4A382C5D8E2F2E0D
SHA-512:	53D101E4BB8831F5F9CC278BCE18EC48582933D114A2086EB144791CC616064BF6C56A2C1775192C1FC006B1DCD4F37C9642BE2AE7DFD312F8BDE3106BE176
Malicious:	false
Preview:	.E..5..... 6a2fd5ad3e06cd365167a16ed75a48f1.....

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):	5.177884301736608
Encrypted:	false
SSDEEP:	6:mn5rq2Pwkn23iKKdK7Uh2ghZIFUtpW59FZmwPW59XkwOwkn23iKKdK7Uh2gnLJ:mJvYf5KklhHh2FUtpWnF/PWnX5Jf5Kks
MD5:	48BBFBD2E1521B8C572FA41FE7644EF1
SHA1:	7AAC35DF69848D5B3CA95BB087BF26028966DD4E
SHA-256:	E573C29420F7F5FAA1BB52137331A818BD106993FB3A21E37CBEBED1012C6639

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
SHA-512:	B4927F2BF95C6ED789BE7E4DF14E2509C32E90944BE0420527CABDFE123D0DCF28A35A1F3002164E40E9545B682E0BE5A3FD9195E53C5535C445276F615999E5
Malicious:	false
Preview:	2021/03/05-19:05:44.553 1b74 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/03/05-19:05:44.554 1b74 Recovering log #3.2021/03/05-19:05:44.554 1b74 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\21e667a9-1214-4ca0-9a39-2ebabc452c46.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):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","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\3e0de6c4-6962-46c5-96a8-7b6b1d2458f7.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):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","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):	5.296499944706037
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
SSDEEP:	6:mn5XlQ+q2Pwkn23iKKdKusNpV/2jMGIFUtpW5/AgZmwPW5YSuiQVkwOwkn23iKKZ:mdvYf5KkFFUtpWP/PWx45Jf5KkOJ
MD5:	FDEEC5EF80117E2577FB9C67239FA70F
SHA1:	17ADC6AC1986973E477A3FABCD568D6573ABA2ED
SHA-256:	873169D9EC70D0D9C0F84B848187E011068CD0534EBE148698EFA2D0645939E5
SHA-512:	899CEDBD20C23946DC457EA7EBA13BAD5AA960006B5AAF4055E09F595138139E8D146C12426CAE992D1EF454C5367485B0C990BCEEC3B2463B06D6BB5804C77
Malicious:	false
Preview:	2021/03/05-19:05:44.778 1828 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/03/05-19:05:44.779 1828 Recovering log #3.2021/03/05-19:05:44.787 1828 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):	5.297053993587122
Encrypted:	false
SSDEEP:	6:mn5z+q2Pwkn23iKKdKusNpqz4rRIFUtpW5q/XZmwPW5oVkwOwkn23iKKdKusNpqS:mYvYf5KkmiuFUtpW0f/PWW5Jf5Kkm2J
MD5:	5E654B39D26B90B8671C40075388CDA6
SHA1:	E8C262ADD6D4082A4FF1A4C50895469969FFC6BC
SHA-256:	A00A626D2372E18AD8120C9519EDA7727A580226C44B6F988D0B59528AA4F400
SHA-512:	E980F7269A43B0599FE50E011560326D8C9AF8649D922868867CA3828617319FF48FB509F0B34FE749A0575A08904CD980996FBE3A86CCFD2EB214BAB75113EF
Malicious:	false
Preview:	2021/03/05-19:05:44.826 1be8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/03/05-19:05:44.827 1be8 Recovering log #3.2021/03/05-19:05:44.830 1be8 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):	5.244898319291469
Encrypted:	false
SSDEEP:	12:FVULcSvYf5KkMFUtp1VUc/P1VUzF5Jf5KkTJ:FVn4Yf5KkUgvVzV4Jf5Kkl
MD5:	0524981B0FD70BC0281274F32D4EED94
SHA1:	B4E240DD852FF106C30492EDF04F2E584AEAA07A
SHA-256:	D1D9968B61D4CB2D5E9BC9175530029F48938F4BA82B563201C1382C4DB12D73
SHA-512:	9A3A423FFE547CD1EF10E36F8CCFE2D7D4E1A988B7D591CD66BADCA5754D8CB9D6CAB987E67952446A8A32D7CB9C9E1277BC22BB74F971A24AEBD8254654882
Malicious:	false
Preview:	2021/03/05-19:06:01.089 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/03/05-19:06:01.090 1834 Recovering log #3.2021/03/05-19:06:01.091 1834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\f9608479-6dc8-4552-aa92-e0e24261c17f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\f9608479-6dc8-4552-aa92-e0e24261c17f.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.975147286312194
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sdHfHYhsBdLJlyH7E4f3K3X
MD5:	A6C1D2076E0E7FFE40E5BFEC0BEAFAA7
SHA1:	F1CD6815325610D07455A215A1C4E724D2F1DC17
SHA-256:	3B3BD7020547A67DD4A6A30E8ADBC4A5921570268D7E0182053BF5412F5BFF50
SHA-512:	7534CBC15D48BEC22E52459AA3832DBA67CE0EF7A0C6B6A1192BA8425C056E8629176C2EF92BA977CC3A6BBB019236243C1C551630D0BC8902F7456AC90B8B0
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\2a5f0dcb-d92e-438f-94e5-003dcda62a99.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):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","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\58943f74-7189-4396-8315-607374d71848.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):	325
Entropy (8bit):	4.963653940178319
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sdHirhsBdLJlyH7E4f3K3X
MD5:	E94036DF834460DF6795F5DDCCCD0B69
SHA1:	0352869460986A77961DDB65A85572FFBF4AC0FF
SHA-256:	4087DF4160118C6F53D2E18B0A65B23FD373796A4285116852AF4EF927C40FA8
SHA-512:	9DD6536B6A73DD499D2FD882A469A51B7EC85AEDB8CD62F3D9C53A08994F8B1E16416C406962050B38F6C2289F77881D814555558A94BB7C59852AB655A9D0A
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.234458156343476
Encrypted:	false
SSDEEP:	12:mLvYf5KkkGHArBFUtpW0/PW05Jf5KkkGHAryJ:YYf5KkkGgPgJJf5KkkGga
MD5:	3FA14CD053199F5126A3E1E63D2D7085
SHA1:	D87E83C9D3647B586B0416F9A609E2C39B4AA000
SHA-256:	A1709742DD585AF86E3C94B58FA8D00880E372B58D1D56C98E8DECC0D27CF949
SHA-512:	2A795B30B8284B60034741B9DBE8915F8BF00275CEF62133318A833DFDF068040BAE92077181F83EFD2517A29F56E17D3132AA57D6D11D668D29E7E07771B68C
Malicious:	false
Preview:	2021/03/05-19:05:48.985 1828 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/03/05-19:05:48.987 1828 Recovering log #3.2021/03/05-19:05:48.987 1828 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.2436406548355
Encrypted:	false
SSDEEP:	12:m4vYf5KkkGHArqiuFUtpWT/PWpU5Jf5KkkGHArq2J:5Yf5KkkGgCg0Jf5KkkGg7
MD5:	A2360A8EEC69466D90527B5A1AE243BA
SHA1:	1066D5012C96727647430F014C34EDBE94B18243
SHA-256:	D7F4B27669C3114436BEFCD5BE2B98AE0355E5ECDB3445D6949B95959548DBC5
SHA-512:	369AE16525B791DAB6EAB055CE4D3F6544E42B98E99736FD5302BD9B66CDC8FABBE7C9DE24B01312306061BEA8477DFF5F4459CA24DD2BE2030083EF135372 4D
Malicious:	false
Preview:	2021/03/05-19:05:48.997 1824 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/03/05-19:05:48.999 1824 Recovering log #3.2021/03/05-19:05:49.001 1824 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.224207907663172
Encrypted:	false
SSDEEP:	12:FVoOvYf5KkkGHArAFUtp1VAk/P1VG5Jf5KkkGHArfJ:FVFYf5KkkGgkgvVAKVQJf5KkkGgV
MD5:	5307EB37F852681FF1A436C1687B5474
SHA1:	7D5EE787072FF97B9ACCBEC3392624B2C24FE259

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
SHA-256:	A7F10F209BD2D72C8BAC21E3ABB54EA2FD8F40361B0C2C49638494037A7F3A69
SHA-512:	E96B397DB0D44E8EA48EF1238EC32631446A5DFA58E8331ACB177B2E1B05C4300BAC2961B4A2ECE674F314D0647091BC1A3F86E53B2021FB2047EB61E8CCEB2
Malicious:	false
Preview:	2021/03/05-19:06:04.247 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/03/05-19:06:04.248 1834 Recovering log #3.2021/03/05-19:06:04.249 1834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\df837a08-30f9-4c60-8265-aa263f6953ee.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):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
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):	5.288629306661684
Encrypted:	false
SSDEEP:	6:mn5Vkq2Pwkn23iKKdKpIFUtpW5dCZmwPW5bXkwOwkn23iKKdKa/WLJ:mPkvYf5KkmFUtpWfC/PWt5Jf5KkaUJ
MD5:	2C5862D4C152151788210E35C188127C
SHA1:	FF9C0080A5FFEC40E04011742B208A800BE2BBF2
SHA-256:	7EF51D91112512925CDF657CEAECF23DD0B6C8CD15588E080FAAF90D1BF2DD6F
SHA-512:	A10C1A95D073D8088F63FA19E4B295E6C686ED220368F29E40A2E14B36C1BA8DD0E93773C86409ED6357545DC0DEC33D00798AF052EB08402D44D4229A1FDD9
Malicious:	false
Preview:	2021/03/05-19:05:44.576 1b74 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/03/05-19:05:44.577 1b74 Recovering log #3.2021/03/05-19:05:44.578 1b74 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Entropy (8bit):	5.3144447386721225
Encrypted:	false
SSDEEP:	12:muvYf5KkkOrsFUtpWUX/PWUF5Jf5KkkOrzJ:7Yf5Kk+gZJf5Kkn
MD5:	F370B75D8EE51C507B0FF5A266931346
SHA1:	E5ABBEFE2E7953B8158FA78925E33DB22DDB2788
SHA-256:	57ABC0B3DC59F7D7561D46B92F71473E8F78CE9BB6561A618F0B95A4E428F806
SHA-512:	4980B08A60D7B876501C78AFEA53283098B883529CFF9D36FFB6E50DA9F7EEAC097F23D6A5D7C5A6298A425E8B6BC554DACFE056896D67443D53DB471B33DD5
Malicious:	false
Preview:	2021/03/05-19:05:51.174 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/03/05-19:05:51.175 1834 Recovering log #3.2021/03/05-19:05:51.175 1834 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):	60
Entropy (8bit):	4.796834613373054
Encrypted:	false
SSDEEP:	3:/qZNll1j3Q1gEaS8tO2n:/qJluWdS8tO2
MD5:	BE9AAA6ACABE10A4210EB59E01956647
SHA1:	287F782F2A8C22868DA4CC2FEDEA41D2291C25DA
SHA-256:	27B8185FB499DDF4891D26D6320A455BE8BEAE7EB2C5E9D8E49099AEE0B733A9
SHA-512:	56FD91F32A370C729C5E35BE8831D83FE9103F0BB7955C86F379524C99F7D54A24F5DCEA1188575F1F14D79DCE115A78F43A3FEB4934CEBA60AB78D2EFD3E64E
Malicious:	false
Preview:	......V.-.w.....u.....%.ep.....Bb.i.7.....r..4..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a0d648d4-cf7d-4101-aea1-410e84d0ec83.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a6da8e63-3b5a-4a9b-9153-1442bc2916cf.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):	1041
Entropy (8bit):	5.568938085899346
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeiXzkq/HeUe8zUef7wURx8RUeiQ:Ym6UUhyKUeiYqPeUekUezwU8UeP
MD5:	D9CC86563B17A6CDD993A6EE8A32C5C2
SHA1:	3B371384C5BF61C588D6D6C5250F0B6A53F8FB3D
SHA-256:	60C5DD80D8B681E9ACA0F263ED1D910C495C45F815937D8D8EBC6E0532E2C41A
SHA-512:	4E628A5F2348B1B4CF433B432B1F77B6397D2EA3B1B17925269DDC088DE3F5ED0F28E850FB0CCBDD23780F360C93C204798848D097D51C6945FCDF49F6884C7
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1646503547.506126,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614967547.506129},{"expiry":1632986995.164829,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\afefa4c5-16a6-4350-a4d8-b69a1dfc878d.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cb7ccd56-693f-4f31-bd9b-3ab65a3f0791.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):	5618
Entropy (8bit):	5.166391738480528
Encrypted:	false
SSDEEP:	96:ndLup4yQSKtXIVRk5k0JCXSRWL88bOTlVuHn:nd+4yQSKtXIQh4XSYb
MD5:	04C31A323EA711DFE5EB7773EA84217D
SHA1:	A43885BD863E0BAF6400AE7C9EB6D4C980FE82A3
SHA-256:	DC975F1D92F0644ADAC60A88EF100A162E39C9FB1616C52C05EED5F89E383F8C
SHA-512:	E2E87E1658E565BBACFF94B773E7910EF3D5B84FE8D9615FC11DC6FD7F3C8C21596F11C6624C0A3B8B4F3458E95FDC2F85B9B94F9F976BF047F1B54F02C8D2E A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13259441144796579","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d7cf1098-11e2-443c-996f-03c8a71426e7.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):	1725
Entropy (8bit):	4.848806953424284
Encrypted:	false
SSDEEP:	48:Y2nzMK6qDHGXCtwWshmRLsh0DshuyKshK3gYhbw:JnzMKxDHGXCOe15VxhM
MD5:	24750437290FACBA24F91958501F498F
SHA1:	17E2B9E80B70A9CA10863E062CDDF06AE65CF5F0
SHA-256:	4EB59E97A1B67FCEA51AD38BD1DA304F2AD421FFE4AB5514AA970818E663390A
SHA-512:	10FE98E900530747B8A84DA6C623ED771570D2EF09E0F05EB719202020DF47905E9E9EE345372A94DDD9F74F702E74E3AF19A0A1CED38BA72E1ABDA88CCE7B9 2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13262033147506011","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
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):	4.596121271370459
Encrypted:	false
SSDEEP:	3:tUK99Q5HsUDEj1Zmwv379Q5HWASV8s79Q5H3oSASWGv:mn5xEJZmwPW52VVvW5XoSVtv
MD5:	4E01A9ACF8779DDE58F9C4F28097A95F
SHA1:	805A4EE1B89F9FC99F5DE91A5F7D4B4B6846556D
SHA-256:	E7B86D2A967F288C36A634667965BDF8B22022D382E4CEF6A08437298A92B7AF
SHA-512:	9FE6A21C0ECFC03DFE466FC3C0DBEE85C8FAA9C9615B77D71B95C30D1DD03CADDDBE93662DED799D83A9B67E2388FED149E44BD12CCAC13153094FB6EAC 70B3
Malicious:	false
Preview:	2021/03/05-19:05:46.351 18dc Recovering log #3.2021/03/05-19:05:46.551 18dc Delete type=0 #3.2021/03/05-19:05:46.552 18dc Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e242bcfd-a4af-45cd-a16a-6871f4c617ec.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):	22620
Entropy (8bit):	5.535805323876925
Encrypted:	false
SSDEEP:	384:COit1LlFXXz1kXqKf/pUZNCgVLH2HfDzrUjHGanZQTRtWwg4C:2Llz1kXqKf/pUZNCgVLH2HfPrUDGanX
MD5:	D316F6B0CF019C098B6CDED88B946C25
SHA1:	30D1377D7C8FE964D9E2ABDD596F60F2798E8C26
SHA-256:	18FAF032E2E1C596A85C66CE10EDD7B27CFB563D643429D7BF78238AE6354314
SHA-512:	1D3F42E8285302F2A816B4320334596666FD4525F9B4D40709EB6B769F0D1388C73F42E61AA113D140F22725B7CB5FF48C04036A814A384C956A2329E1B397EF
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":"13259441144572704","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\e390495a-fe3b-41b7-a80e-210f3e7faa33.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):	5378
Entropy (8bit):	5.15631523836105
Encrypted:	false
SSDEEP:	96:ndLAp4yQSKtXIVRk5k0JCKL8bbOTlVuHn:ndg4yQSKtXIQh4Km
MD5:	72A4E7761E6A586C4B6DF568D50CEECA
SHA1:	9D2B56A4ABC4BAF1A978BAF64FD9E8EF45877ADA
SHA-256:	03B6173030CCEF54867196A42D0E0909A8145A14A6C56F7F4DB035BC63B0E700
SHA-512:	14A2ED21268B0DE8E0C168A48967B834898671E5B210C2A140F4A65D4C63F37070888C65F52E4ADE915A71891402E23AC189C378C16B601539A5556D9E5C2996
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13259441144796579","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f9510351-8504-4291-812a-35da44af02ed.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):	22618
Entropy (8bit):	5.535974141195091
Encrypted:	false
SSDEEP:	384:COit8LlFXXz1kXqKf/pUZNCgVLH2HfDzrUjHGhnZpTRbWwg4u:tLllz1kXqKf/pUZNCgVLH2HfPrUDGhnK
MD5:	4B0BD8614A6C4B4C19A160A8AB2991FA
SHA1:	53274EE582147F17B0DB6B6D7FA782F12A93F114
SHA-256:	2322A3E897B83290D08B62C10B3982EDC7887B5F705F48B47D1AF368F7F9E896
SHA-512:	BCBC5B2481051AACD0F29F79EBEE31859348497A09F3893F1B1EE327C97752C6D3026CA121718F17CE38052EC848096B3154E67AD9D1B9ADF66CB61C0ED9320
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":"13259441144572704","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\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):	5.212256558030104
Encrypted:	false
SSDEEP:	6:mn5Ttq2Pwkn23iKKdKfrzAdIFUtpW5zI8XZmwPW5zI8FkwOwkn23iKKdKfrzILJ:m1tvYf5Kk9FUtpWFIo/PWFIw5Jf5Kk2J
MD5:	7861745F8B5006875112A9DEDE35A6B2
SHA1:	1AF2E0B2E76D4AD3CF6E8A23B8854FF29A0E10A7
SHA-256:	A516C28B8C265A827DFB0B7C9E50593F41B0B5E942E9A240F732F6E5F0DE85B6
SHA-512:	AA153C199B452B37CB734A7B8C7927FC025F3E679BCE7D61614A2AF9BD5BC57EE6678F22C2040D60DC49F9A922E5A9A1DC150DD3A6CB38FBB88ADB4B76598I 8C
Malicious:	false
Preview:	2021/03/05-19:05:46.942 1ba0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/03/05-19:05:46.943 1ba0 Recovering log #3.2021/03/05-19:05:46.943 1ba0 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.19.0\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_dir6868_785586536\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	223592
Entropy (8bit):	4.9638585725691575
Encrypted:	false
SSDEEP:	3072:SRztNSIhnVr91m7Y+VFwPmqSqm2+Sc4Q2PRbKbG5uu5hrExzu6KyGbx+9Omzpj:ShNZDE7nxPC5cVr6xE
MD5:	FCCFC2303ACCE4945A4E5B17FEB074D6
SHA1:	314086BBE1D350CB8850C76D89C00EC6D4E7B0BE
SHA-256:	6139961F1E07AE33628E913D3551469AFB1AD57A29F0520B2281879A44CBC92F
SHA-512:	7F8E9D7919C5A4896113EBFDACC5B9728DC9F56138B163FD92E9CC82B393890B125FADE7586B3A4373B9930311035E5581B14705167070A28FDB5D42D69EA14E
Malicious:	false
Preview:	.....d.....5..... ....`...D.....|.....t..p.....h...d..`.....t...L...T...8...@...<...8...4.....,...(.....uocca.....&.....ozama.....3..0.....0iupb.....@_..H.....g.bat.....`.....onwod.....x.....ennab.....d.....nozam.....(v.....geips.....rekoj.....lgoog.....`.....uotpo.....lreko.....o.....x7.....x.....tf.....H...,.....P...L.....@...<...t...4...0...P...(...0... .....h.....H.....(.....l.....H.....(.....t.....l...h...d...`.....T...P...L...H...X...@...<...8...4...0...,...(...$... .....d.....@..... .....p.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\cce5b500-1ed6-4aab-b607-8b2714b2813b.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):	156989
Entropy (8bit):	6.052645098419966
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\cce5b500-1ed6-4aab-b607-8b2714b2813b.tmp	
SSDEEP:	3072:nwe9QSr571ljD6v2CcDPvZaerlibFcbXafIB0u1GOJmA3iuRN:wAQwh1xFTJ4kaqfIlUOoSiuRN
MD5:	AF72D4AA87AC970B3B9FB0A822B94C8F
SHA1:	63083CD0114345C2370CB02F403FAFEB5909395B
SHA-256:	BD4AD204DA17EC7A47A091E7BEEBDEB54CE69C7184F1424A7F4B25276F7B5DEE
SHA-512:	BD407592CA01744B4E464853B2B4324C069348B825D698D8BF5BF7D50322FC583AAC9454CF1FB8D19C774EA0B2C1633EBBE67C9D9D92F515EB97AAB4E612BA6
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614967547635927e+12,"network":1.614967549e+12,"ticks":304047759.0,"uncertainty":4526021.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Os h5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2P KkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":

C:\Users\user\AppData\Local\Google\Chrome\User Data\e4d66e5e-d7f2-4fbc-9aa0-05422cfe7674.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.744347289394037
Encrypted:	false
SSDEEP:	384:7bhCG4fd08rGFN6rvvuW3lugRH8xGhIrjgqwxNEYALrzGm/kDQa+GFOEoWNn16Dx:zCVBSQtpMebQSoEXv2SK4GapC
MD5:	569175AC784580BC4716538F037F396A
SHA1:	05C0F58C4663E10544B4470BC29135079F32CFD8
SHA-256:	EC67A36DC2D1FBE511D615DB58E85674B376FFA942144076982FCDF48B2388A9
SHA-512:	A817B78465D028107E928C23EFCD7410D9BFE93398BB87A8FA1B66AC7ECDEF07F82CBB8C98EA6DF6A244B91CD1B6B5B9FB1BFDC740822E5286A4F364871A9874
Malicious:	false
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...j38.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\Temp\3a94ea7e-fd04-4802-8ea2-16cd43ee63aa.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..''0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n. <Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..& ..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,.. .W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6.. @?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\51e5668b-1c0d-4075-884f-fb7aad6a8166.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

C:\Users\user\AppData\Local\Temp\51e5668b-1c0d-4075-884f-fb7aad6a8166.tmp	
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\6868_1218504966\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\6868_1400507617\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):	3.872935977280404
Encrypted:	false
SSDEEP:	3:S0bEVMqCVQD5mhG8d6+qGn:SGlQUhG8Im
MD5:	A43371DACA3F176ED5A048BC5E2899B1
SHA1:	32FC0A9ECB568BDF3CE13F9EA17E827A900EDB42
SHA-256:	736DB43A7CCB37136CAEFF0B80670BD76BFE528203856CB19CB6C3D161B48F9C
SHA-512:	8754C5D823A9EED2749852B37084F5ED14176B6CB74D946CA3F152DD91F2C03CC4457F1CA0219D883522C7213C4CD04FCD2E33BBB31C7F7EBD6968CEE35AF91
Malicious:	false
Preview:	1.a8a79d350c2a5e3bc36226633a8e0bed0dfab184e77f38fc8f0820ebacf8eafc

C:\Users\user\AppData\Local\Temp\6868_1418553254\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):	3.8184870675314144
Encrypted:	false
SSDEEP:	3:SSgdRQtXPjnQVLX4I2LNyzXdn:SSgdRQxPjnQ14tAzXd
MD5:	DE50A5B093F2233B688C710F12E2816D
SHA1:	2E0EDDCCB2E6144A5E640AD9ED92B4D27A88B9C9
SHA-256:	505E9F362B6BDCCF6AA007C4F5228D999B6CFB553980BAE38CF3204D6DF872AA
SHA-512:	B455D4C22B21D779544816F1B505C6AC701A159BECBC84AD535F60EC8CDA0CE1FDEB16B1E41407C47D456F161EF8D01288E40F15FA778CD4B820BC286F95B7A
Malicious:	false
Preview:	1.7d315645c6a7a98c8c88c51eaaa64575081d492ae50f58e686b8119864023087

C:\Users\user\AppData\Local\Temp\6868_2057984965\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):	3.9477608398895883
Encrypted:	false
SSDEEP:	3:SdUoLS6MTYUAZdXtbJXBVGHIVWfE:S/7MTYUATPv8c
MD5:	AFFD907C7BB49B4A7449E67EE49D99C7
SHA1:	3DAEC57822D8C39E0BDE14BCD19B906CED0F55ED

C:\Users\user\AppData\Local\Temp\6868_2057984965\manifest.fingerprint	
SHA-256:	D5CDD87B76D7E6C3DC16374D41B8350519BE46B978EAC80AB70E6386F6E702FB
SHA-512:	488D45EA5C58C2F27360E86CC50F487AE81F6E5C8D58D82C0155346297AAA542018BBCCAD138972D173E3E822F06D62A95EFDE2426D8823AC1C987214D67D01
Malicious:	false
Preview:	1.869f6197c3fdd474910319ff37ee13b73f8fb8ceeaaa62517e2d056b6a03ff54

C:\Users\user\AppData\Local\Temp\6868_532910252\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):	3.866533712632772
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\6868_607618670\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9570514164363635
Encrypted:	false
SSDEEP:	3:SVCBGERJd9WaHpYx4eiXoA:SVCwERJdVMiXd
MD5:	C6ABF42CB5AF869629971C2E42A87FD5
SHA1:	6EB0FAE28D9466E76FA12E31FE6CDADD3ACCE4D1
SHA-256:	D281AFDA759075F4CB7D7CEEC4A3CB2AF135213B4D691F27090E13F238486AD1
SHA-512:	EDDF7E4883E82718743C589E8F2E48BEAD948428E730231FEFADAD380853343332BC56C9DC61C963B3F537CD4865B06FF330CEF012B152CEA35F8A0AA2C7B56D
Malicious:	false
Preview:	1.fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace

C:\Users\user\AppData\Local\Temp\6868_925890476\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):	3.9669759926795995
Encrypted:	false
SSDEEP:	3:SfvHUTa8URTTH/BXDj6:SXD3TfB36
MD5:	E3EDA33A5C956F4FC9C5BBD91FF10252
SHA1:	182B989E299A3EC306622A9DD45C3B74A4DF6077
SHA-256:	6D7A462B703F1617286B65BFE0116F267328BEFC379812BCE774D8C640289647
SHA-512:	A49FF4979FEC3512C44899840CCF8D112806330C93812C515F09953B9B6DBA6B1DAB1828382D634235CF23E093C983AEFA860B7A75FDCB5F3F98DD928D4F47D
Malicious:	false
Preview:	1.d730fdd6875bfda19ae43c639e89fe6c24e48b53ec4f466b1d7de2001f97e03c

C:\Users\user\AppData\Local\Temp\b11569e6-fe25-4b3d-a5d0-45e0bf1f7704.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

C:\Users\user\AppData\Local\Temp\b11569e6-fe25-4b3d-a5d0-45e0bf1f7704.tmp	
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\ed9d3ab7-c7fb-4642-bd1f-f4d3ddcf75c2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir6868_23867426\3a94ea7e-fd04-4802-8ea2-16cd43ee63aa.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir6868_23867426\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6868_23867426\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir6868_23867426\CRX_INSTALL_locales\ca\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB B4
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": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6868_23867426\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488 B
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

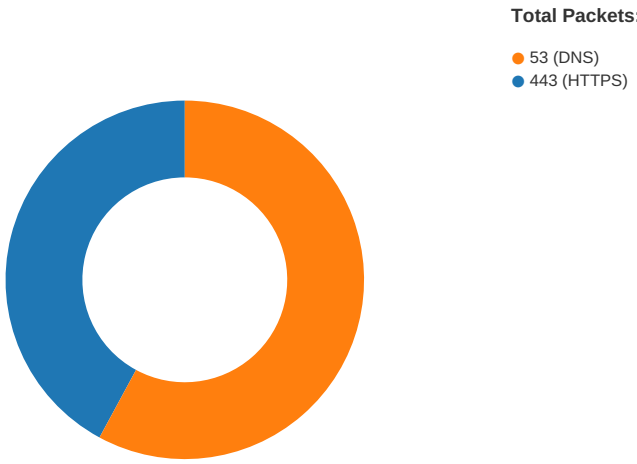
Static File Info

General

File type:	HTML document, ASCII text, with no line terminators
Entropy (8bit):	5.082833230831259
TrID:	• HyperText Markup Language (31031/1) 100.00%
File name:	audio_cheri.riley@treetop.com_file.htm
File size:	128
MD5:	ce5eab4d11db52a141d75d5e0f6d4c74
SHA1:	973c43de204871ad4482918636e07499c0025ba2
SHA256:	bae99731991ee7c320218ca713b916d18755cb0d14b1d6 9f5a307aaae3d5eaad
SHA512:	007ee3b839176e387ad6b254eec602badb5548de4eff3a3 ddfdc68bc05754c3480491653d36dac9711d1b30f66061a d92e586b776a2e7765addcd8cab84ca782
SSDEEP:	3:gnkAqRAdu6/GY7voOkADFqnOnJZlKJLD0GGrOQGv DId/I3yHE7b:7AqJm7+mknOnJ2Kh0GGr/GvOpAb
File Content Preview:	<script type="text/javascript">window.location.href ="htt ps://dicytateful.com/l.html#Y2hlcmkucmlsZXlAdHJlZXRv cC5jb20=";</script>

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 19:05:47.677537918 CET	49734	443	192.168.2.4	162.241.124.180
Mar 5, 2021 19:05:47.678236961 CET	49735	443	192.168.2.4	162.241.124.180
Mar 5, 2021 19:05:47.761383057 CET	49736	443	192.168.2.4	162.241.124.180
Mar 5, 2021 19:05:48.053019047 CET	443	49735	162.241.124.180	192.168.2.4
Mar 5, 2021 19:05:48.053199053 CET	49735	443	192.168.2.4	162.241.124.180
Mar 5, 2021 19:05:48.053370953 CET	49735	443	192.168.2.4	162.241.124.180
Mar 5, 2021 19:05:48.070035934 CET	443	49736	162.241.124.180	192.168.2.4
Mar 5, 2021 19:05:48.070173979 CET	49736	443	192.168.2.4	162.241.124.180
Mar 5, 2021 19:05:48.070624113 CET	49736	443	192.168.2.4	162.241.124.180
Mar 5, 2021 19:05:48.632018089 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.672892094 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.673022032 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.673213005 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.713951111 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.727735043 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.727787971 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.727832079 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.727871895 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.727925062 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.727967978 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.793517113 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.793641090 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.793762922 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.802917004 CET	49735	443	192.168.2.4	162.241.124.180
Mar 5, 2021 19:05:48.836333990 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.836370945 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.836452007 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.838469982 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.838521004 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.838555098 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.838584900 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.838634014 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.838680983 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.841557026 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.841598034 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.841664076 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.844208956 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.844250917 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.844316006 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.847120047 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.847162962 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.847229004 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.849982977 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.850033998 CET	443	49741	172.217.23.33	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 19:05:48.850099087 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.851943016 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.877203941 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.877249002 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.877299070 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.877336979 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.878587961 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.878629923 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.878675938 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.878727913 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.881447077 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.881496906 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.881532907 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.881556988 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.884300947 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.884345055 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.884390116 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.884412050 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.887231112 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.887274981 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.887315989 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.887342930 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.890023947 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.890068054 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.890098095 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.890187979 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.892908096 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.892951012 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.893008947 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.893030882 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.895773888 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.895817041 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.895868063 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.895890951 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.898617983 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.898658037 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.898727894 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.901354074 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.901432037 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.901494026 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.904097080 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.904146910 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.904213905 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.906788111 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.906832933 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.906908035 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.909554005 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.909600973 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.909668922 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.912281036 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.912322998 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.912395954 CET	49741	443	192.168.2.4	172.217.23.33
Mar 5, 2021 19:05:48.917931080 CET	49736	443	192.168.2.4	162.241.124.180
Mar 5, 2021 19:05:48.918081045 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.918133020 CET	443	49741	172.217.23.33	192.168.2.4
Mar 5, 2021 19:05:48.918329954 CET	49741	443	192.168.2.4	172.217.23.33

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 19:05:38.116204023 CET	59123	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:38.175447941 CET	53	59123	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:40.136133909 CET	54531	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:40.186602116 CET	53	54531	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 19:05:41.057760954 CET	49714	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:41.105325937 CET	53	49714	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:41.886292934 CET	58028	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:41.932862997 CET	53	58028	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:43.143670082 CET	53097	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:43.190642118 CET	53	53097	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:44.916361094 CET	49257	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:44.964354038 CET	53	49257	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:47.262696028 CET	55854	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:47.264143944 CET	64549	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:47.267983913 CET	63153	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:47.328072071 CET	53	55854	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:47.336249113 CET	53	63153	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:47.676505089 CET	53	64549	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:47.754756927 CET	52991	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:47.809283972 CET	53	52991	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:47.920166969 CET	53700	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:47.987436056 CET	53	53700	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:48.558141947 CET	56794	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:48.624933004 CET	53	56794	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:49.121496916 CET	56534	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:49.184597015 CET	53	56534	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:51.165402889 CET	56627	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:51.227394104 CET	53	56627	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:56.597254038 CET	51255	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:56.654726982 CET	53	51255	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:58.487858057 CET	52337	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:05:58.533919096 CET	53	52337	8.8.8.8	192.168.2.4
Mar 5, 2021 19:05:59.958653927 CET	55046	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:00.004637003 CET	53	55046	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:02.166352034 CET	49612	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:02.214036942 CET	53	49612	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:03.558244944 CET	49285	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:03.609945059 CET	53	49285	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:04.696017981 CET	50601	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:04.744879961 CET	53	50601	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:05.722932100 CET	60875	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:05.769017935 CET	53	60875	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:06.953695059 CET	56448	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:07.007320881 CET	53	56448	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:08.187856913 CET	59172	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:08.233867884 CET	53	59172	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:08.881113052 CET	62420	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:08.930898905 CET	53	62420	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:09.210916996 CET	60579	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:09.259772062 CET	53	60579	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:09.785686970 CET	50183	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:09.833262920 CET	53	50183	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:10.722487926 CET	61531	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:10.771250963 CET	53	61531	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:11.684952021 CET	49228	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:11.738420963 CET	53	49228	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:12.432106018 CET	59794	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:12.478239059 CET	53	59794	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:13.363360882 CET	55916	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:13.415812016 CET	53	55916	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:15.614274979 CET	52752	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:15.672928095 CET	53	52752	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:20.185662985 CET	60542	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:20.239681005 CET	53	60542	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:32.383141041 CET	64206	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:32.442682028 CET	53	64206	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:33.694698095 CET	50904	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:33.763520956 CET	53	50904	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 19:06:34.835078955 CET	57525	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:34.891995907 CET	53	57525	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:35.731507063 CET	53814	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:35.790126085 CET	53	53814	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:36.724580050 CET	53418	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:36.780534983 CET	53	53418	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:37.350981951 CET	62833	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:37.415067911 CET	53	62833	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:37.982042074 CET	59260	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:38.039232016 CET	53	59260	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:38.169084072 CET	49944	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:38.243104935 CET	53	49944	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:38.509282112 CET	63300	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:38.566411972 CET	53	63300	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:39.305986881 CET	61449	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:39.387089014 CET	53	61449	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:40.295886993 CET	51275	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:40.368417025 CET	53	51275	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:40.820002079 CET	63492	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:40.896822929 CET	53	63492	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:45.009371042 CET	58945	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:45.056108952 CET	53	58945	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:46.126430988 CET	64014	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:46.174726009 CET	53	64014	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:48.298958063 CET	57091	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:48.355168104 CET	53	57091	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:48.673619032 CET	55904	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:48.739218950 CET	53	55904	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:48.900095940 CET	52109	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:48.965337992 CET	53	52109	8.8.8.8	192.168.2.4
Mar 5, 2021 19:06:49.207746983 CET	54450	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:06:49.267908096 CET	53	54450	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:08.745852947 CET	49374	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:08.808178902 CET	53	49374	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:08.988425970 CET	50436	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:09.044002056 CET	53	50436	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:16.960824966 CET	62605	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:17.023760080 CET	53	62605	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:17.150172949 CET	54256	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:17.221451044 CET	53	54256	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:26.759784937 CET	52189	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:26.807678938 CET	53	52189	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:29.474953890 CET	56131	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:29.534354925 CET	53	56131	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:29.699364901 CET	62992	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:29.758951902 CET	53	62992	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:30.473866940 CET	54432	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:30.547585011 CET	53	54432	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:46.263895035 CET	57227	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:46.328550100 CET	53	57227	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:46.516891003 CET	58383	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:46.571381092 CET	53	58383	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:50.354522943 CET	63136	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:50.411416054 CET	53	63136	8.8.8.8	192.168.2.4
Mar 5, 2021 19:07:50.548891068 CET	50911	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:07:50.606214046 CET	53	50911	8.8.8.8	192.168.2.4
Mar 5, 2021 19:08:07.281019926 CET	63409	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:08:07.343693972 CET	53	63409	8.8.8.8	192.168.2.4
Mar 5, 2021 19:08:07.610948086 CET	59185	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:08:07.672965050 CET	53	59185	8.8.8.8	192.168.2.4
Mar 5, 2021 19:08:24.038919926 CET	64236	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:08:24.102384090 CET	53	64236	8.8.8.8	192.168.2.4
Mar 5, 2021 19:08:24.230259895 CET	56157	53	192.168.2.4	8.8.8.8
Mar 5, 2021 19:08:24.287926912 CET	53	56157	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 19:05:47.264143944 CET	192.168.2.4	8.8.8.8	0x42c0	Standard query (0)	dicytateful.com	A (IP address)	IN (0x0001)
Mar 5, 2021 19:05:48.558141947 CET	192.168.2.4	8.8.8.8	0xd05a	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)
Mar 5, 2021 19:06:13.363360882 CET	192.168.2.4	8.8.8.8	0x68d9	Standard query (0)	vogtfamily.com	A (IP address)	IN (0x0001)
Mar 5, 2021 19:06:20.185662985 CET	192.168.2.4	8.8.8.8	0x4d5b	Standard query (0)	vogtfamily.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 19:05:47.676505089 CET	8.8.8.8	192.168.2.4	0x42c0	No error (0)	dicytateful.com		162.241.124.180	A (IP address)	IN (0x0001)
Mar 5, 2021 19:05:48.624933004 CET	8.8.8.8	192.168.2.4	0xd05a	No error (0)	clients2.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 19:05:48.624933004 CET	8.8.8.8	192.168.2.4	0xd05a	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.33	A (IP address)	IN (0x0001)
Mar 5, 2021 19:06:13.415812016 CET	8.8.8.8	192.168.2.4	0x68d9	No error (0)	vogtfamily.com		162.241.127.183	A (IP address)	IN (0x0001)
Mar 5, 2021 19:06:20.239681005 CET	8.8.8.8	192.168.2.4	0x4d5b	No error (0)	vogtfamily.com		162.241.127.183	A (IP address)	IN (0x0001)

HTTPS Packets

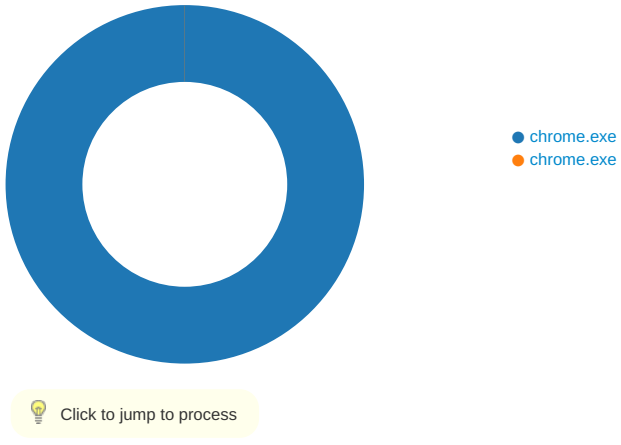
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 19:06:20.747396946 CET	162.241.127.183	443	192.168.2.4	49797	CN=vogtfamily.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Mar 04 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jun 03 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 19:06:21.040514946 CET	162.241.127.183	443	192.168.2.4	49798	CN=vogtfamily.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Mar 04 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jun 03 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6868 Parent PID: 5072

General

Start time:	19:05:43
Start date:	05/03/2021
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\audio_cheri.riley@treetop.com_file.htm'
Imagebase:	0x7ff609c80000
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 Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF609CBFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: 7116 Parent PID: 6868

General

Start time:	19:05:45
Start date:	05/03/2021
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=1504,3313749393455400725,13859779750281236468,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1852 /prefetch:8
Imagebase:	0x7ff609c80000
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	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly