ID: 458746
Sample Name: #Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm
Cookbook: default.jbs
Time: 17:55:12
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

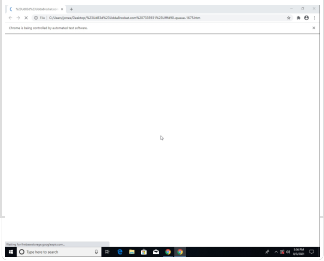
Windows Analysis Report #Ud83d#Udda8rocket.com 73…

Overview

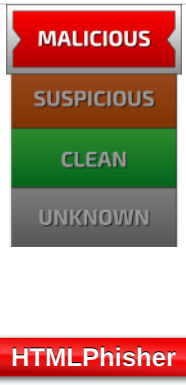
General Information

Sample Name:	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm
Analysis ID:	458746
MD5:	0861c3ccccf34eb..
SHA1:	5a0bb102052fe2b.
SHA256:	09ba757400f8a28.
Infos:	

Most interesting Screenshot:



Detection



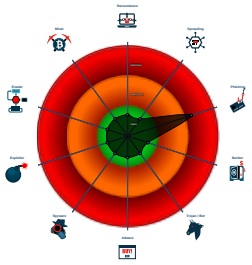
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish10
- Found iframes
- IP address seen in connection with o…
- No HTML title found
- None HTTPS page querying sensitiv…
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6584 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6832 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1592,3364816180486248382,9358393064765381631,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

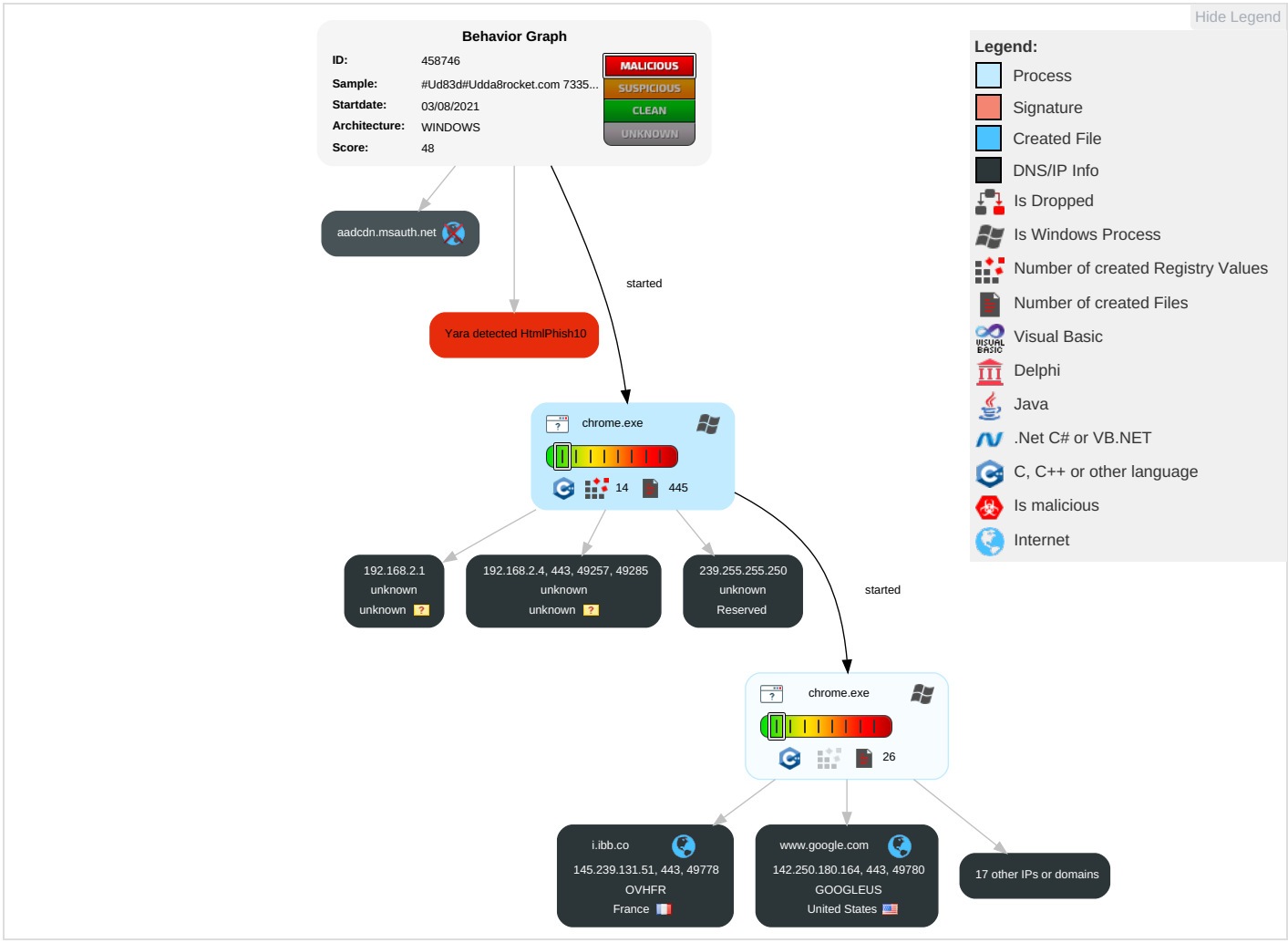
Phishing:

Yara detected HtmlPhish10

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
Drive-by Compromise 1	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	M S F
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	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

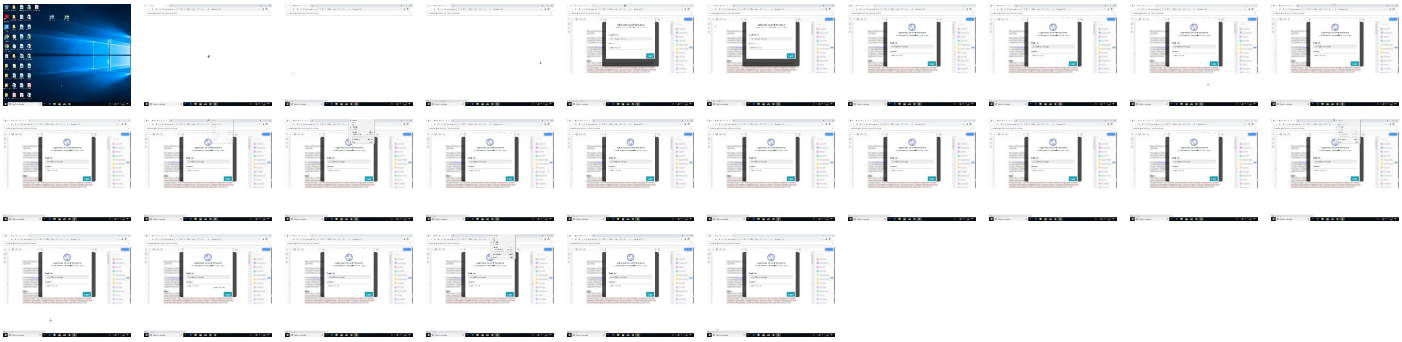
Behavior Graph

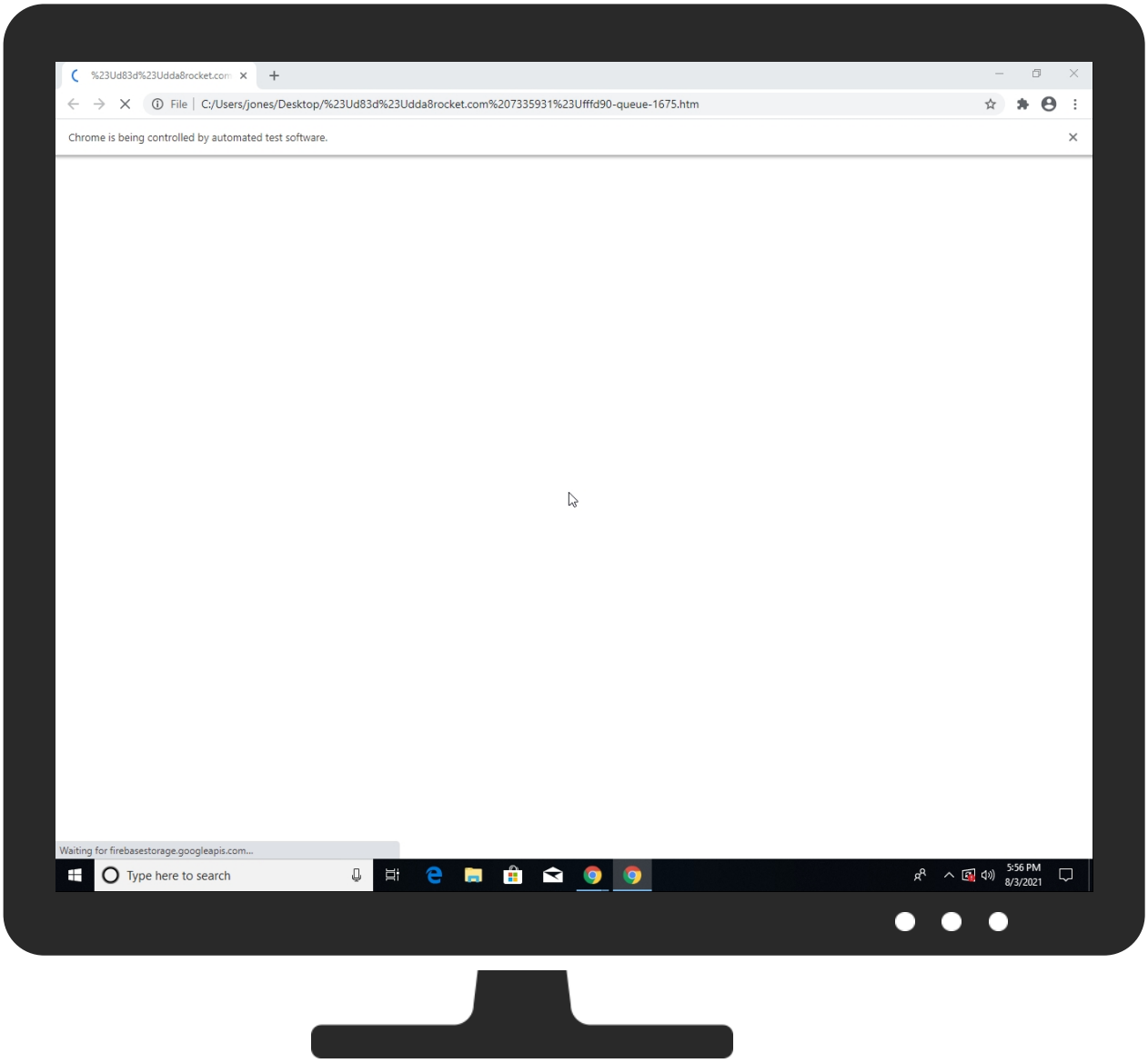


Screenshots

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

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
api.statvoo.com	0%	Virustotal		Browse
api-images.statvoo.com	0%	Virustotal		Browse
aadcdn.msftauth.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/FaviconHttp/external	0%	Avira URL Cloud	safe	
http://https://anti-acne.co/wp-includes/office/mail.php	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://api.statvoo.com	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	216.58.198.3	true	false		high
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	216.58.205.77	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
www.google.com	142.250.180.164	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
api.statvoo.com	172.67.159.15	true	false	• 0%, Virustotal, Browse	unknown
api-images.statvoo.com	104.21.41.23	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	216.58.208.161	true	false		high
i.ibb.co	145.239.131.51	true	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
aadcdn.msauth.net	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
login.microsoftonline.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/%23Ud83d%23Udda8rocket.com%207335931%23Ufffd90-queue-1675.htm	true		low
http://https://login.microsoftonline.com/logout.srf	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
145.239.131.51	i.ibb.co	France		16276	OVHFR	false
216.58.198.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
142.250.180.164	www.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
172.67.159.15	api.statvoo.com	United States		13335	CLOUDFLARENETUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458746
Start date:	03.08.2021
Start time:	17:55:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.winHTM@34/224@15/13
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:56:19	API Interceptor	2x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
145.239.131.51	VUBuRErqKh.dll	Get hash	malicious	Browse	
	Pay Slip- No-$142,851.53.html	Get hash	malicious	Browse	
	ADI INV-RECON #_891976.html	Get hash	malicious	Browse	
	securedocs _56797_9166.html	Get hash	malicious	Browse	
	Tax Folder.doc	Get hash	malicious	Browse	
	#Ud83d#Udda8rocket.com 1208421(69-queue-2615.htm	Get hash	malicious	Browse	
	treetop-payroll-075491-pdf.HtmL	Get hash	malicious	Browse	
	hibudhotel-payroll-607512-pdf.HtmL	Get hash	malicious	Browse	
	$108,459.00.html	Get hash	malicious	Browse	
	billykang_payment-advice.htm	Get hash	malicious	Browse	
	WSSG INV RECON _ 302456_10920.HTML	Get hash	malicious	Browse	
	dechert-Investment078867-xlsx.Html	Get hash	malicious	Browse	
	1076897 (1).HTML	Get hash	malicious	Browse	
	mferreira@itpros.us.com.pff.HTM	Get hash	malicious	Browse	
	Sid.dll	Get hash	malicious	Browse	
	VoIP-Byungil.lim.HTM	Get hash	malicious	Browse	
	Payment Advice.xlsx	Get hash	malicious	Browse	
	cremocompany-Invoice_216083-xlsx.html	Get hash	malicious	Browse	
	#U260e#Ufe0f.htm	Get hash	malicious	Browse	
	#U260e#Ufe0f.htm	Get hash	malicious	Browse	
172.67.159.15	Fax-Message-to-sandbox.htm	Get hash	malicious	Browse	
	(786) 274-1357-Hartmann.info.html	Get hash	malicious	Browse	
	treetop-payroll-075491-pdf.HtmL	Get hash	malicious	Browse	
	redcape.com.au-857585.htm	Get hash	malicious	Browse	
	ATT54364.html	Get hash	malicious	Browse	
	hibudhotel-payroll-607512-pdf.HtmL	Get hash	malicious	Browse	
	glumac-payroll-530666-pdf.HtmL	Get hash	malicious	Browse	
	dot_invoice_Tuesday 05042021._xslx.hTML	Get hash	malicious	Browse	
	dot-payroll-492220-pdf.HtmL	Get hash	malicious	Browse	
	holla.htm	Get hash	malicious	Browse	
	#Ud83d#Udce9.htm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	ATT66004.HTM	Get hash	malicious	Browse	• 104.16.19.94
	BadFile.HTM	Get hash	malicious	Browse	• 104.16.18.94
	ATT17444.HTM	Get hash	malicious	Browse	• 104.16.19.94
	ATT75446.HTM	Get hash	malicious	Browse	• 104.16.18.94
	ATT23582.HTM	Get hash	malicious	Browse	• 104.16.18.94
	HTM.html	Get hash	malicious	Browse	• 104.16.19.94
	ATT96886.HTM	Get hash	malicious	Browse	• 104.16.18.94
	ATT04604.HTM	Get hash	malicious	Browse	• 104.16.19.94
	SBSA_Statement_2021-07-29.pdf.html	Get hash	malicious	Browse	• 104.16.18.94
	Encova.com_Fax-Message.htm	Get hash	malicious	Browse	• 104.16.18.94
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	Ach Remittance advice.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	ATT22486.htm	Get hash	malicious	Browse	• 104.16.19.94
	ATT07001.htm	Get hash	malicious	Browse	• 104.16.18.94
	ATT26728(1).htm	Get hash	malicious	Browse	• 104.16.19.94
	.htm.htm	Get hash	malicious	Browse	• 104.16.19.94
	.htm.htm	Get hash	malicious	Browse	• 104.16.18.94
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.16.19.94
	Subscription_AgreementJuly 28, 2021-25496344.HTM	Get hash	malicious	Browse	• 104.16.18.94
	ATT96756.htm	Get hash	malicious	Browse	• 104.16.19.94
cs1100.wpc.omegacdn.net	psconstruction.ca Attachment.htm	Get hash	malicious	Browse	• 152.199.23.37
	OneDrive-besked.htm	Get hash	malicious	Browse	• 152.199.23.37
	phish.html	Get hash	malicious	Browse	• 152.199.23.37
	Medius.html	Get hash	malicious	Browse	• 152.199.23.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Aging invoice.html	Get hash	malicious	Browse	• 152.199.23.37
	globalfoundries_MNT484_XEROStubs_XjJzNZsjSWLmtRAHrKczAOlwztYjTcVMspUZaJnMJERgMTdevl.HTML	Get hash	malicious	Browse	• 152.199.23.37
	It.servicedesk-it.servicedesk@ovolohotels.com.html	Get hash	malicious	Browse	• 152.199.23.37
	VM 1min.htm	Get hash	malicious	Browse	• 152.199.23.37
	Prosserhealth.html	Get hash	malicious	Browse	• 152.199.23.37
	Convert HEX uit phishing mail.htm	Get hash	malicious	Browse	• 152.199.23.37
	192-3216-Us.gt.com.html	Get hash	malicious	Browse	• 152.199.23.37
	voice mail.html	Get hash	malicious	Browse	• 152.199.23.37
	New Working C0D377B99993939393939939.htm	Get hash	malicious	Browse	• 152.199.23.37
	20210714_110346.html	Get hash	malicious	Browse	• 152.199.23.37
	qET1iJuly 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 152.199.23.37
	July 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 152.199.23.37
	It.servicedesk_FAXit.servicedesk@ovolohotels.com.html	Get hash	malicious	Browse	• 152.199.23.37
	Globalfoundries#Scanned-thomas.caulfield.html	Get hash	malicious	Browse	• 152.199.23.37
	Deepspacesystems Signed Waiver .html	Get hash	malicious	Browse	• 152.199.23.37
	deepspacesystems_fxdocstub-jwuKfDGIIoVteWuSsmBhNalGOOjkUsDfVlSBHLFvYbMhqYpqCi.HTM	Get hash	malicious	Browse	• 152.199.23.37

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	ATT66004.HTM	Get hash	malicious	Browse	• 104.16.19.94
	JUP2A9ptp5.exe	Get hash	malicious	Browse	• 104.21.19.200
	7vd7MuxjGd.exe	Get hash	malicious	Browse	• 104.21.92.87
	xar2.dll	Get hash	malicious	Browse	• 172.67.70.134
	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• 23.227.38.74
	BadFile.HTM	Get hash	malicious	Browse	• 104.16.18.94
	Stolen Images Evidence.js	Get hash	malicious	Browse	• 104.21.95.9
	LOPEZ CV.exe	Get hash	malicious	Browse	• 104.21.19.200
	Stolen Images Evidence.js	Get hash	malicious	Browse	• 104.21.95.9
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	banload.msi	Get hash	malicious	Browse	• 104.23.98.190
	PO_1994.exe	Get hash	malicious	Browse	• 172.67.188.154
	bothlee2010.exe	Get hash	malicious	Browse	• 172.65.232.115
	D0CUMENT DE ENV#U00cdO.pdf.exe	Get hash	malicious	Browse	• 104.21.39.75
	temple.exe	Get hash	malicious	Browse	• 104.21.19.200
	CyLELjM5zk.exe	Get hash	malicious	Browse	• 104.21.70.98
	gunzipped.exe	Get hash	malicious	Browse	• 104.23.99.190
	RFQ_20210518_131536.doc	Get hash	malicious	Browse	• 104.21.19.200
	Remittance copy.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	09087900900000000.exe	Get hash	malicious	Browse	• 172.67.188.154
OVHFR	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• 51.83.52.226
	KNZot6bpK5.exe	Get hash	malicious	Browse	• 51.254.69.209
	SARS_DOCUMENT - Copy.html	Get hash	malicious	Browse	• 145.239.131.55
	FaHdx8tldN.exe	Get hash	malicious	Browse	• 51.79.243.236
	DZzq7ovMzl.apk	Get hash	malicious	Browse	• 178.32.130.175
	SPARE PARTS Provision_pdf.exe	Get hash	malicious	Browse	• 198.50.252.64
	R5L9IoaG67.exe	Get hash	malicious	Browse	• 51.79.243.236
	4d97a3f97aeeebb6e15603acba4108e09254581222131.exe	Get hash	malicious	Browse	• 149.202.65.221
	sVE1ufLR4J	Get hash	malicious	Browse	• 51.79.65.49
	b7l3YhX4ij	Get hash	malicious	Browse	• 51.79.65.49
	OPL7aedXuH	Get hash	malicious	Browse	• 51.79.65.49
	iFMr2HSJ1l	Get hash	malicious	Browse	• 51.79.65.49
	M6aFOA0ME5	Get hash	malicious	Browse	• 51.79.65.49
	spiYcxfKrv	Get hash	malicious	Browse	• 51.79.65.49
	cfVMvZPHsZ	Get hash	malicious	Browse	• 51.79.65.49
	2957K5pvQb	Get hash	malicious	Browse	• 51.79.65.49
	Installer.exe	Get hash	malicious	Browse	• 91.121.146.23
	U7m2xUJY8L.exe	Get hash	malicious	Browse	• 54.37.125.37
	ZIRIr99ard.exe	Get hash	malicious	Browse	• 54.37.125.37
	KClSJbbY7X	Get hash	malicious	Browse	• 192.99.154.65

JA3 Fingerprints

No context

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, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	122040
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	3072:0tdeYPiuWAVtlLBGbtdeYPiuWAVtlLBGm:0rec7VDBGbrec7VDBGm
MD5:	516136E560C1392A28EDFA1A957050D7
SHA1:	BBDF208E48EFC052D332255EF84184BFC946BF5F
SHA-256:	4F812F7C8163C50FE75F441AC6797E18D02B8B66895BC94D0E1153FE24FADEFE
SHA-512:	8F25750E9014F7576E5C81E1A3DE605BB29839A38F0E60D58AB79E034ED1847D9E88A427A834BCA95BF7C4627197AC1194D5A487E0D5E5F88B95E46C4574A425
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....\.....,.....I.....l.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$...._.Y..Y`&..s.1.....s.{..,."':o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...l.....D0.....Ba...Z.0.o..l.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f\|.*...'^K`\..e.....j/..\|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.[]}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.138306953121762
Encrypted:	false
SSDEEP:	12:G5kPlE99SNxAhUe0ec+5kPlE99SNxAhUe0et:G5kPcUQUfec+5kPcUQUfet
MD5:	DBC09B0669DAFFBD2BC9600000069DED
SHA1:	8498438958319762E4E5073BE333E3DFC6420BB7
SHA-256:	41BA5794108AF3F3B2843330720D314887102644A4C6A4705AF5D206FA2A3A6E
SHA-512:	CE665CE20DC5BF90ECC21F8F9C5D0EA8A5E936D029B9DE5843EA234F71002388389C789E2DEE52C50DEC68351AC2015750801D1B50A811D0CAC05BCBB3501E 8
Malicious:	false
Reputation:	low
Preview:	p..... .....s.....(..... .....T'._.....$.....\...h.t.t.p.:././/.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...p..... ..... >+....(..... .....T'._.....$.....\...h.t.t.p. :././/.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\003cbe01-3ca9-4c61-8f9b-95477d634036.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):	174390
Entropy (8bit):	6.0796951644131845
Encrypted:	false
SSDEEP:	3072:GCAicfpuYAZ20//XkjhbEkzrw7hFcbXafIB0u1GOJmA3iuRZ:nAlpUubULaqfIlUOoSiuRZ
MD5:	00E3761D1A94DB23E61313F8DA399BE6
SHA1:	FBA51CF0ED757F5982FA7F407E62F7B64BC9A147
SHA-256:	3CAD77FF22163552AE77A8A813BBDB38A8D4090159450BC6D5F0DACDA579EFD1
SHA-512:	3573F6CA87484E2C1E8FD1F40DE4D2EC92A2F6DD7A771C3940F4814BC3AD859563004327F0C0784B534C9C3E56834807EC1F1F1EB82DB99B5DCEDE6B2FF1CB 8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\003cbe01-3ca9-4c61-8f9b-95477d634036.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628006178758276e+12,"network":1.62800618e+12,"ticks":4013174559.0,"uncertainty":4284321.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+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\0e34b72f-8af4-4b4d-80ae-92351ced855b.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):	174390
Entropy (8bit):	6.079695382300019
Encrypted:	false
SSDEEP:	3072:G8sicfpuYAZ20//XkjhbEkzrw7hFcbXafIB0u1GOJmA3iuRZ:hslpUubULaqfIlUOoSiuRZ
MD5:	FC897A595A43D2BE9098CE8A16A79427
SHA1:	5FA1FB973FE74E81DB7BCF0F3A3A2A684C7D0A54
SHA-256:	B86D4275FA43DBF51A6ADFFAF58DF3E9C9A6B5DC684B69AD82C65EC8C1141C5F
SHA-512:	397A3010E1204CE39B4B0E0FF5B6DFDAE9CE969CCFC2944F1DA44E3F22D95C59B71A7AC837F80DB526407198E3C66FFA16756DD1730AD70065D982F1C605B8
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":1.628006178758276e+12,"network":1.62800618e+12,"ticks":4013174559.0,"uncertainty":4284321.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+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\12bdd1d1-5384-4aaf-aae4-fce394af02ad.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.749454308522369
Encrypted:	false
SSDEEP:	384:LrIH3tK0d1aLmNTr4vvV3YnN0HdUGUDre5DPxl5pNori/ma96l7LbEOBJzN21zyO:Aa11yxUEcervhxQXfu9Kf1bZZa
MD5:	D178602CC1A526EA9D10D86CF5EF5799
SHA1:	50E56EF0DE301E4407C8F31399C675316AD0CE11
SHA-256:	35A03BBD01521841A2D5AC7EA471FC44246907F3D9BEB372E9F3FA57BC77CE21
SHA-512:	FC604249C077B44BC6E4B538510226DD06245E30169049FFEE1ECF3184BBC4F14DF95BB8DDBBBD24B2BE4726A6329354541FF57436E9C4352F78FB39A031B478
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.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\12f6a51f-b993-4fbd-9071-4c57145df059.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):	174390
Entropy (8bit):	6.079695718196347
Encrypted:	false
SSDEEP:	3072:38sicfpuYAZ20//XkjhbEkzrw7hFcbXafIB0u1GOJmA3iuRZ:sslpUubULaqfIlUOoSiuRZ
MD5:	62F11C1893225EC2815DFC0190B01F7D
SHA1:	B3F56E488FE26DCBBE29EC834C3DDC1463B1C0C7
SHA-256:	60723CF402D866EB7A3E02D9E06D0BAE1DA4E995E29D536D2141F4C009AC1120
SHA-512:	5C3C0DA475F46F32B94A73C8500E94035E0FEFE994B5D608709385396D43F18BA987338F9F174EAA58D583122D3777C3D3F9EFB20834CEEF7FDEE2C0B7CCAE4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\12f6a51f-b993-4fbd-9071-4c57145df059.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628006178758276e+12,"network":1.62800618e+12,"ticks":4013174559.0,"uncertainty":4284321.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715624247"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\13c34c8b-9614-4494-a8ce-f47c62702b79.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7499796303527435
Encrypted:	false
SSDEEP:	384:lrIH3tK0xu1JVW8LmNTr4vvV3YnN0HdUGUDre5DPxI5pNori/ma96l7LbEOBJzNO:lGa11yxUEcervhxQXfu9Kf1bZa
MD5:	743285B6CCE241800306A28CB6CDE443
SHA1:	20B43164075CB29155D34607750C52876F3FC6CA
SHA-256:	3019CAFCFBCB775214C3EAF96D5BDB96BF1143625FD2BA8296D106422AB56C55
SHA-512:	0E236E5270F93F50C5EBBF685C9B6D4B32D0D6A211A7BCF0B93A698EF1B9C6F83EC6445108A4F83BD061889B01834D697E99D194207D291403A5D475C1FACC6
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....A8.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\6579b264-85e1-47ac-bdc0-0c6fc2d7bd38.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):	166123
Entropy (8bit):	6.050642163691906
Encrypted:	false
SSDEEP:	3072:UicfpuYAZ20//XkjhbEkzrw7hFcbXafIB0u1GOJmA3iuRZ:UlpUubULaqfIlUOoSiuRZ
MD5:	3F0B62E2D00144CECE6507D33DC800E9
SHA1:	A9D8B7ADC128C1D1124F1B665E478633F5D7ABB8
SHA-256:	792B25BBB5CE33EC44E2CF4A2262B5F8E8585F5B4F8BA4E550E8D2C47F8F13DC
SHA-512:	B5B1F36637AFD5A57250CA6F0B01CD7632B2A535427A068372FA94D14E5E61388222747C7D1CEF6E3C2FDC9BC1DD212E168424C3E061844ED5833BAC515EE79
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":1.628006178758276e+12,"network":1.62800618e+12,"ticks":4013174559.0,"uncertainty":4284321.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715624247"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\8d6a1b73-db4a-4450-9e66-7a961b3f3326.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7498175700543377
Encrypted:	false
SSDEEP:	384:VrIH3tK0xu1JVW8LmNTr4vvV3YnN0HdUGUDre5DPxI5pNori/ma+g6l7LbEOBJz6:1Ga11yx0EcervhxQXfu9Kf1bZU
MD5:	009CC6C8CF9B263FE50CBD601EAF407D
SHA1:	0F8B8E97E8EB4A9AFBCDB6EF79694CAE710B5444
SHA-256:	A514CC46B02C3F2869748341E8E72257F3883EEA03A71822E20B8E4C283C69EE
SHA-512:	174B1D56E32D4A5F494C8D35D4670A9DA3AC2F9FC4DA6D5F6E1B917FEC74348908D1485BDB9B1D9C0C6A115AD03F1BC168FA06129002C48E4CA6DD0B500271 5
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\8d6a1b73-db4a-4450-9e66-7a961b3f3326.tmp	
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.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\8e797e35-4aa9-42c6-8bec-39b6d197fc5e.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):	165925
Entropy (8bit):	6.050068791744396
Encrypted:	false
SSDEEP:	3072:QicfpuYAZ20//XkjhbEkzrw7hFcbXafIB0u1GOJmA3iuRZ:QlpUubULaqfIlUOoSiuRZ
MD5:	CDD224E24601E0B6B8291A7DCDC983FF
SHA1:	B6CD464A63E9E996B4642CFF26BC6EAF79B0FAE4
SHA-256:	8D87ACE77E69CCCEB1345ECC5510D5683CF05B94237E15747D70E58F84B20508
SHA-512:	40C3FA9A4103FF287B5CE4A7B8406420E194127ECCC41E91C4BC36B5D7A0CD91F4F16B325DD40468E8F3F41F381116642B679DC36264E4C972798201F5FA8BA7
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":1.628006178758276e+12,"network":1.62800618e+12,"ticks":4013174559.0,"uncertainty":4284321.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715624247"},"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
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\02cb1fa7-c2c5-4f81-94aa-d63a2a212fc9.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):	1540
Entropy (8bit):	5.586894825702751
Encrypted:	false
SSDEEP:	48:YgYVwUvUF6UUhd0KUKLYqPeUekUezwUwrsYUaEPUeP:n3UvUMUUIKUUHPeU3UJU7YUpPUg
MD5:	D5420ED23C61CB6A9439C145D78FF8D7
SHA1:	53034DA920D08C69C93EAF0E2A6DD636995D6E23
SHA-256:	81101866E0DD306A27A585EA4B1252282BC180DCCD90C15BF11100AF872CA758
SHA-512:	04F352094DA8B6BEB021560DEA555A7214FFA91AB89E45386DA7D6DFC0A7382A92EE34B868F0112EF568D2AEAF3639903321721603BA4BCE919A4D964B079872
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1643786178.967912,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628006178.967918},{"expiry":1659542179.00608,"host":"F8CDsiT0h6lTN4Nqwoyb2wNyqqjWSTsRj/gzlYU3NfY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628006179.006088},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbl1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659542178.96927,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628006178.969275},{"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_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\110c3eca-f24c-43c3-bf8d-c7d34aa964d6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\110c3eca-f24c-43c3-bf8d-c7d34aa964d6.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5487
Entropy (8bit):	5.161932349334823
Encrypted:	false
SSDEEP:	96:nYLvT9WTMEBdgNIKIW5k0JCKL8bbOTlVuHn:nYLb9/NIMh4Km
MD5:	565435D73E96C4BD114CFA75738D31E8
SHA1:	A8FAE24B8E447F1E371B8368500F7684F5D39D20
SHA-256:	6DD171AC18F7629FCB4064EF6D2ACDA792A2CD306D66C2201598F1B4469346E3
SHA-512:	58DBB4E138156FD08CBC53FADE211DA66A8538E9704079871DF009B1ECDD98874970F9FF352A49581CCC3C21A67DE5F20373D58DC797A6B1AFE3363DCB8523E 2
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272479774032231","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":{"default_browser_infobar_last_declined":"13245924607060180","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_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\12e6e45b-2728-46bf-aac3-84e751a93519.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):	5513
Entropy (8bit):	5.164698683842019
Encrypted:	false
SSDEEP:	96:nYLST9WTMEBdgNIKIW5k0JCKL8tbOTlVuHn:nYLs9/NIMh4Kk
MD5:	7C61C3B6E1D2589C937214DCC2FEF99D
SHA1:	6D5674E2A1D72DFEE290CE484E3441BA6D7EFECB
SHA-256:	1824DE9CB2032A87DDBFF8F4B89AC91D4CF458B56C96E9858F5221F6027141F9
SHA-512:	7E424BAEF58732F7F0E05FA690B1FED619A36DC78DB6FF00330C68B958A4A9F386151683CBB26C6BA2FBDCC927D5CEE5BE8A0D9C3E79D3D95A2730B8552EF8 B4
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272479774032231","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":{"default_browser_infobar_last_declined":"13245924607060180","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_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1970a5ab-9545-4d36-8e91-3efc08c9d2e6.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):	5513
Entropy (8bit):	5.164668913030689
Encrypted:	false
SSDEEP:	96:nYLbT9WTMEBdgNIKIW5k0JCKL8tbOTlVuHn:nYL39/NIMh4Kk
MD5:	A86BE63275805B43A4118860DBFAF175
SHA1:	39148DA6EDA092034D9AD613FB725C08120A87FD
SHA-256:	3A0C2BB7DB686016A81BEE5950C998C2539938AEE7C9E74999D4BC7F15484CF2
SHA-512:	1398ACD9DD5853FA38F5BDE902925F969BBBD291C5C0B6E46A28AA336399E7BB688F173DEF948AE953F3E727C549946978283DCF62364FE50BAA9FCF19A130D B
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272479774032231","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":{"default_browser_infobar_last_declined":"13245924607060180","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_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\231e5485-0abd-48de-a5a7-f4a7a9abdfe4.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):	5513
Entropy (8bit):	5.164698683842019

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\231e5485-0abd-48de-a5a7-f4a7a9abdfe4.tmp	
Encrypted:	false
SSDEEP:	96:nYLST9WTMEBdgNIKIW5k0JCKL8tbOTlVuHn:nYLs9/NIMh4Kk
MD5:	7C61C3B6E1D2589C937214DCC2FEF99D
SHA1:	6D5674E2A1D72DFEE290CE484E3441BA6D7EFECB
SHA-256:	1824DE9CB2032A87DDBFF8F4B89AC91D4CF458B56C96E9858F5221F6027141F9
SHA-512:	7E424BAEF58732F7F0E05FA690B1FED619A36DC78DB6FF00330C68B958A4A9F386151683CBB26C6BA2FBDCC927D5CEE5BE8A0D9C3E79D3D95A2730B8552EF8 B4
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272479774032231","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":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2f16e91f-8bd9-4bbf-9ffb-01bec3571ff6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\387859a6-e42b-4b7b-b9a6-86a48cc6c2ad.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):	4891
Entropy (8bit):	4.935551630563578
Encrypted:	false
SSDEEP:	48:YcYkKSChkliLqAOqqTlYGlQKHoTw0wrf4MqM8C1Nfct/9BhUJo3KhmeSnpNGzFen:nYLkt9pIKIW5k0JCKL8bbOTlVuHn
MD5:	AFDBE409557F5D43CC7187A631A4F6BA
SHA1:	6D940CFA5F5923D00849A3367DEC78882145C53D
SHA-256:	2A76F3C6757FC111D42CD4064F700A65492DE3E110637BDC342FC0DC9C3A5AD1
SHA-512:	5CF220A08C5577CE9C3820DBFA2CAA0253E23BF63D8C24C8BDF5B026DE74382E97A465479C9FF546A3A56C18E498EE52DA30F597C1F361AB363D6D5D00C4E8 A
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272479774032231","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":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\42bdf1da-b1e6-4bee-a3e5-f6e15b8db971.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):	5513
Entropy (8bit):	5.164698683842019
Encrypted:	false
SSDEEP:	96:nYLST9WTMEBdgNIKIW5k0JCKL8tbOTlVuHn:nYLs9/NIMh4Kk
MD5:	7C61C3B6E1D2589C937214DCC2FEF99D
SHA1:	6D5674E2A1D72DFEE290CE484E3441BA6D7EFECB
SHA-256:	1824DE9CB2032A87DDBFF8F4B89AC91D4CF458B56C96E9858F5221F6027141F9
SHA-512:	7E424BAEF58732F7F0E05FA690B1FED619A36DC78DB6FF00330C68B958A4A9F386151683CBB26C6BA2FBDCC927D5CEE5BE8A0D9C3E79D3D95A2730B8552EF8 B4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\42bdf1da-b1e6-4bee-a3e5-f6e15b8db971.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272479774032231","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":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4c3be495-94ca-405f-b39b-a4e3f998620d.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):	5513
Entropy (8bit):	5.164698683842019
Encrypted:	false
SSDEEP:	96:nYLST9WTMEBdgNIKIW5k0JCKL8tbOTlVuHn:nYLs9/NIMh4Kk
MD5:	7C61C3B6E1D2589C937214DCC2FEF99D
SHA1:	6D5674E2A1D72DFEE290CE484E3441BA6D7EFECB
SHA-256:	1824DE9CB2032A87DDBFF8F4B89AC91D4CF458B56C96E9858F5221F6027141F9
SHA-512:	7E424BAEF58732F7F0E05FA690B1FED619A36DC78DB6FF00330C68B958A4A9F386151683CBB26C6BA2FBDCC927D5CEE5BE8A0D9C3E79D3D95A2730B8552EF8B4
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272479774032231","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":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5e94e920-430e-447f-8cbd-a519951d7d87.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):	22602
Entropy (8bit):	5.5357630135379035
Encrypted:	false
SSDEEP:	384:Vm5toLlrbXA1kXqKf/pUZNCgVLH2HfD9rU+HGPnZBt1px4D:hLlfA1kXqKf/pUZNCgVLH2HfxrUuGPns
MD5:	3C6EBEF215B0D85A8CADDB11BFA1715D
SHA1:	A3E0ED0A69270E2E0CE278BE03D7E7403B9AEE57
SHA-256:	C862D7CA3C94D11A7566E095FF77E4FA8C09C94B19D946F2BE5E2F10F9D72973
SHA-512:	8ABD3EFAEE79357C3BD65F2165A818F818D5EAAB6E48EEE723FB5AE162EF3697BFD131A62E0103DBC9BFA67B5241988A72C84F1231EE29AB25ACD7AE4FE888E
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":"13272479773643030","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\851ff2f8-f3bb-4f1b-bd1b-193bf3274b1f.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):	1876
Entropy (8bit):	5.582800683818056
Encrypted:	false
SSDEEP:	48:YgYVwUvUK2wUK86UUhd0KUKLYqPeUekUef+UKoFwUwrsYUaEPUeP:n3UvUiUOUUIKUUHPeU3UU+U9GU7YUpPt
MD5:	2915E51F258E33B405E2ABCCA5F7DC5E
SHA1:	CE6E8C0ADD766D8A3FB3EF12BD33A62F1A0BF322
SHA-256:	9281E4C162C8D597FCE0F6F32269735BADAC3B3E6BAA739DE0FC6203F6FC9E21
SHA-512:	30CEB6607A3E36E36111DC16E8E2CA0CCBA6D5575DACE3E0D5EE591E9AB656A37693C66231727C826E9D321A4E029A2EF92C49152839B104F51EAA73DF80CEC
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\851ff2f8-f3bb-4f1b-bd1b-193bf3274b1f.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1643786178.967912,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628006178.967918},{"expiry":1659542179.00608,"host":"F8CDsiT0h6lTN4Nqwoyb2wNyqqjWSTsRj/gzlYU3NfY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628006179.006088},{"expiry":1643558241.396162,"host":"MmvkdkL5VfySrkgf46RcMa812w+Y8Zl7wGpCsfjsbSc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628006241.396168},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbl1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659542178.96927,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628006178.969275},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\90bed1ff-3e54-42e0-9bc6-27d8de7a07af.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577269342901512
Encrypted:	false
SSDEEP:	384:Vm5tJLlrbXA1kXqKf/pUZNCgVLH2HfD9rUPtopx4k:SLlfA1kXqKf/pUZNCgVLH2HfxrUP+T/
MD5:	E722F61F30E94B568F03732DAE56059F
SHA1:	4977A1E4D7249122478103B24313EC0225BE2D14
SHA-256:	75E0DCF320FDE8CD3C9720FA44E7B58DCBE38CEB5A4826D915A15D5FAE752C7B
SHA-512:	99BA5DE0CA9170219E31C8F2C43E1525D47FBCE22550061D022334734F8A5F4B57B4E99D9A87DE8D9ADC3B41F20766F55EEB4BF0450C2C131B7508AFCE70DAAB
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":"13272479773643030","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.287578504606681
Encrypted:	false
SSDEEP:	6:moML4q2Pwkn23iKKdK9RXXTZIFUtpTM5LJZmwPTM5LDkwOwkn23iKKdK9RXX5LJ:jMMvYf5Kk7XT2FUtpTM59/PTM5P5Jf51
MD5:	841B3010D404F2B15C639E67EA985053
SHA1:	E69818829F26FC2D140613BBB33AE8DBF446DCC7
SHA-256:	D017C29FC341919051C56330A79A233E9A052CB163DF5429A9B3CF64DA4DBC73
SHA-512:	79F72D15B05D5FEE0E3F2E3236210636065DB22588AD3EF9CA266AA88A2B83FA4A706053FF158112707BD6243F847F1C43DF81F643FE9F6C9FE40857CC6DA466
Malicious:	false
Preview:	2021/08/03-17:56:28.677 1d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-17:56:28.679 1d04 Recovering log #3.2021/08/03-17:56:28.679 1d04 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\AutofillStrikeDatabase\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.287578504606681
Encrypted:	false
SSDEEP:	6:moML4q2Pwkn23iKKdK9RXXTZIFUtpTM5LJZmwPTM5LDkwOwkn23iKKdK9RXX5LJ:jMMvYf5Kk7XT2FUtpTM59/PTM5P5Jf51
MD5:	841B3010D404F2B15C639E67EA985053
SHA1:	E69818829F26FC2D140613BBB33AE8DBF446DCC7
SHA-256:	D017C29FC341919051C56330A79A233E9A052CB163DF5429A9B3CF64DA4DBC73
SHA-512:	79F72D15B05D5FEE0E3F2E3236210636065DB22588AD3EF9CA266AA88A2B83FA4A706053FF158112707BD6243F847F1C43DF81F643FE9F6C9FE40857CC6DA466
Malicious:	false
Preview:	2021/08/03-17:56:28.677 1d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-17:56:28.679 1d04 Recovering log #3.2021/08/03-17:56:28.679 1d04 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.2418387994674065
Encrypted:	false
SSDEEP:	6:moe4q2Pwkn23iKKdKyDZIFUtpTOuJZmwPTuBDkwOwkn23iKKdKyJLJ:j9vYf5Kk02FUtpTd/PTW5Jf5KkWJ
MD5:	0AC732B3DEB6147267B4BB1DD693B5DD
SHA1:	D648E74442D15BF918658A19BA0B8E58BEAF14FA
SHA-256:	AC4B3C7D51B4E9A08BD3D0C371974FC7210443DCE638445B45584391A4712EF3
SHA-512:	5237E4786B0872D16BA64FDDB20C54EECA9D5B69D282FF592022339F6F42A28D16BE42D6851F4EE693D8EC0C62404A1571E732329087C0D38737E820E021DEF0
Malicious:	false
Preview:	2021/08/03-17:56:28.640 1d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-17:56:28.658 1d04 Recovering log #3.2021/08/03-17:56:28.660 1d04 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\BudgetDatabase\LOG.oldz. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.2418387994674065
Encrypted:	false
SSDEEP:	6:moe4q2Pwkn23iKKdKyDZIFUtpTOuJZmwPTuBDkwOwkn23iKKdKyJLJ:j9vYf5Kk02FUtpTd/PTW5Jf5KkWJ
MD5:	0AC732B3DEB6147267B4BB1DD693B5DD
SHA1:	D648E74442D15BF918658A19BA0B8E58BEAF14FA
SHA-256:	AC4B3C7D51B4E9A08BD3D0C371974FC7210443DCE638445B45584391A4712EF3
SHA-512:	5237E4786B0872D16BA64FDDB20C54EECA9D5B69D282FF592022339F6F42A28D16BE42D6851F4EE693D8EC0C62404A1571E732329087C0D38737E820E021DEF0
Malicious:	false
Preview:	2021/08/03-17:56:28.640 1d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-17:56:28.658 1d04 Recovering log #3.2021/08/03-17:56:28.660 1d04 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):	24576
Entropy (8bit):	3.1176394881449014
Encrypted:	false
SSDEEP:	96:dNwOnscfsLrQsZ36UszFzs5sc0sYs6sHVDQZcLsHffmosHjVUs8sascJsasOls4+:duZRKDFfZmXEOdfuDE5RKDFApmXUOd
MD5:	89EE4857FADA08212D368CD8676CB905
SHA1:	0ED6FA738DA2A74A8C948926297ECCBF3EDF4E67
SHA-256:	1BEB115B7BEB76942E3F4269BDE4860009313A28DC5FC464EAA1A8031A8123D2
SHA-512:	8C43FAE60005CB487EC0BE3469B7EA5B4FFF29F00C15C77C99D2198FBAEE9E2363BB54AF38C99F9B62D16CC293175C0817147AC02050659B8B5C363D993B4CA9
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):	25672
Entropy (8bit):	1.961774181151863
Encrypted:	false
SSDEEP:	96:AuINAcNwWRRnscfsLrQsZ36UszFzs5sc0sYs6sHVDQZcLsHffmosHjVUs8sCscJ/:AuINAcuW4RKDFfZmXgOdFMuY
MD5:	8214E16C0A86A5A6C916C3E093C625A0
SHA1:	B700CF0C050A13ADE316BACFAF403DEC62D96810
SHA-256:	A10A517D8066052D2320469450D86EF973EFAC0052AE244A032E8135DC018FCE
SHA-512:	0CFAF291DBA8A25AB4DD67392EBD6765E68CB88CC98C2547CA335DE91DA04CE19B3437E63A05446B9511E8CD5E515DFBE55269EE9E0A9B0E815A7C7DBBA3A902
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Preview:	.....N..... ....

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):	3890
Entropy (8bit):	3.360596354965502
Encrypted:	false
SSDEEP:	48:34xvWYPxRTp9atl1J6lUKY4Tp9aopTp9aD1zzWa9uP56lUKY4Tp9aGRRRRRRRRRL:34hWYratjlvLaYaRYwlvLal
MD5:	901350B05C41AE86291103FD7CC232AB
SHA1:	85822F483093E4252A97E7EC0AD29F94D37F6510
SHA-256:	102587CC87B1A74574E859910EC4DFFA85ECFDDDCF1314BFFEA4179FDC8530C9
SHA-512:	DBD771660E99FD4020DEC71F04E3E53B5578279DA68CA8CDDE61C039711C99D4B9CD9EC31357AE34B718AED2CC218944767DCB7D262F0433F5F80A8C5C98C 6
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...82223f49_dd14_4861_8aff_6810424ad601..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....\...file:///C:/Users/user/Desktop/%23Ud83d%23Udda8rocket.com %207335931%23Ufffd90-queue-1675.htm.....h.....`..... .....(..... .....j.....k.....`.....x.....\...f.i.l.e.:././/.C .:./.U.s.e.r.s./.j.o.n.e.s./.D.e.s.k.t.o.p./.%.2.3.U.d.8.3.d.%.2.3.U.d.d.a.8.r.o.c.k.e.t...c.o.m.%.2.0.7.3.3.5.9.3.1.%.2.3.U.f.f.f.d.9.0.-.q.u.e.u.e.-.1.6.7.5...h.t.m..... .....8.....0.....8..... .....h.....`.....

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:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.232568160721826
Encrypted:	false
SSDEEP:	6:moYRCq2Pwkn23iKKdK8aPrqIFUtpTY6ZZmwPTY6zkwOwkn23iKKdK8amLJ:jYRCvYf5KkL3FUtpTYu/PTYC5Jf5KkQJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
MD5:	4344FFB0D21F03966AD48379E21E666B
SHA1:	B977F66FD29156DE72D0EB8DE0A4974B15F4281B
SHA-256:	9159051D1EC520F4B7F421B97E6120DBE8BD7C37C31FCA2FC6D1E172A5F4A86D
SHA-512:	774C2869887175EB85DFD04C9BE5F71BC98180CFBD59D96CA612810A31F66C9EB608BEB16F9A0FA80A7B2062D2D61E1E0647260C93D59957FAFA80DE4F0BAFF 4
Malicious:	false
Preview:	2021/08/03-17:56:14.068 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-1 7:56:14.072 1ad4 Recovering log #3.2021/08/03-17:56:14.072 1ad4 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 Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.232568160721826
Encrypted:	false
SSDEEP:	6:moYRCq2Pwkn23iKKdK8aPrqIFUtpTY6ZZmwPTY6zkwOwkn23iKKdK8amLJ:jYRCvYf5KkL3FUtpTYu/PTYC5Jf5KkQJ
MD5:	4344FFB0D21F03966AD48379E21E666B
SHA1:	B977F66FD29156DE72D0EB8DE0A4974B15F4281B
SHA-256:	9159051D1EC520F4B7F421B97E6120DBE8BD7C37C31FCA2FC6D1E172A5F4A86D
SHA-512:	774C2869887175EB85DFD04C9BE5F71BC98180CFBD59D96CA612810A31F66C9EB608BEB16F9A0FA80A7B2062D2D61E1E0647260C93D59957FAFA80DE4F0BAFF 4
Malicious:	false
Preview:	2021/08/03-17:56:14.068 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-1 7:56:14.072 1ad4 Recovering log #3.2021/08/03-17:56:14.072 1ad4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....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):	5.2274891644591275
Encrypted:	false
SSDEEP:	6:moY9Iq2Pwkn23iKKdK8NIFUtpTY3LG9ZmwPTYxCFzkwOwkn23iKKdK8+eLJ:jY9IvYf5KkpFUtpTYy/PTYxO5Jf5KkqJ
MD5:	9EC47BB848A67BDE057EA28AA4C1E6BA
SHA1:	5B5DBC48C39E0E81FE32FABEF598EF3948E48B0A
SHA-256:	BB20459F81DAAE00FB541AD34D4D237748D8E2D6557A6C3F71B9F7A9A744C82A
SHA-512:	0CF0D826E6D36B1B9D6DBA5C88914E834EE46A1B5F8FC93BD84522527741084D3FCE3BFDC1ACFDBA07186F29FC3C1233D27710740F82343D130D252D780FD94
Malicious:	false
Preview:	2021/08/03-17:56:18.270 1ac4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-1 7:56:18.273 1ac4 Recovering log #3.2021/08/03-17:56:18.275 1ac4 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\Extension State\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.2274891644591275
Encrypted:	false
SSDEEP:	6:moY9Iq2Pwkn23iKKdK8NIFUtpTY3LG9ZmwPTYxCFzkwOwkn23iKKdK8+eLJ:jY9IvYf5KkpFUtpTYy/PTYxO5Jf5KkqJ
MD5:	9EC47BB848A67BDE057EA28AA4C1E6BA
SHA1:	5B5DBC48C39E0E81FE32FABEF598EF3948E48B0A
SHA-256:	BB20459F81DAAE00FB541AD34D4D237748D8E2D6557A6C3F71B9F7A9A744C82A
SHA-512:	0CF0D826E6D36B1B9D6DBA5C88914E834EE46A1B5F8FC93BD84522527741084D3FCE3BFDC1ACFDBA07186F29FC3C1233D27710740F82343D130D252D780FD9
Malicious:	false
Preview:	2021/08/03-17:56:18.270 1ac4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-17:56:18.273 1ac4 Recovering log #3.2021/08/03-17:56:18.275 1ac4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
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\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.296669895629142
Encrypted:	false
SSDEEP:	6:moMH4q2Pwkn23iKKdK25+Xqx8chI+IFUtpTSJZmwPTSxDkwOwkn23iKKdK25+Xqp:jMYvYf5KkTXfchI3FUtpTs/PTS5Jf5KN
MD5:	19BB77E2EF27C69242361D65747C30DF
SHA1:	EAC2244A9DE61ABB61CAD3806151BA08823D6CE6
SHA-256:	504E4C56B1D94C243F2B7C75162F309BD6D58B7FA867081793A6C2454E110D76
SHA-512:	E44254A4E4E2F22A399D42B4199AFF83004F1BF3336D36AAC2BDF0845937016EA9AB0419F210BF75D0918F0540B4921BAAD8928F26E7265A79B93DE40800EC5D
Malicious:	false
Preview:	2021/08/03-17:56:28.288 1d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-17:56:28.316 1d04 Recovering log #3.2021/08/03-17:56:28.435 1d04 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\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.296669895629142
Encrypted:	false
SSDEEP:	6:moMH4q2Pwkn23iKKdK25+Xqx8chI+IFUtpTSJZmwPTSxDkwOwkn23iKKdK25+Xqp:jMYvYf5KkTXfchI3FUtpTs/PTS5Jf5KN
MD5:	19BB77E2EF27C69242361D65747C30DF
SHA1:	EAC2244A9DE61ABB61CAD3806151BA08823D6CE6
SHA-256:	504E4C56B1D94C243F2B7C75162F309BD6D58B7FA867081793A6C2454E110D76
SHA-512:	E44254A4E4E2F22A399D42B4199AFF83004F1BF3336D36AAC2BDF0845937016EA9AB0419F210BF75D0918F0540B4921BAAD8928F26E7265A79B93DE40800EC5D
Malicious:	false
Preview:	2021/08/03-17:56:28.288 1d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-17:56:28.316 1d04 Recovering log #3.2021/08/03-17:56:28.435 1d04 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):	5.248487542625083
Encrypted:	false
SSDEEP:	6:moQH4q2Pwkn23iKKdK25+XuoIFUtpT4BJZmwPTP4DkwOwkn23iKKdK25+XuxWLJ:jBvYf5KkTXYFUtpTo/PTP25Jf5KkTXHJ
MD5:	C5E1F2E37DA28DAEB0741A9E68D6943C
SHA1:	A36BD17C584DC68E45083447640CE34EDE7F5C24
SHA-256:	AB9F5571598E8752919FEE1DE0AE0AE44A860E8B2F916AA2F7B005940EC5AA81
SHA-512:	64F7D3DDDFED7F0F7592B5C2C68535A8F8BBECA8D980F3F93998EBADA146B8CDA7BB1C1E3AA18E1CE844A6C9C8EB32C37AC375792B061B8F0BDEA6B2AAB9C18F
Malicious:	false
Preview:	2021/08/03-17:56:28.143 1d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-17:56:28.147 1d04 Recovering log #3.2021/08/03-17:56:28.152 1d04 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\Feature Engagement Tracker\EventDB\LOG.old (copy)	
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\EventDB\LOG.old (copy)	
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.248487542625083
Encrypted:	false
SSDEEP:	6:moQH4q2Pwkn23iKKdK25+XuoIFUtpT4BJZmwPTP4DkwOwkn23iKKdK25+XuxWLJ:jBvYf5KkTXYFUtpTo/PTP25Jf5KkTXHJ
MD5:	C5E1F2E37DA28DAEB0741A9E68D6943C
SHA1:	A36BD17C584DC68E45083447640CE34EDE7F5C24
SHA-256:	AB9F5571598E8752919FEE1DE0AE0AE44A860E8B2F916AA2F7B005940EC5AA81
SHA-512:	64F7D3DDDFED7F0F7592B5C2C68535A8F8BBECA8D980F3F93998EBADA146B8CDA7BB1C1E3AA18E1CE844A6C9C8EB32C37AC375792B061B8F0BDEA6B2AAB9C18F
Malicious:	false
Preview:	2021/08/03-17:56:28.143 1d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-17:56:28.147 1d04 Recovering log #3.2021/08/03-17:56:28.152 1d04 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):	5.261470781142316
Encrypted:	false
SSDEEP:	6:moYYL4q2Pwkn23iKKdKWT5g1IdqIFUtpTaIJZmwPTa3DkwOwkn23iKKdKWT5g1Iu:jYNvYf5Kkg5gSRFUtpTP/PTw5Jf5Kkgk
MD5:	63B9AEE364E110658A8C2BF3BDDF7D8E
SHA1:	426DEE033F175AF8925F35D6BA0E526E22292DDF
SHA-256:	2D7742622F71B1E6DA271F94E461827D2CECAA93E9FA0C829CEFCD74D77D9928
SHA-512:	F239726F37CBB87458042B760C9FE35A427BBDA4F1E7627A49E9EEB131203DF9A214A46AED6EE699A89267E20F3ADA0916084152FE09C8211AF07041111B63F8
Malicious:	false
Preview:	2021/08/03-17:56:28.058 1d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-17:56:28.072 1d04 Recovering log #3.2021/08/03-17:56:28.073 1d04 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\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.261470781142316
Encrypted:	false
SSDEEP:	6:moYYL4q2Pwkn23iKKdKWT5g1IdqIFUtpTaIJZmwPTa3DkwOwkn23iKKdKWT5g1Iu:jYNvYf5Kkg5gSRFUtpTP/PTw5Jf5Kkgk
MD5:	63B9AEE364E110658A8C2BF3BDDF7D8E
SHA1:	426DEE033F175AF8925F35D6BA0E526E22292DDF
SHA-256:	2D7742622F71B1E6DA271F94E461827D2CECAA93E9FA0C829CEFCD74D77D9928
SHA-512:	F239726F37CBB87458042B760C9FE35A427BBDA4F1E7627A49E9EEB131203DF9A214A46AED6EE699A89267E20F3ADA0916084152FE09C8211AF07041111B63F8
Malicious:	false
Preview:	2021/08/03-17:56:28.058 1d04 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-17:56:28.072 1d04 Recovering log #3.2021/08/03-17:56:28.073 1d04 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):	32768
Entropy (8bit):	0.14142595580187606
Encrypted:	false
SSDEEP:	12:TL+A/yps4Bfcg6WXpgULHNuQPeGI/qnvBfcg6WXpgm:TLxis4pcg9XqqtuGpcg9Xqm
MD5:	589D8C5E51AD64C70AEABE543DF7EFFB
SHA1:	C0DE1BDC2B75E6F1422EDBDF41918A59754B768E
SHA-256:	67B8AD06917CC66C9FE7131949AD7FAC1DBB314B4E04821EF9D496C508D7CCD2
SHA-512:	DDE2A6E1CFBAA83085D3ABCE565E72BB85CFB018E50438CA57A3B339D82AC7B7A9910125650F011D3730318F00000E343DFE20E1EA567EB1595782F20F49882A
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):	819
Entropy (8bit):	5.34539797535953
Encrypted:	false
SSDEEP:	24:+2mV7lf0zSgx38XE/Iz0uVlMfn1Bq+lMSDY78BJgskfa9yBDOxdGpcg9Xq1:+2mVpGxAkoxyfn1B9l7HUwep9a1
MD5:	6DC59A6D334AC1D814FD7D20673A0EA8
SHA1:	D1E2EEB8006253F12CEBC571930EDCF9C6E54780
SHA-256:	21A7D1A16EFD91CC301AF8C5DF2FEAF7267D2EDA1BB1CC8C70E09FFBF9EEA883
SHA-512:	271C1FA95302709226A8BA0895D8D94996946094DB0565B992AF9F962AD1ADEDD44493CCDD5A2FC92FC546050FEE01136BF7B094B5F3BBE8330636B89DA878D
Malicious:	false
Preview:	....."_....1675..7335931..c..com..desktop..file..htm..user..queue..ud83d..udda8rocket..ufffd90..users*.....1675.....7335931.....c.....com.....desktop.....file.....htm.....user.....queue.....ud83d.....udda8rocket.....ufffd90.....users..2.....0.....1.....3.....5.....6.....7.....8.....9.....a.....c.....d.....e.....f.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....w..... ....*\file:///C:/Users/user/Desktop/%23Ud83d%23Udda8rocket.com%207335931%23Ufffd90-queue-1675.htm2.:.....J..... &26>FLQ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.1170439630518394
Encrypted:	false
SSDEEP:	6:UlSBlyslHElWlG+lkl7lfg9bNFlWCj/lo59/l3lm4/fMt76Y4QZeS/rG99pG/5qo:hkPqLBj/O3lm4nMWQASjG9LDBQZ8fOJ
MD5:	C4F46797C58FF02B683D3B6D8433B0B9
SHA1:	51919BC49FBF496CE9E20B1BF1296B006105EF1A
SHA-256:	50F8AA7F6987BBBE8052A7BDCA8AAA46FA310081E2D1CCB57FD96EE0BE405908
SHA-512:	50F6E69CECBC556C20E59092E315E2AD8C6FC721FB3EB194C95767C763E3E7B3A034A3E3619C338A909DE5C984CCAC51F9BA538CFA8D91B80638B51AC78A514
Malicious:	false
Preview:	.....-.wS..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session.O (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3890
Entropy (8bit):	3.360596354965502
Encrypted:	false
SSDEEP:	48:34xvWYPxRTp9atl1J6IUKY4Tp9aopTp9aD1zzWa9uP56IUKY4Tp9aGRRRRRRRRRL:34hWYratjlvLaYaRYwlvLaI
MD5:	901350B05C41AE86291103FD7CC232AB
SHA1:	85822F483093E4252A97E7EC0AD29F94D37F6510
SHA-256:	102587CC87B1A74574E859910EC4DFFA85ECFDDDCF1314BFFEA4179FDC8530C9
SHA-512:	DBD771660E99FD4020DEC71F04E3E53B5578279DA68CA8CDDE61C039711C99D4B9CD9EC31357AE34B718AED2CC218944767DCB7D262F0433F5F80A8C5C98C6
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...82223f49_dd14_4861_8aff_6810424ad601..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....\...file:///C:/Users/user/Desktop/%23Ud83d%23Udda8rocket.com%207335931%23Ufffd90-queue-1675.htm.....h.....`..... .....(..... .....j.....k.....`.....x.....\...f.i.l.e.:././.C.:./.U.s.e.r.s./.j.o.n.e.s./.D.e.s.k.t.o.p./.%.2.3.U.d.8.3.d.%.2.3.U.d.d.a.8.r.o.c.k.e.t...c.o.m.%.2.0.7.3.3.5.9.3.1.%.2.3.U.f.f.f.d.9.0.-.q.u.e.u.e.-.1.6.7.5...h.t.m..... .....8.....0.....8..... .....h.....`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabske (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabske (copy)	
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\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.477054783647822
Encrypted:	false
SSDEEP:	48:gJGzJa73Mr8dbW7LcbQSefgGXNrS0U9RdiN9r:7a73M4dbW7LcbQ5fgGdrS0B
MD5:	6F601B9A404753CD48C3EB3F198B2B23
SHA1:	81FDE1C4829498466740892E5151C2226BC1B380
SHA-256:	70BCCD6A9540EB4291689B7096C6949E3D5BFA943C0339E38B84214978E30529
SHA-512:	C41260AE1FFF41299AD20C3EEEC3C89EAC7BF429791EDD2BA94E13077300B0E22C8F8A6B9A0457424559D0E6EF4BB7CE00FFCA890092D70411399AEE3DFD3C86
Malicious:	false
Preview:	..;....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..437423000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 17:56:30.08][INFO][mr.Init] MR instance ID: a0803ffe-f8e6-4dc2-b35a-f649e3ff1490\n","[2021-08-03 17:56:30.08][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 17:56:30.08][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 17:56:30.08][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 17:56:30.08][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 17:56:30.09][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 17:56:30.09][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.1611660548830995
Encrypted:	false
SSDEEP:	6:moYs+q2Pwkn23iKKdK8a2jMGIFUtpTYdZWZmwPTYKEzVkwOwkn23iKKdK8a2jMmd:jYs+vYf5Kk8EFUtpTYdZW/PTYbV5Jf5i
MD5:	3F6B204BDF3C89CA0D714CB4DD4B5DC7
SHA1:	8F02DAEF2C0EE5070616F745BD97EB99E626576F
SHA-256:	D65F9D52298E586684050F66C4994FF1791526A39D6ADE769D3D2DCCC9E00A73
SHA-512:	DDDB1FD241CEEF2F336D5578B127BB4934DBD0E7C2559AF252E23EE21D4852BC774C546A3290CF8FEC6D4509C0086AB0841E4D57A8DF1FF0E4B9874F326ED49
Malicious:	false
Preview:	2021/08/03-17:56:13.705 1aec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-17:56:13.707 1aec Recovering log #3.2021/08/03-17:56:13.708 1aec 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\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.1611660548830995
Encrypted:	false
SSDEEP:	6:moYs+q2Pwkn23iKKdK8a2jMGIFUtpTYdZWZmwPTYKEzVkwOwkn23iKKdK8a2jMmd:jYs+vYf5Kk8EFUtpTYdZW/PTYbV5Jf5i
MD5:	3F6B204BDF3C89CA0D714CB4DD4B5DC7
SHA1:	8F02DAEF2C0EE5070616F745BD97EB99E626576F
SHA-256:	D65F9D52298E586684050F66C4994FF1791526A39D6ADE769D3D2DCCC9E00A73
SHA-512:	DDDB1FD241CEEF2F336D5578B127BB4934DBD0E7C2559AF252E23EE21D4852BC774C546A3290CF8FEC6D4509C0086AB0841E4D57A8DF1FF0E4B9874F326ED49
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
Preview:	2021/08/03-17:56:13.705 1aec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-17:56:13.707 1aec Recovering log #3.2021/08/03-17:56:13.708 1aec 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 Persistent State (copy)	
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):	2124
Entropy (8bit):	4.83234700996353
Encrypted:	false
SSDEEP:	48:Y2nzM3qyvKDHGXtwTAsCc66NuzsC8zsCRLsM6qCGYhbw:JnzMa+KDHGXOTj66N2E3xC7hM
MD5:	09427A015BED89233F962DF7EC8B375D
SHA1:	39D7A77586B31B701DE937859A5D176EB0ACF7C0
SHA-256:	13D7BE792B4A991A41CFB3A687A6025BCE473420CBF6EFFF790139CB2D0DD443
SHA-512:	86B783E8EDB23BD9C7AE51A6D0C6EAB59566E488EE4524304B622013CB42A587CCD68F8C234F26CCDC09EAEC79E5F0E52BF853DBA59D72E576980BD8240BF920
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://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.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://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://maxcdn.bootstrapcdn.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275071778898614","port":443,"protocol_str":"quic"}],"isolatio

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State. (copy)	
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):	2770
Entropy (8bit):	4.860244630115105
Encrypted:	false
SSDEEP:	48:Y2zMKDHGXtwT56MsC8zsCRLsM6q7sluqNHvsFnNs2yKsiZ3zsSMHtYhbw:JzMKDHGXOT56WE3xstNH4nBXZPGKhM
MD5:	FD5303DC2A19C1434A4783245CD45855
SHA1:	D53A5AD85208B141FAF32317D8BD9B700C11324D
SHA-256:	7505C842B176615A00B7B9099DDFD0886DC176139BCA3EE1212FD70F8B37E7BE
SHA-512:	F5194970654E81180301C100AF79CF3210C8683EC82B4DDFD5D4DAA957C9830C41CD6B52B98B21F74F28F18587E8D021D2F5C2D99AC6758E40CA84E32991ACC
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.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://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://maxcdn.bootstrapcdn.com","supports_spdy":true},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275071778928961","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ajax.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275071778949519","port"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateE (copy)	
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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.203342192474329
Encrypted:	false
SSDEEP:	6:moYhyq2Pwkn23iKKdKgXz4rRIFUtpTYcr1ZmwPTYXYRkwOwkn23iKKdKgXz4q8LJ:jYkvYf5KkgXiuFUtpTYcr1/PTYw5Jf5j
MD5:	8B4875A36C5022BC122641B1F5F610D6
SHA1:	D06CAD14CF01E13346B365AB4CB389AFA8C5D1B9
SHA-256:	F70D5BBCAEEC0E4481C0678F518D5962B59981C9FCA475E8988CF029339596F2
SHA-512:	ED4792DCBFA5B8DBBE5567FAAEFDE80D78816565D3C05292B02AC45D6596DDD1DDF8B7E392022EA783EE9B019DF0C67B62B4C592C9FEB0F166402018F2C12 B4
Malicious:	false
Preview:	2021/08/03-17:56:14.076 1ae0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-17:56:14.079 1ae0 Recovering log #3.2021/08/03-17:56:14.080 1ae0 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.203342192474329
Encrypted:	false
SSDEEP:	6:moYhyq2Pwkn23iKKdKgXz4rRIFUtpTYcr1ZmwPTYXYRkwOwkn23iKKdKgXz4q8LJ:jYkvYf5KkgXiuFUtpTYcr1/PTYw5Jf5j
MD5:	8B4875A36C5022BC122641B1F5F610D6
SHA1:	D06CAD14CF01E13346B365AB4CB389AFA8C5D1B9
SHA-256:	F70D5BBCAEEC0E4481C0678F518D5962B59981C9FCA475E8988CF029339596F2
SHA-512:	ED4792DCBFA5B8DBBE5567FAAEFDE80D78816565D3C05292B02AC45D6596DDD1DDF8B7E392022EA783EE9B019DF0C67B62B4C592C9FEB0F166402018F2C12 B4
Malicious:	false
Preview:	2021/08/03-17:56:14.076 1ae0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-17:56:14.079 1ae0 Recovering log #3.2021/08/03-17:56:14.080 1ae0 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\Preferences (copy)	
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):	5513
Entropy (8bit):	5.164668913030689
Encrypted:	false
SSDEEP:	96:nYLbT9WTMEBdgNIKIW5k0JCKL8tbOTlVuHn:nYL39/NIMh4Kk
MD5:	A86BE63275805B43A4118860DBFAF175
SHA1:	39148DA6EDA092034D9AD613FB725C08120A87FD
SHA-256:	3A0C2BB7DB686016A81BEE5950C998C2539938AEE7C9E74999D4BC7F15484CF2
SHA-512:	1398ACD9DD5853FA38F5BDE902925F969BBBD291C5C0B6E46A28AA336399E7BB688F173DEF948AE953F3E727C549946978283DCF62364FE50BAA9FCF19A130D B
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272479774032231","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":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences. (copy)	
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):	5513
Entropy (8bit):	5.164698683842019
Encrypted:	false
SSDEEP:	96:nYLST9WTMEBdgNIKIW5k0JCKL8tbOTlVuHn:nYLs9/NIMh4Kk
MD5:	7C61C3B6E1D2589C937214DCC2FEF99D
SHA1:	6D5674E2A1D72DFEE290CE484E3441BA6D7EFECB
SHA-256:	1824DE9CB2032A87DDBFF8F4B89AC91D4CF458B56C96E9858F5221F6027141F9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences. (copy)	
SHA-512:	7E424BAEF58732F7F0E05FA690B1FED619A36DC78DB6FF00330C68B958A4A9F386151683CBB26C6BA2FBDCC927D5CEE5BE8A0D9C3E79D3D95A2730B8552EF8 B4
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272479774032231","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":{"default_browser_infobar_last_declined":"13245924607060180","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_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	57344
Entropy (8bit):	1.3233742872101493
Encrypted:	false
SSDEEP:	192:wIElwQF8mpcS4yNIElwQF8mpcSi5ibqU5xbT8o:RkOCr
MD5:	F7BF2407A1D97FE3465A6B5F4E99E673
SHA1:	0660A28F909C1F34237783E437D2340BFC3422C4
SHA-256:	B7FF71878F58DFCB05CB8B2920427EF5D47D16EA992AD21D50BEC609A2EB215B
SHA-512:	125B5929164216A5A588823C4FB52135C8D5D70180BE35253C68FF73230F781C59D7973A7E035E9FED7B90EC3291C2E25103ADA09D6AD02C15AD2F541C6659C
Malicious:	false
Preview:	SQLite format 3......@ ....C..........g...^.........j..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	58504
Entropy (8bit):	0.852303582642528
Encrypted:	false
SSDEEP:	192:oxgCawsUhIElwQF8mpcS09yxIElwQF8mpcSC:qcAK
MD5:	CB3C77D468B835EB6C03542B605BA092
SHA1:	3C58F2E286AAF38956A4D45EB1FC007B446DB425
SHA-256:	001F334A98B5F8188F563709D370A0DC9FDE37A2B2F737D438AF128B08EBE535
SHA-512:	2347FEB0182B9714DE410F2F327F645AA1F813B4E1E28295B630259911892F4B4856A655741A4303A362094749737BC2155F48282E2210B1D358A0092CCE94B7
Malicious:	false
Preview:	............{...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
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):	22602
Entropy (8bit):	5.5357630135379035
Encrypted:	false
SSDEEP:	384:Vm5toLlrbXA1kXqKf/pUZNCgVLH2HfD9rU+HGPnZBt1px4D:hLlfA1kXqKf/pUZNCgVLH2HfxrUuGPns
MD5:	3C6EBEF215B0D85A8CADDB11BFA1715D
SHA1:	A3E0ED0A69270E2E0CE278BE03D7E7403B9AEE57
SHA-256:	C862D7CA3C94D11A7566E095FF77E4FA8C09C94B19D946F2BE5E2F10F9D72973
SHA-512:	8ABD3EFAEE79357C3BD65F2165A818F818D5EAAB6E48EEE723FB5AE162EF3697BFD131A62E0103DBC9BFA67B5241988A72C84F1231EE29AB25ACD7AE4FE888 8E
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":"13272479773643030","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\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.211548150103978
Encrypted:	false
SSDEEP:	6:moYZADM+q2Pwkn23iKKdKrQMxIFUtpTYOWAgZmwPTY/sADMVkwOwkn23iKKdKrQq:jYZADM+vYf5KkCFUtpTYOWAg/PTY0ADG
MD5:	40E481AEDC3DFE229ADF7291A7D66F97
SHA1:	BB10F11EE83B81BE6D4D1AB2C9E9FFC3C9FC20A4
SHA-256:	6F7E9E97974419508F71C43A7FBCF51B132BA0031CF03C87B74614036CAB8DFE
SHA-512:	488FCBEC378E292E14B26E3294C57CAD5D720D5A00534D3F7BD5A683303B4998B3618E11CCDAE4F57309A85C5D9EDB669CC610E0BB8C39B02981FFA99D33C7C
Malicious:	false
Preview:	2021/08/03-17:56:13.972 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-17:56:13.974 1a8c Recovering log #3.2021/08/03-17:56:13.975 1a8c 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\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.211548150103978
Encrypted:	false
SSDEEP:	6:moYZADM+q2Pwkn23iKKdKrQMxIFUtpTYOWAgZmwPTY/sADMVkwOwkn23iKKdKrQq:jYZADM+vYf5KkCFUtpTYOWAg/PTY0ADG
MD5:	40E481AEDC3DFE229ADF7291A7D66F97
SHA1:	BB10F11EE83B81BE6D4D1AB2C9E9FFC3C9FC20A4
SHA-256:	6F7E9E97974419508F71C43A7FBCF51B132BA0031CF03C87B74614036CAB8DFE
SHA-512:	488FCBEC378E292E14B26E3294C57CAD5D720D5A00534D3F7BD5A683303B4998B3618E11CCDAE4F57309A85C5D9EDB669CC610E0BB8C39B02981FFA99D33C7C
Malicious:	false
Preview:	2021/08/03-17:56:13.972 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-17:56:13.974 1a8c Recovering log #3.2021/08/03-17:56:13.975 1a8c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.189254290209692
Encrypted:	false
SSDEEP:	6:moY34q2Pwkn23iKKdK7Uh2ghZIFUtpTY33JZmwPTYQDkwOwkn23iKKdK7Uh2gnLJ:jYIvYf5KkIhHh2FUtpTYp/PTYe5Jf5KF
MD5:	330BDF6AB8394357E22CB5F723E90DC9
SHA1:	297C555BF2B7D7D5C99D0450DCC250B6A0B134F7
SHA-256:	8AADCAF07A8CADA22DA14AEA64E60BC1BDB045D4947DF3738CDC1C9FE2531640
SHA-512:	C8738A3EFC8CEB15EF1687B986A51196E65AC747562528AD3A4B7E03415D56233C81C41D48D3991998B58207FC67A87DA8FD6075E7E83D7CF509B75D0BDE677
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Preview:	2021/08/03-17:56:13.603 1a84 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-17:56:13.614 1a84 Recovering log #3.2021/08/03-17:56:13.628 1a84 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\Site Characteristics Database\LOG.oldhk (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.189254290209692
Encrypted:	false
SSDEEP:	6:moY34q2Pwkn23iKKdK7Uh2ghZIFUtpTY33JZmwPTYQDkwOwkn23iKKdK7Uh2gnLJ:jYIvYf5KkIhHh2FUtpTYp/PTYe5Jf5KF
MD5:	330BDF6AB8394357E22CB5F723E90DC9
SHA1:	297C555BF2B7D7D5C99D0450DCC250B6A0B134F7
SHA-256:	8AADCAF07A8CADA22DA14AEA64E60BC1BDB045D4947DF3738CDC1C9FE2531640
SHA-512:	C8738A3EFC8CEB15EF1687B986A51196E65AC747562528AD3A4B7E03415D56233C81C41D48D3991998B58207FC67A87DA8FD6075E7E83D7CF509B75D0BDE677
Malicious:	false
Preview:	2021/08/03-17:56:13.603 1a84 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/08/03-17:56:13.614 1a84 Recovering log #3.2021/08/03-17:56:13.628 1a84 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\75e70f2c-af0b-45a7-89e5-cd129e345a7d.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):	5.254239694520501
Encrypted:	false
SSDEEP:	6:moY39q2Pwkn23iKKdKusNpV/2jMGIFUtpTYiZZmwPTYtFkwOwkn23iKKdKusNpV0:jYtvYf5KkFFUtpTY2/PTYz5Jf5KkOJ
MD5:	F005472C1B9C6CF117E33FB1C06E20F8
SHA1:	2079CBD9624A1B9282977CB1DCD76E4F898BA70F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG

SHA-256:	17E9F8624AC76FA7B9F55215531871E12C225CFA0F27754DF9428BD57975801F
SHA-512:	A4E69312EE308028DB09FC42CD601DF83A23473BB91651F5C8D2928C48B74ABF609AF13F35CB991689EBDE354229FABCDB45EDFD6503EBBC22907F59A82AAA7
Malicious:	false
Preview:	2021/08/03-17:56:14.009 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-17:56:14.010 1ad4 Recovering log #3.2021/08/03-17:56:14.011 1ad4 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\Local Storage\leveldb\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.254239694520501
Encrypted:	false
SSDEEP:	6:moY39q2Pwkn23iKKdKusNpV/2jMGIFUtpTYiZZmwPTYtFkwOwkn23iKKdKusNpV0:jYtvYf5KkFFUtpTY2/PTYz5Jf5KkOJ
MD5:	F005472C1B9C6CF117E33FB1C06E20F8
SHA1:	2079CBD9624A1B9282977CB1DCD76E4F898BA70F
SHA-256:	17E9F8624AC76FA7B9F55215531871E12C225CFA0F27754DF9428BD57975801F
SHA-512:	A4E69312EE308028DB09FC42CD601DF83A23473BB91651F5C8D2928C48B74ABF609AF13F35CB991689EBDE354229FABCDB45EDFD6503EBBC22907F59A82AAA7
Malicious:	false
Preview:	2021/08/03-17:56:14.009 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-17:56:14.010 1ad4 Recovering log #3.2021/08/03-17:56:14.011 1ad4 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\Network Persistent State (copy)

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\Platform Notifications\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.291816017837911
Encrypted:	false
SSDEEP:	12:jYBmvYf5KkmiuFUtpTYj/PTYMF5Jf5Kkm2J:j0kYf5KkSghgjXJf5Kkr
MD5:	FFB5D41FCF361B96D14B6277E2C34DCD
SHA1:	A34097092D11983DE66294A61490E3AB13DB9662
SHA-256:	1C6EE1563B677EB49DB2932392DEA9B41770BD11440CDC250B5FD930E418D757
SHA-512:	5635C3D7E24519530B95E7432AAD5498E9540F0DA5E5689F4CB8E8555C08304CF17223F1F98681E4E6B00BFB77FA51D77360F2FC0B67C17F9A38C1ED401D3C5E
Malicious:	false
Preview:	2021/08/03-17:56:14.069 1ae4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-17:56:14.074 1ae4 Recovering log #3.2021/08/03-17:56:14.075 1ae4 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\Platform Notifications\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.291816017837911
Encrypted:	false
SSDEEP:	12:jYBmvYf5KkmiuFUtpTYj/PTYMF5Jf5Kkm2J:j0kYf5KkSghgjXJf5Kkr
MD5:	FFB5D41FCF361B96D14B6277E2C34DCD
SHA1:	A34097092D11983DE66294A61490E3AB13DB9662
SHA-256:	1C6EE1563B677EB49DB2932392DEA9B41770BD11440CDC250B5FD930E418D757
SHA-512:	5635C3D7E24519530B95E7432AAD5498E9540F0DA5E5689F4CB8E8555C08304CF17223F1F98681E4E6B00BFB77FA51D77360F2FC0B67C17F9A38C1ED401D3C5E
Malicious:	false
Preview:	2021/08/03-17:56:14.069 1ae4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-17:56:14.074 1ae4 Recovering log #3.2021/08/03-17:56:14.075 1ae4 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):	5.268427664334422
Encrypted:	false
SSDEEP:	12:jxF4vYf5KkMFUtpTeoRX/PT4jz5Jf5KkTJ:j+Yf5KkUghLz4jlJf5Kkl
MD5:	C557815581361038C17C8BBC9F6DA4FE
SHA1:	6E4B8A6675CCFAA5B6318708D892E1F6850E04C8
SHA-256:	0156426DC474167F5B757403FA1453C46C0801E38868A671C584F9517DE421AE
SHA-512:	FD8C47FB1AE5DCA3EFA4321BB5C6E3DED41D784933C4415F735CCF1DA7FF698738EC927A777BBE7E016E6F7ABA9A919FC973835C4A06E9357A7C5DE5CD876B9
Malicious:	false
Preview:	2021/08/03-17:56:32.502 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-17:56:32.504 1ad4 Recovering log #3.2021/08/03-17:56:32.505 1ad4 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\Session Storage\LOG.olda. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.268427664334422
Encrypted:	false
SSDEEP:	12:jxF4vYf5KkMFUtpTeoRX/PT4jz5Jf5KkTJ:j+Yf5KkUghLz4jlJf5Kkl
MD5:	C557815581361038C17C8BBC9F6DA4FE
SHA1:	6E4B8A6675CCFAA5B6318708D892E1F6850E04C8
SHA-256:	0156426DC474167F5B757403FA1453C46C0801E38868A671C584F9517DE421AE
SHA-512:	FD8C47FB1AE5DCA3EFA4321BB5C6E3DED41D784933C4415F735CCF1DA7FF698738EC927A777BBE7E016E6F7ABA9A919FC973835C4A06E9357A7C5DE5CD876B9
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.olda. (copy)	
Preview:	2021/08/03-17:56:32.502 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-17:56:32.504 1ad4 Recovering log #3.2021/08/03-17:56:32.505 1ad4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\290e82b3-dd62-41eb-8203-6a8bcdd51adf.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\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.2345645494404955
Encrypted:	false
SSDEEP:	12:j+MvYf5KkkGHArBFUtpTS/PTfD5Jf5KkkGHAryJ:j7Yf5KkkGgPghS9Jf5KkkGga
MD5:	9D470774EA5195ECEB611EDA403442A0
SHA1:	C8D3C43A9055FB67F1336BE39D386EB5B55964F6
SHA-256:	6F32120AA1115930BCED4427C9E5DB6A583CA54E1FE47F5E5BE2C3F9B39699D2
SHA-512:	D0DD6C2ABDB9C4AD9CD5AFC5A2B99D800C6B8D7E1F5FEB4823B1CF774BD6BE808D21DF5F0AD94BE96F2B3D2A7C375E0E9604E504334586CB06297813697D264
Malicious:	false
Preview:	2021/08/03-17:56:28.344 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-17:56:28.353 1ad4 Recovering log #3.2021/08/03-17:56:28.356 1ad4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.2345645494404955
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
SSDEEP:	12:j+MvYf5KkkGHArBFUtpTS/PTfD5Jf5KkkGHAryJ:j7Yf5KkkGgPghS9Jf5KkkGga
MD5:	9D470774EA5195ECEB611EDA403442A0
SHA1:	C8D3C43A9055FB67F1336BE39D386EB5B55964F6
SHA-256:	6F32120AA1115930BCED4427C9E5DB6A583CA54E1FE47F5E5BE2C3F9B39699D2
SHA-512:	D0DD6C2ABDB9C4AD9CD5AFC5A2B99D800C6B8D7E1F5FEB4823B1CF774BD6BE808D21DF5F0AD94BE96F2B3D2A7C375E0E9604E504334586CB06297813697D2 64
Malicious:	false
Preview:	2021/08/03-17:56:28.344 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-17:56:28.353 1ad4 Recovering log #3.2021/08/03-17:56:28.356 1ad4 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\Network Persistent State (copy)	
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:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2 F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isol ation":[],"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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.265303576198239
Encrypted:	false
SSDEEP:	12:jmvYf5KkkGHArqiuFUtpTkZ/PTe5Jf5KkkGHArq2J:jkYf5KkkGgCghkFIJf5KkkGg7
MD5:	5B36A0130F19546186DF86C9AA24061F
SHA1:	F57EF2120FEE81C20C386FC713874F5906F2E709
SHA-256:	6AB6E48ACF048D980B89FBC82E8FCE668490E308BCD518231EF40217C6D988C1
SHA-512:	91766B7BD34B8F7C44D5466D27A92B7FAB8140F01F219B0203CC54D9B06D363018D3C1C787E193D4BB7947835FCB3E3B176B4A8695438B3026D43231554274C5
Malicious:	false
Preview:	2021/08/03-17:56:28.354 1a84 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/03-17:56:28.359 1a84 Recovering log #3.2021/08/03-17:56:28.362 1a84 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\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.265303576198239
Encrypted:	false
SSDEEP:	12:jmvYf5KkkGHArqiuFUtpTkZ/PTe5Jf5KkkGHArq2J:jkYf5KkkGgCghkFIJf5KkkGg7
MD5:	5B36A0130F19546186DF86C9AA24061F
SHA1:	F57EF2120FEE81C20C386FC713874F5906F2E709
SHA-256:	6AB6E48ACF048D980B89FBC82E8FCE668490E308BCD518231EF40217C6D988C1
SHA-512:	91766B7BD34B8F7C44D5466D27A92B7FAB8140F01F219B0203CC54D9B06D363018D3C1C787E193D4BB7947835FCB3E3B176B4A8695438B3026D43231554274C5
Malicious:	false
Preview:	2021/08/03-17:56:28.354 1a84 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/03-17:56:28.359 1a84 Recovering log #3.2021/08/03-17:56:28.362 1a84 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):	5.229396112966951
Encrypted:	false
SSDEEP:	12:jOvYf5KkkGHArAFUtpT9uEZ/PT9uEz5Jf5KkkGHArfJ:jMYf5KkkGgkghUEFUElJf5KkkGgV
MD5:	152592A17185E799BBC91A10B39BB1B6
SHA1:	B25AE0D0F3A17F793FB64F893829397507F522EE
SHA-256:	BB27F5D8B281CEEC48123D6312F2690D331D1F2ECF8821DD7E595E75A789C89B
SHA-512:	0A16FCA26D634015981363438A33EB4A3362E84AC22E3443325F2A746CFF5134FB58009BDC466BE8CF344BABDF65B4E9D90A1E562E7C8FA598871FF9D698FA98
Malicious:	false
Preview:	2021/08/03-17:56:43.683 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/03-17:56:43.685 1ad4 Recovering log #3.2021/08/03-17:56:43.685 1ad4 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\Session Storage\LOG.old.c (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.229396112966951
Encrypted:	false
SSDEEP:	12:jOvYf5KkkGHArAFUtpT9uEZ/PT9uEz5Jf5KkkGHArfJ:jMYf5KkkGgkghUEFUElJf5KkkGgV
MD5:	152592A17185E799BBC91A10B39BB1B6
SHA1:	B25AE0D0F3A17F793FB64F893829397507F522EE
SHA-256:	BB27F5D8B281CEEC48123D6312F2690D331D1F2ECF8821DD7E595E75A789C89B
SHA-512:	0A16FCA26D634015981363438A33EB4A3362E84AC22E3443325F2A746CFF5134FB58009BDC466BE8CF344BABDF65B4E9D90A1E562E7C8FA598871FF9D698FA98
Malicious:	false
Preview:	2021/08/03-17:56:43.683 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/03-17:56:43.685 1ad4 Recovering log #3.2021/08/03-17:56:43.685 1ad4 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
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):	5.249984371913051
Encrypted:	false
SSDEEP:	6:moYoUZN+q2Pwkn23iKKdKpIFUtpTYcZmwPTYXVkwOwkn23iKKdKa/WLJ:jYJZIvYf5KkmFUtpTYc/PTYl5Jf5KkaQ
MD5:	AEC2C6491854380A1E872C01215D9EE4
SHA1:	832BCC48B5FE1FB9ED6616520A9A50598056DE82
SHA-256:	F9B50B51559DF37F3DFBCD136020B02946C8821D07523C412EDE9748A0CF316B
SHA-512:	46FBEF2CF284BC4545A31AEA7E2C6F51B8C9643611577B3D7EEF4D1CC07408876B88E52DB4D4284951CD28D6776AC483FB5F4974B64F7199BAFB63FD815E35AB
Malicious:	false
Preview:	2021/08/03-17:56:13.668 1a58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-17:56:13.670 1a58 Recovering log #3.2021/08/03-17:56:13.679 1a58 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 Data\LevelDB\LOG.oldg (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.249984371913051
Encrypted:	false
SSDEEP:	6:moYoUZN+q2Pwkn23iKKdKpIFUtpTYcZmwPTYXVkwOwkn23iKKdKa/WLJ:jYJZIvYf5KkmFUtpTYc/PTYl5Jf5KkaQ
MD5:	AEC2C6491854380A1E872C01215D9EE4
SHA1:	832BCC48B5FE1FB9ED6616520A9A50598056DE82
SHA-256:	F9B50B51559DF37F3DFBCD136020B02946C8821D07523C412EDE9748A0CF316B
SHA-512:	46FBEF2CF284BC4545A31AEA7E2C6F51B8C9643611577B3D7EEF4D1CC07408876B88E52DB4D4284951CD28D6776AC483FB5F4974B64F7199BAFB63FD815E35AB
Malicious:	false
Preview:	2021/08/03-17:56:13.668 1a58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-17:56:13.670 1a58 Recovering log #3.2021/08/03-17:56:13.679 1a58 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
Entropy (8bit):	5.302941111782431
Encrypted:	false
SSDEEP:	12:jCvYf5KkkOrsFUtpTfJ/PTfD5Jf5KkkOrzJ:jIYf5Kk+ghfVfVJf5Kkn
MD5:	A54786110528D50697076C3D86129255
SHA1:	55627893BEE65BAAC5E041EC327C83124AEDB872
SHA-256:	9417EE4D4096A66236617DFC1EB5F0F34B7CDAA818B174A4DD5EC60E51534703
SHA-512:	75FA6D88904B57B8993C69A2FC362F3AE6EFD9A776AFBA791B71A4880829630A082C007A6568D8040D7FCBB4AB414EDA6C3EEAC3F0F49E9D440ED751ABCCD05B
Malicious:	false
Preview:	2021/08/03-17:56:30.061 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-17:56:30.063 1ad4 Recovering log #3.2021/08/03-17:56:30.063 1ad4 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\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.302941111782431
Encrypted:	false
SSDEEP:	12:jCvYf5KkkOrsFUtpTfJ/PTfD5Jf5KkkOrzJ:jIYf5Kk+ghfVfVJf5Kkn

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old (copy)	
MD5:	A54786110528D50697076C3D86129255
SHA1:	55627893BEE65BAAC5E041EC327C83124AEDB872
SHA-256:	9417EE4D4096A66236617DFC1EB5F0F34B7CDAA818B174A4DD5EC60E51534703
SHA-512:	75FA6D88904B57B8993C69A2FC362F3AE6EFD9A776AFBA791B71A4880829630A082C007A6568D8040D7FCBB4AB414EDA6C3EEAC3F0F49E9D440ED751ABCCD05B
Malicious:	false
Preview:	2021/08/03-17:56:30.061 1ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-17:56:30.063 1ad4 Recovering log #3.2021/08/03-17:56:30.063 1ad4 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\TransportSecurity (copy)	
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):	1540
Entropy (8bit):	5.586894825702751
Encrypted:	false
SSDEEP:	48:YgYVwUvUF6UUhd0KUKLYqPeUekUezwUwrsYUaEPUeP:n3UvUMUUIKUUHPeU3UJU7YUpPUg
MD5:	D5420ED23C61CB6A9439C145D78FF8D7
SHA1:	53034DA920D08C69C93EAF0E2A6DD636995D6E23
SHA-256:	81101866E0DD306A27A585EA4B1252282BC180DCCD90C15BF11100AF872CA758
SHA-512:	04F352094DA8B6BEB021560DEA555A7214FFA91AB89E45386DA7D6DFC0A7382A92EE34B868F0112EF568D2AEAF3639903321721603BA4BCE919A4D964B079872
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1643786178.967912,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628006178.967918},{"expiry":1659542179.00608,"host":"F8CDsiT0h6lTN4Nqwoyb2wNyqqjWSTsRj/gzlYU3NfY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628006179.006088},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659542178.96927,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628006178.969275},{"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_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity64 (copy)	
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):	1876
Entropy (8bit):	5.582800683818056
Encrypted:	false
SSDEEP:	48:YgYVwUvUK2wUK86UUhd0KUKLYqPeUekUef+UKoFwUwrsYUaEPUeP:n3UvUiUOUUIKUUHPeU3UU+U9GU7YUpPt
MD5:	2915E51F258E33B405E2ABCCA5F7DC5E
SHA1:	CE6E8C0ADD766D8A3FB3EF12BD33A62F1A0BF322
SHA-256:	9281E4C162C8D597FCE0F6F32269735BADAC3B3E6BAA739DE0FC6203F6FC9E21
SHA-512:	30CEB6607A3E36E36111DC16E8E2CA0CCBA6D5575DACE3E0D5EE591E9AB656A37693C66231727C826E9D321A4E029A2EF92C49152839B104F51EAA73DF80CEC
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1643786178.967912,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628006178.967918},{"expiry":1659542179.00608,"host":"F8CDsiT0h6lTN4Nqwoyb2wNyqqjWSTsRj/gzlYU3NfY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628006179.006088},{"expiry":1643558241.396162,"host":"MmvkdkL5VfySrkgf46RcMa812w+Y8Zl7wGpCsfjsbSc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628006241.396168},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659542178.96927,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628006178.969275},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:msEn:U
MD5:	ABEBD64FF18BCFFB9D16433EEE413356
SHA1:	33C32FA4DF3CBA64484F386BBAA5B94241C2AAB6
SHA-256:	24B2D941312552C0301375DB7A8C89D280A0EDE676F2EBD55093B541635EC2D9
SHA-512:	DB58CDA6D1272FCB69B1D131444BF4B30BE2A35CFE0046D75AECB3167739DADA61C03CC64F39D4CF702814849EB208029437C4D5D72E3F6769D1B133EE6226C
Malicious:	false

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

Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a94d927b-92df-4aeb-b675-95ebb19f720d.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):	5487
Entropy (8bit):	5.161932349334823
Encrypted:	false
SSDEEP:	96:nYLvT9WTMEBdgNIKIW5k0JCKL8bbOTlVuHn:nYLb9/NIMh4Km
MD5:	565435D73E96C4BD114CFA75738D31E8
SHA1:	A8FAE24B8E447F1E371B8368500F7684F5D39D20
SHA-256:	6DD171AC18F7629FCB4064EF6D2ACDA792A2CD306D66C2201598F1B4469346E3
SHA-512:	58DBB4E138156FD08CBC53FADE211DA66A8538E9704079871DF009B1ECDD98874970F9FF352A49581CCC3C21A67DE5F20373D58DC797A6B1AFE3363DCB8523 2
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272479774032231","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":{"default_browser_infobar_last_declined":"13245924607060180","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_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ac60b9b1-0825-4d8a-bb4f-35633ea92514.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):	2770
Entropy (8bit):	4.860244630115105
Encrypted:	false
SSDEEP:	48:Y2zMKDHGXtwT56MsC8zsCRLsM6q7sluqNHvsFnNs2yKsiZ3zsSMHtYhbw:JzMKDHGXOT56WE3xstNH4nBXZPGKhM
MD5:	FD5303DC2A19C1434A4783245CD45855
SHA1:	D53A5AD85208B141FAF32317D8BD9B700C11324D
SHA-256:	7505C842B176615A00B7B9099DDFD0886DC176139BCA3EE1212FD70F8B37E7BE
SHA-512:	F5194970654E81180301C100AF79CF3210C8683EC82B4DDFD5D4DAA957C9830C41CD6B52B98B21F74F28F18587E8D021D2F5C2D99AC6758E40CA84E32991ACC
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.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://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://maxcdn.bootstrapcdn.com","supports_spdy":true},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275071778928961","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ajax.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275071778949519","port"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b781d688-cb0f-4683-b14d-a3cd8144df2f.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):	22601
Entropy (8bit):	5.536121862603987
Encrypted:	false
SSDEEP:	384:Vm5toLlrbXA1kXqKf/pUZNCgVLH2HfD9rU+HGAnZBtppx4T:hLlfA1kXqKf/pUZNCgVLH2HfxrUuGAnU
MD5:	44D2984A03E2BE17057B80E3CB15647B
SHA1:	EA03762508981CE41949126BBB1A886E5F1018C3
SHA-256:	3ECA89DA987F6EE6FBF9FD073BF8174A569E6A38D1642F29C05C86B7A804E9EF
SHA-512:	A8E73033922C1A31D2E3938181E5C3C0F4D6269F3871E6356921B19F2326DD4790FBD103FC03125F855F5F80E279F64ECA52F2644DAB1B1D5B1CE8CFE4FEEA0(
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":"13272479773643030","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	4.853857210169542
TrID:	
File name:	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm
File size:	29372
MD5:	0861c3ccccf34eba88e5a9f8a0e16f34
SHA1:	5a0bb102052fe2b4eebb6be76ea6251cf21325b4
SHA256:	09ba757400f8a2823e54036d837ac4f7a23718f98dda278ae86f79446b4d9fb0
SHA512:	752c3726b1b9d2e8c8abc4a929d1ccce011ecd7cc3e2cc054a8301d18c23bd627b36dbe8d8343be58955fd62e8df4dfc6a4d416946ef86d0127136c5daeca248
SSDEEP:	768:sh7/mNBlLe+FQ+WdBK9zr8Tc9xqoTHbFnXHbTRgc9p1PvenE1wrw6bn:G/qBlLe+FQ+WdBK9zr8Tc9xqoTHbFnX+
File Content Preview:	..<HTML>..<HEAD>..<SCRIPT>.. /..code = "%3Cmeta%20charset%20%3D%20%22UTF-8%22%20/%3E%0A%3Chtml%20lang%3D%22en%22%3E%3Chead%3E%3Cstyle%3E%0A%23pewddiued%20%7B%0A%20%20background-color%3A%20%23235296%3B%0A%20%20color%3A%20%23072285%3B%0A%20%20font-family

File Icon

Icon Hash:	e8d6a08c8882c461

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 17:56:19.035207987 CEST	192.168.2.4	8.8.8.8	0xdf70	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.037336111 CEST	192.168.2.4	8.8.8.8	0x5b0a	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.042740107 CEST	192.168.2.4	8.8.8.8	0xe1de	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.044625998 CEST	192.168.2.4	8.8.8.8	0xf339	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.050947905 CEST	192.168.2.4	8.8.8.8	0xafdf	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.085906029 CEST	192.168.2.4	8.8.8.8	0x1537	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.662858009 CEST	192.168.2.4	8.8.8.8	0x737f	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.726900101 CEST	192.168.2.4	8.8.8.8	0x236e	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:21.522243977 CEST	192.168.2.4	8.8.8.8	0x5cb9	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 17:56:21.939729929 CEST	192.168.2.4	8.8.8.8	0x3eed	Standard query (0)	api.statvoo.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:21.942786932 CEST	192.168.2.4	8.8.8.8	0xd2bf	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.120800018 CEST	192.168.2.4	8.8.8.8	0x9010	Standard query (0)	api-images .statvoo.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.234452963 CEST	192.168.2.4	8.8.8.8	0x82aa	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:27.435822010 CEST	192.168.2.4	8.8.8.8	0x675	Standard query (0)	clients2.g oogle.com	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:28.227643013 CEST	192.168.2.4	8.8.8.8	0x5fd2	Standard query (0)	clients2.g oogleuserc ontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 17:56:19.069463015 CEST	8.8.8.8	192.168.2.4	0xf339	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 17:56:19.072788954 CEST	8.8.8.8	192.168.2.4	0x5b0a	No error (0)	clients2.g oogle.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 17:56:19.072788954 CEST	8.8.8.8	192.168.2.4	0x5b0a	No error (0)	clients.l. google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.078095913 CEST	8.8.8.8	192.168.2.4	0xdf70	No error (0)	accounts.g oogle.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.079724073 CEST	8.8.8.8	192.168.2.4	0xe1de	No error (0)	login.micr osoftonline.com	ak.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 17:56:19.079724073 CEST	8.8.8.8	192.168.2.4	0xe1de	No error (0)	ak.private link.msside ntity.com	www.tm.ak.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 17:56:19.085897923 CEST	8.8.8.8	192.168.2.4	0xafdf	No error (0)	maxcdn.boo tstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.085897923 CEST	8.8.8.8	192.168.2.4	0xafdf	No error (0)	maxcdn.boo tstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.121548891 CEST	8.8.8.8	192.168.2.4	0x1537	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.121548891 CEST	8.8.8.8	192.168.2.4	0x1537	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.665986061 CEST	8.8.8.8	192.168.2.4	0x66d0	No error (0)	gstaticads sl.l.google.com		216.58.198.3	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:19.710727930 CEST	8.8.8.8	192.168.2.4	0x737f	No error (0)	aadcdn.msa uth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 17:56:19.764096022 CEST	8.8.8.8	192.168.2.4	0x236e	No error (0)	aadcdn.msf tauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 17:56:19.764096022 CEST	8.8.8.8	192.168.2.4	0x236e	No error (0)	cs1100.wpc .omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:21.555305004 CEST	8.8.8.8	192.168.2.4	0x5cb9	No error (0)	aadcdn.msa uth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 17:56:21.976864100 CEST	8.8.8.8	192.168.2.4	0x3eed	No error (0)	api.statvoo.com		172.67.159.15	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:21.976864100 CEST	8.8.8.8	192.168.2.4	0x3eed	No error (0)	api.statvoo.com		104.21.41.23	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.059315920 CEST	8.8.8.8	192.168.2.4	0xd2bf	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.059315920 CEST	8.8.8.8	192.168.2.4	0xd2bf	No error (0)	i.ibb.co		152.228.223.13	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.059315920 CEST	8.8.8.8	192.168.2.4	0xd2bf	No error (0)	i.ibb.co		152.228.223.13	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 17:56:22.059315920 CEST	8.8.8.8	192.168.2.4	0xd2bf	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.059315920 CEST	8.8.8.8	192.168.2.4	0xd2bf	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.059315920 CEST	8.8.8.8	192.168.2.4	0xd2bf	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.059315920 CEST	8.8.8.8	192.168.2.4	0xd2bf	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.160207033 CEST	8.8.8.8	192.168.2.4	0x9010	No error (0)	api-images.statvoo.com		104.21.41.23	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.160207033 CEST	8.8.8.8	192.168.2.4	0x9010	No error (0)	api-images.statvoo.com		172.67.159.15	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:22.266804934 CEST	8.8.8.8	192.168.2.4	0x82aa	No error (0)	www.google.com		142.250.180.164	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:27.476663113 CEST	8.8.8.8	192.168.2.4	0x675	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 17:56:27.476663113 CEST	8.8.8.8	192.168.2.4	0x675	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 17:56:28.263956070 CEST	8.8.8.8	192.168.2.4	0x5fd2	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 17:56:28.263956070 CEST	8.8.8.8	192.168.2.4	0x5fd2	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.161	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6584 Parent PID: 1256

General

Start time:	17:56:12
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.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:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 6832 Parent PID: 6584

General

Start time:	17:56:14
Start date:	03/08/2021
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=1592,3364816180486248382,9358393064765381631,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /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:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

