ID: 363748
Sample Name:
equinitiTicket#51347303511505986.htm
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 10:03:54
Date: 05/03/2021
Version: 31.0.0 Emerald

Table of Contents

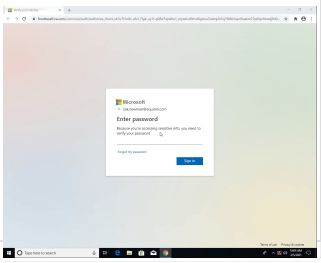
Analysis Report equinitiTicket#51347303511505986.htm

Overview

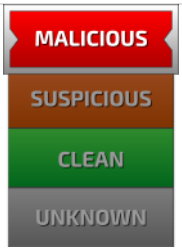
General Information

Sample Name:	equinitiTicket#5134730351 1505986.htm
Analysis ID:	363748
MD5:	07a72696ec306e..
SHA1:	56ce4d5adf0e27e.
SHA256:	ff12c57b1e82a05..
Infos:	

Most interesting Screenshot:



Detection



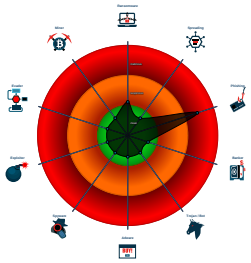
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6960 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\equinitiTicket#51347303511505986.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5684 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,15388751358428902676,16190953219467586011,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1800 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

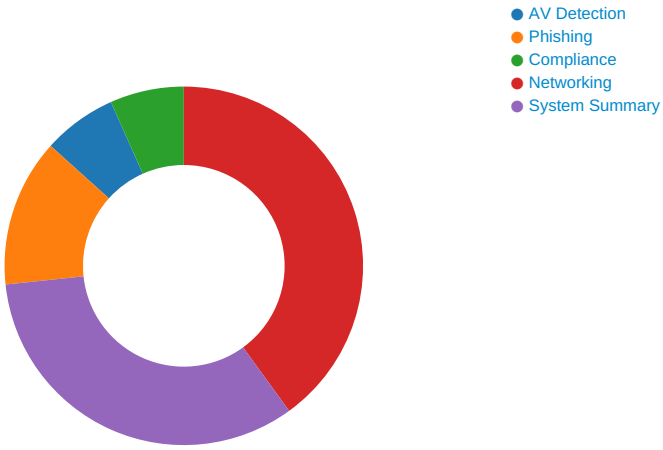
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

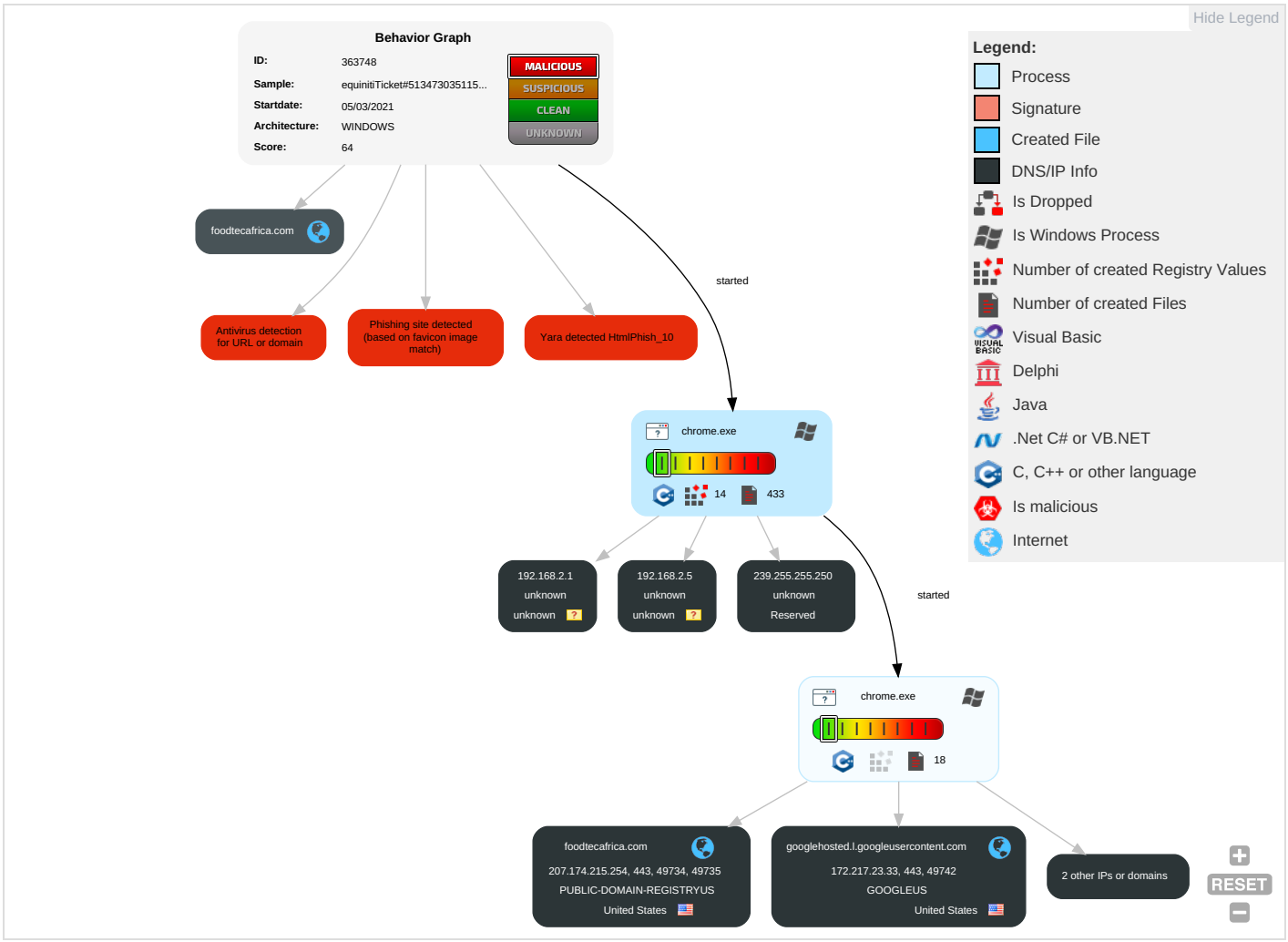
Compliance:

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

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

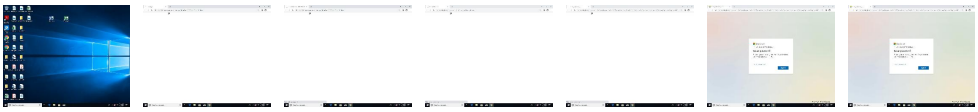
Behavior Graph

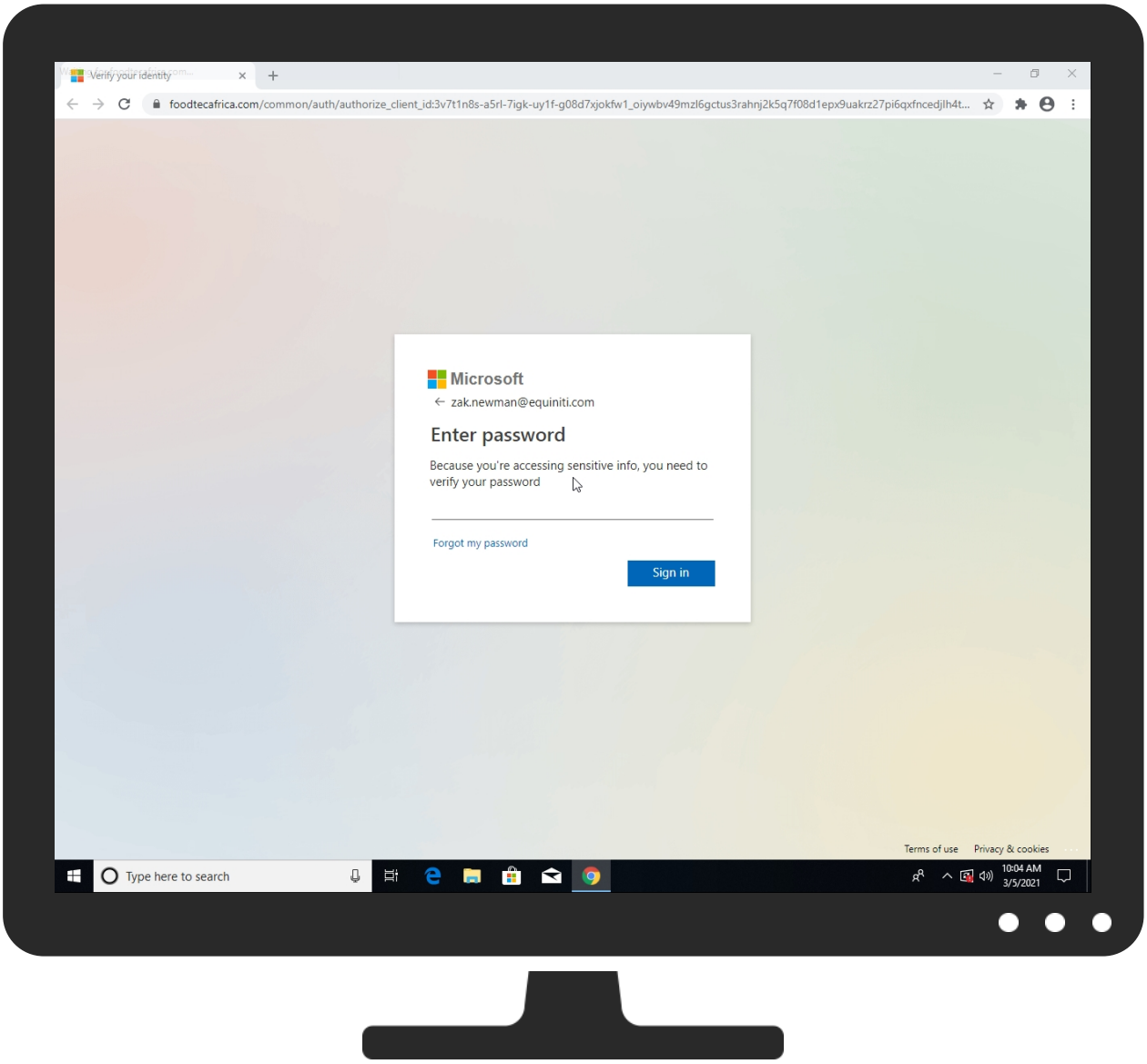


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
equinitiTicket#51347303511505986.htm	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://https://foodtecafrica.com/common/auth/authorize_client_id:3v7t1n8s-a5rl-7igk-uy1f-g08d7xjokfw1_oiywbv49mzl6gctus3rahnj2k5q7f08d1epx9uakrz27pi6qxfncedjlh4tmo8vy5g0wb13siynf6e2boasx5mgjph9twcdvk8zr3714ul0q?data=emFrLm5ld21hbkBlcXVpbml0aS5jb20=	100%	UrlScan	phishing brand: microsoft	Browse

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://foodtecafrica.com/common/auth/authorize_client_id:3v7t1n8s-a5rl-7igk-uy1f-g08d7xjokfw1_oiywb	0%	Avira URL Cloud	safe	
http://https://foodtecafrica.com/common/auth/?/emFrLm5ld21hbkBlcXVpbml0aS5jb20=	0%	Avira URL Cloud	safe	
http://https://foodtecafrica.com/common?zak.newman	0%	Avira URL Cloud	safe	
http://https://foodtecafrica.com/common/auth/?/emFrLm5ld21hbkBlcXVpbml0aS5jb20=Verify	0%	Avira URL Cloud	safe	
http://https://foodtecafrica.com/common/auth?/emFrLm5ld21hbkBlcXVpbml0aS5jb20=	0%	Avira URL Cloud	safe	
http://https://foodtecafrica.com/common/auth?/emFrLm5ld21hbkBlcXVpbml0aS5jb20=Verify	0%	Avira URL Cloud	safe	
http://https://foodtecafrica.com	0%	Avira URL Cloud	safe	
http://https://foodtecafrica.com/common/auth/?/emFrLm5ld21hbkBlcXVpbml0aS5jb20==	0%	Avira URL Cloud	safe	
http://https://foodtecafrica.com/common/?zak.newman	0%	Avira URL Cloud	safe	
http://https://foodtecafrica.com/common/auth/images/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
foodtecafrica.com	207.174.215.254	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.23.33	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

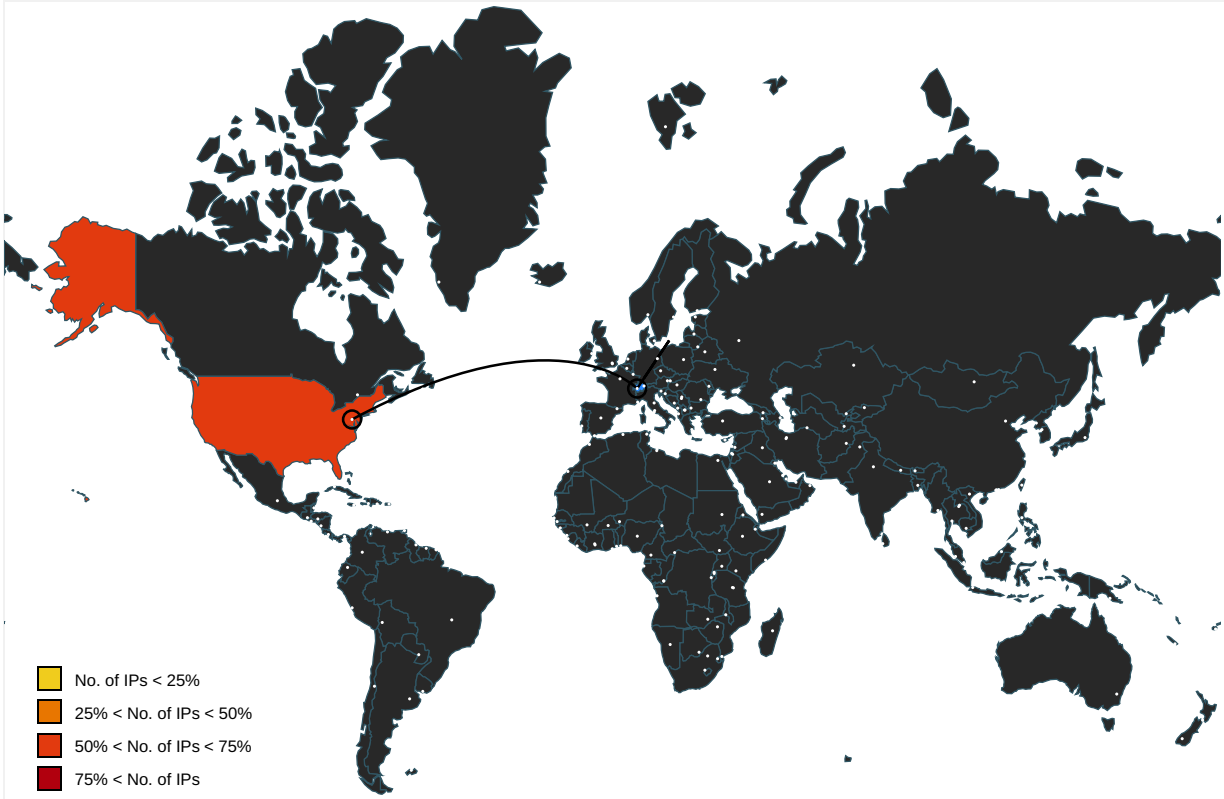
Name	Malicious	Antivirus Detection	Reputation
http://https://foodtecafrica.com/common/auth/authorize_client_id:3v7t1n8s-a5rl-7igk-uy1f-g08d7xjokfw1_oiywbv49mzl6gctus3rahnj2k5q7f08d1epx9uakrz27pi6qxfncedjlh4tmo8vy5g0wb13siynf6e2boasx5mgjph9twcdvk8zr3714ul0q?data=emFrLm5ld21hbkBlcXVpbml0aS5jb20=	true	• 100%, UrlScan, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	e72e0f2c-6e97-4ca9-8d2a-3cc80341ca33.tmp.1.dr, 5bccae93-e38e-4f82-9914-5484dce55fc1.tmp.1.dr, 5bd75231-5773-48a9-b9fd-f8c53144f5e5.tmp.1.dr, bafaf7f6-9d61-48b4-b4ed-987c02904db1.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://foodtecafrica.com/common/auth/authorize_client_id:3v7t1n8s-a5rl-7igk-uy1f-g08d7xjokfw1_oiywb	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://foodtecafrica.com/common/auth/?/emFrLm5ld21hbkBlcXVpbml0aS5jb20=	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://foodtecafrica.com/common?zak.newman	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://foodtecafrica.com/common/auth/?/emFrLm5ld21hbkBlcXVpbml0aS5jb20=Verify	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://foodtecafrica.com/common/auth?/emFrLm5ld21hbkBlcXVpbml0aS5jb20=	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://foodtecafrica.com/common/auth?/emFrLm5ld21hbkBlcXVpbml0aS5jb20=Verify	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://foodtecafrica.com	Current Session.0.dr, e72e0f2c-6e97-4ca9-8d2a-3cc80341ca33.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://foodtecafrica.com/common/auth/?/emFrLm5ld21hbkBlcXVpbml0aS5jb20==	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	e72e0f2c-6e97-4ca9-8d2a-3cc80341ca33.tmp.1.dr, 5bccae93-e38e-4f82-9914-5484dce55fc1.tmp.1.dr	false		high
http://https://foodtecafrica.com/common/?zak.newman	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://foodtecafrica.com/common/auth/images/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.174.215.254	foodtecafrica.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.23.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	363748
Start date:	05.03.2021
Start time:	10:03:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	equinitiTicket#51347303511505986.htm
Cookbook file name:	defaultwindowshtmlcookbook.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
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:	mal64.phis.winHTM@36/171@3/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.42.151.234, 104.43.193.48, 216.58.207.163, 172.217.20.238, 172.217.22.237, 172.217.22.206, 74.125.108.38, 142.250.185.74, 142.250.185.106, 142.250.185.170, 142.250.185.202, 216.58.212.170, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 172.217.18.106, 216.58.212.138, 93.184.220.29, 204.79.197.222, 20.82.210.154, 52.155.217.156, 20.54.26.129, 172.217.20.227, 173.194.160.139, 92.122.213.194, 92.122.213.247, 74.125.108.40, 172.217.130.6 • Excluded domains from analysis (whitelisted): fp.msedge.net, r5---sn-h0jeen7d.gvt1.com, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, clientservices.googleapis.com, a1449.dscg2.akamai.net, r3---sn-h0jeenle.gvt1.com, arc.msn.com, r1---sn-h0jeenle.gvt1.com, a-0019.a-msedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, clients2.google.com, redirector.gvt1.com, ocsp.digicert.com, update.googleapis.com, 1.perf.msedge.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, www.gstatic.com, img-prod-cms-rt-microsoft-com.akamaized.net, r1---sn-h0jeened.gvt1.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, accounts.google.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, www.googleapis.com, skypedataprdcolcus15.cloudapp.net, r1.sn-h0jeenle.gvt1.com, ris.api.iris.microsoft.com, r5.sn-h0jeen7d.gvt1.com, r3.sn-h0jeenle.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, r1.sn-h0jeened.gvt1.com • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

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

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Payments_Confirmation.exe	Get hash	malicious	Browse	• 204.11.58.28
	Payments_Confirmation.exe	Get hash	malicious	Browse	• 204.11.58.28
	PO #047428.exe	Get hash	malicious	Browse	• 208.91.199.224
	Gl2fGYPXPc.exe	Get hash	malicious	Browse	• 208.91.198.23
	VzbkNbEk38.exe	Get hash	malicious	Browse	• 208.91.198.23
	vn9cTg2oA8.exe	Get hash	malicious	Browse	• 208.91.198.23
	7pzxP3NdAG.exe	Get hash	malicious	Browse	• 208.91.199.224
	PROJECT KROHM STAHL GmbH Inquiry.exe	Get hash	malicious	Browse	• 208.91.199.225
	[1909373834] MT103 Credit.jpg.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO #047428.exe	Get hash	malicious	Browse	• 208.91.199.224
	6U9X8nSvQT.dll	Get hash	malicious	Browse	• 216.10.242.142
	BAYHthx8Ax.dll	Get hash	malicious	Browse	• 216.10.242.142
	CRQbVng2o2.dll	Get hash	malicious	Browse	• 216.10.242.142
	AlLFazTsKi.dll	Get hash	malicious	Browse	• 216.10.242.142
	uZWgLZmWY1.dll	Get hash	malicious	Browse	• 216.10.242.142
	sm6HLTjRy1.dll	Get hash	malicious	Browse	• 216.10.242.142
	0Nxv2y8QIW.dll	Get hash	malicious	Browse	• 216.10.242.142
	BNITMCa3F2.dll	Get hash	malicious	Browse	• 216.10.242.142
	OSvTx4VPM7.dll	Get hash	malicious	Browse	• 216.10.242.142
	v115p9stMY.dll	Get hash	malicious	Browse	• 216.10.242.142

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	condiz_03.21.doc	Get hash	malicious	Browse	• 207.174.215.254
	pago de documento de pedido.exe	Get hash	malicious	Browse	• 207.174.215.254
	remmittance859405__.htm	Get hash	malicious	Browse	• 207.174.215.254
	SecuriteInfo.com.Variant.Midie.79660.31247.exe	Get hash	malicious	Browse	• 207.174.215.254
	WinRAR_1845561462.exe	Get hash	malicious	Browse	• 207.174.215.254
	annualreport.xlsx	Get hash	malicious	Browse	• 207.174.215.254
	Weekly Vacancy Status Report.xlsm	Get hash	malicious	Browse	• 207.174.215.254
	Order MR-B. 04 03 21.exe	Get hash	malicious	Browse	• 207.174.215.254
	RemittanceAdvice-000010434.htm	Get hash	malicious	Browse	• 207.174.215.254
	Weekly Vacancy Status Report.xlsm	Get hash	malicious	Browse	• 207.174.215.254
	audio_shanti.ramesh@cae.com_file.htm	Get hash	malicious	Browse	• 207.174.215.254
	Weekly Vacancy Status Report.xlsm	Get hash	malicious	Browse	• 207.174.215.254
	PaymentConfirmation_9QE1-NSSB8U-CHF3.htm	Get hash	malicious	Browse	• 207.174.215.254
	Document (2).exe	Get hash	malicious	Browse	• 207.174.215.254
	SecuriteInfo.com.__vbaHresultCheckObj.5571.exe	Get hash	malicious	Browse	• 207.174.215.254
	Waybill.html	Get hash	malicious	Browse	• 207.174.215.254
	Synaptics.exe	Get hash	malicious	Browse	• 207.174.215.254
	MT103 SWIFT COPY TT.exe	Get hash	malicious	Browse	• 207.174.215.254
	V3HZtftyV5.xlsb	Get hash	malicious	Browse	• 207.174.215.254
	aJA1Ldh1iR.xlsb	Get hash	malicious	Browse	• 207.174.215.254

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\03a0c5e5-58a0-4387-9ea8-36a830cee9c3.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):	165129
Entropy (8bit):	6.081609912007944
Encrypted:	false
SSDEEP:	3072:9Fe2VQRlj6UuIX5KN7iW2inex9Oe4jFcbXafIB0u1GOJmA3iuRy:De0QvjfKkW2Xx9OewaqfIlUOoSiuRy
MD5:	736F0742081FAE2886B6C576A15DBDBA
SHA1:	68E3665C53646E2CDB16CF0BF7DB4E81B5F66B86
SHA-256:	758E0D2B5F4C105D36127E3EBB8EFC58CF27335E85128F6AD765FAD3BFE8D5BC
SHA-512:	F01F9BE692661DA82D6049FF6A6F5CB7F4D0E5469AB7A16845C963C32A12E8848FEEA4C61CF80562CFADAD17D55E9AD5421001FADA74C8243B6AF7DA5C31803
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\03a0c5e5-58a0-4387-9ea8-36a830cee9c3.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":1.614935085943618e+12,"network":1.614935087e+12,"ticks":305376941.0,"uncertainty":4782826.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+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\30defbab-99ea-4aec-b2be-163024b6888c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94772
Entropy (8bit):	3.7383108200688167
Encrypted:	false
SSDEEP:	384:mL0Ln9OsRqB9VawXSNHrUvzp3kjlgH58G4nridnfxURdZcrmnmWCgep3XvAOxRPD:AaKVVuJgkQeXTx9QP3SVKn97w0
MD5:	B6B4789E12AA96FE0D85AA2CE83085AA
SHA1:	1CB38661BB0D506DFD6DA087A568D851BAEF74E8
SHA-256:	77A3579696E91241DE4E7B75261A103BC0E8F2B63A62F599FB61D198A80B6367
SHA-512:	0AED410AAB13D9B9E57AE95DA8F581C0F72203D4B08A21FC5BF6898C1FFAF1C29B51531543D5334FC1BED7AE6F4A1DCE6BB0FB5DB8106CD9FE378ADE4A1A6B9B
Malicious:	false
Reputation:	low
Preview:	0r.....*...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.....*...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...a38.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\4db1974b-9d5a-41b2-af1d-7018f13f1c23.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):	156884
Entropy (8bit):	6.052081906918273
Encrypted:	false
SSDEEP:	3072:b2VQRlj6UuIX5KN7iW2inex9Oe4jFcbXafIB0u1GOJmA3iuRy:b0QvjfKkW2Xx9OewaqfIlUOoSiuRy
MD5:	F2D66DE03E2B9FF5F6B2AFCC3A14742A
SHA1:	A60E87F1F7E6D782679E2B93F9459FCCCF92FE28
SHA-256:	5CD9706C0361C42AC101E0CBF2579354436CE870DB14DB82483B250AC6E37606
SHA-512:	DD646B2A4428E67D03F8B553FEBAC143FFE6602FE4EFA7D75FB8C8A05E7746AC5080568E116CBAA336A0A3C067BDBEA4E17DCB41ED4FF2A9EBB230D312E2B737
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":1.614935085943618e+12,"network":1.614935087e+12,"ticks":305376941.0,"uncertainty":4782826.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":

C:\Users\user\AppData\Local\Google\Chrome\User Data\5b8215bb-e8a6-441a-b515-36bf25456c8a.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):	165129
Entropy (8bit):	6.081609912007944
Encrypted:	false
SSDEEP:	3072:9Fe2VQRlj6UuIX5KN7iW2inex9Oe4jFcbXafIB0u1GOJmA3iuRy:De0QvjfKkW2Xx9OewaqfIlUOoSiuRy
MD5:	736F0742081FAE2886B6C576A15DBDBA
SHA1:	68E3665C53646E2CDB16CF0BF7DB4E81B5F66B86
SHA-256:	758E0D2B5F4C105D36127E3EBB8EFC58CF27335E85128F6AD765FAD3BFE8D5BC
SHA-512:	F01F9BE692661DA82D6049FF6A6F5CB7F4D0E5469AB7A16845C963C32A12E8848FEEA4C61CF80562CFADAD17D55E9AD5421001FADA74C8243B6AF7DA5C31803
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\5b8215bb-e8a6-441a-b515-36bf25456c8a.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":1.614935085943618e+12,"network":1.614935087e+12,"ticks":305376941.0,"uncertainty":4782826.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+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\6940f551-cbe9-43c2-bf80-0b1fab78159e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94052
Entropy (8bit):	3.738721752492618
Encrypted:	false
SSDEEP:	384:4L0Ln9OsRqB9VawXSNHrUvzp3kjlgH58G4nridnfxURdZcrmnmWhep3XvAOxRPNv:OaKVVuJ0kQeXTx9QP3SVKn97wy
MD5:	47AACC065C54284F6D50C66772FD916E
SHA1:	895A45C8593CC10BB0D58096C51268B8BEB443E3
SHA-256:	CDB15DB46AFEA6CDE38E8E0594C2DB814F5DEEC6E8A815F6A552E31E3B61D041
SHA-512:	960C22690AA6328FFE5CDA2DEC5EF46443B77FF5B19E52A32BEC594A274E9F2DA33B3996BFFC4BB300412B0F449A9AD2A822ACAC210A3AF6827294B1CC32ADE1
Malicious:	false
Reputation:	low
Preview:	`o.....*...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...a38.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\7238b5f9-3653-435c-88e9-dfefaafea197.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):	156641
Entropy (8bit):	6.051363579364118
Encrypted:	false
SSDEEP:	3072:T2VQRlj6UuIX5KN7iW2inex9Oe4jFcbXafIB0u1GOJmA3iuRy:T0QvjfKkW2Xx9OewaqfIlUOoSiuRy
MD5:	FD7593B2321A1C2A87F96EAE4BC238A8
SHA1:	FEA9BD192A735B8DBC2149F0093E51D025C7B8E3
SHA-256:	6EADF68D9552AC5994FC97902CADF3806E710897523178A3B961BA1B00969BAB
SHA-512:	8407CC456FA23FAC20513A451190F67F35D57F64ED5DA163C3B21B699740BD21FB1E034609C5246B57F105395C995862F152E875C6750B8A7AD233A2A92F5BFA
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":1.614935085943618e+12,"network":1.614935087e+12,"ticks":305376941.0,"uncertainty":4782826.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715727952"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\94262eb7-32b3-4221-94ce-f0aae00850d7.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):	165129
Entropy (8bit):	6.081609833072234
Encrypted:	false
SSDEEP:	3072:tFe2VQRlj6UuIX5KN7iW2inex9Oe4jFcbXafIB0u1GOJmA3iuRy:Te0QvjfKkW2Xx9OewaqfIlUOoSiuRy
MD5:	2CEA1DC316940BCED2D7CDC5B4203B8D
SHA1:	552BC6DE0EA486874EC6915475325D0BF3D3F417
SHA-256:	D3593DB0216F0CFFCFDEE38A1374A26EFE9B1260F4A4B4111DD152C8C1F1F4AB
SHA-512:	49F4D04788BE0D7959A5EC4B3FB6E9C9BAF60B09457F055DB377152A2501B2BA5E6E6177723FAD8F355DA920B7CA99E0C23BE8F05AF185EBEBABA85C3CBD1CD6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\94262eb7-32b3-4221-94ce-f0aae00850d7.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":1.614935085943618e+12,"network":1.614935087e+12,"ticks":305376941.0,"uncertainty":4782826.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715727952"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\957c9426-6dc8-42f9-a64b-37271ae45a76.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92068
Entropy (8bit):	3.7380312971803047
Encrypted:	false
SSDEEP:	384:3L0Ln9Os9BGXSNHrUvzp3kjlgH58G4nridnfxURdZcrmnmWhep3XvAOxRPNO1vuO:cKVVuJ0kQeXTx9QP3SVKn97w5
MD5:	02A07A34CAA790699523E7BA923C9388
SHA1:	F9007266B52F8FD73036DD57266BEEDAF245593D
SHA-256:	EBF15D6AAFAAE4BBB4F05102920106306279E1514BDA887103FEC661D9BCE8B5
SHA-512:	46A4E0BC2A05B7E711A4616BDA467780F9B096920D4B2DD694D79F4F9A8C2684006D6A8CBC06591044C3C6E2F526BB5DD8EF5BACEAF23A03D4992D3F4BD5B94
Malicious:	false
Reputation:	low
Preview:	.g.....*...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...a38.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	moderate, very likely benign file
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\2d42eebd-bd10-4bf1-ab75-6e950f0ce2a3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22618
Entropy (8bit):	5.535564595455083
Encrypted:	false
SSDEEP:	384:NXA1tnLlnLXA1kXqKf/pUZNCgVLH2HfDGrUMHGrnZdvC95c4R:ALlTA1kXqKf/pUZNCgVLH2HfirUAGrn+
MD5:	5BAD3BF13254E76577876F02A623C801
SHA1:	63B7F80B94DC1E61FEFFE4B85D37A1C78C47ABE2
SHA-256:	A7D29749BA49CD086A73809FD64163B0D89EF261BCBC0E36B5D0F36F325E54AD
SHA-512:	8E06434BB1114575F40E34D3A059C12DDC3E7C52400FB7E003D5B9D434913857A4E439CF28BEB563945D93E6EB0433CCB39E2D44B8874C98FEB41462701E3D60
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2d42eebd-bd10-4bf1-ab75-6e950f0ce2a3.tmp

Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13259408682716888","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\37e6ab63-00ca-4ede-8e83-cfe32e62e863.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):	5392
Entropy (8bit):	5.150101040661784
Encrypted:	false
SSDEEP:	48:YcKkMkliljwqALRqpgcBLb2t4lYGlQuoTw09kwrf4MqM8C1Nfct/9BhUJo3KhmeK:n8Lhk4pgcBHHIVH5k0JCKL8bbOTlVuHn
MD5:	CE0D80FA21A577F6DEE26376092C0461
SHA1:	A225BE9923EF45CE91DA863E10E3B01BCA2C38B3
SHA-256:	AB1F0FE26E659C0BBE4BDA7822BD37F4FF4419970B50B8C79FEEA5B32E2F92AC
SHA-512:	EE34BC91E725F62D9B189F63DEFB40DA3E8BC59EC73B1928A1D88951EA24FA5BE5B14F43EC9EEF29266B65872670E54C1C4B84073D106490949AFFA8E7F2989
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13259408683001031","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5bccae93-e38e-4f82-9914-5484dce55fc1.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIlyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	moderate, very likely benign file
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\720c0f87-269c-4f42-a7fe-af5c088991a1.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22620
Entropy (8bit):	5.535928550156024
Encrypted:	false
SSDEEP:	384:NXA1tKLlnLXA1kXqKf/pUZNCgVLH2HfDGrUMHG4nZivW95c4v:7LlTA1kXqKf/pUZNCgVLH2HfirUAG4nJ
MD5:	F7D5F4685F2B8249044B9113B1B077C9
SHA1:	3F483A5EE6A95E8EAC0E33FFD3BB7CC9B25BC690
SHA-256:	164BE63292C73FBED8DADAAC29EFA40B4D4230A8D4D0AA28AD65F51F15DB5A4A
SHA-512:	4DBD8E6291C77CB05047E9DCDB13D6208A3C5BE709DF2FE7F4570A9FD5F993087678DAD6C99A47F9E4621ABF2789B052F4212B5C45E005D40B0597C4B36BAE C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\720c0f87-269c-4f42-a7fe-af5c088991a1.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13259408682716888","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.205730652065178
Encrypted:	false
SSDEEP:	6:mxfmqRNAVq2Pwkn23iKKdK9RXXTZIFUtpyfm+AgZmwPyfmEuAIkwOwkn23iKKdKT:cm0AVvYf5Kk7XT2FUtpMm+Ag/PMm5AIz
MD5:	227670400960B7A107829AE3DE99B009
SHA1:	74C4C5EE152CFDDA25795F40E846F22293DBDFCD
SHA-256:	60927EB519491F0F4C34675C448292B0B4C1DCFAB039C9888E57693828C07497
SHA-512:	43A85E800366800022945B1886DC2AF952A20E6B6FCA42C37B4EE7DCE5A94C92B39A8106BBD7F0F628F8BB7C2C19A827C1E72B621E9768CC3BA199381CE2E22
Malicious:	false
Preview:	2021/03/05-10:04:50.826 1bb4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/03/05-10:04:50.828 1bb4 Recovering log #3.2021/03/05-10:04:50.829 1bb4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.18325900002891
Encrypted:	false
SSDEEP:	6:mxfgLAVq2Pwkn23iKKdKyDZIFUtpyfmiNAgZmwPyfmINAIkwOwkn23iKKdKyJLJ:cgLAVvYf5Kk02FUtpMmiNAg/PMm6AI5E
MD5:	7BE25670C9F9996D53F1DC6F6B062AFD
SHA1:	ED61838EC1EB215A7DD4C0284AE7ACCA6BF4A50D
SHA-256:	0E146B0AA51130C3182F7D871FC20C67F989269F8E12CAE83698260583E37862
SHA-512:	F28DBD61BC9852707B24BCD1E27A46DB6E7D82635EEC29969AAD2FA22BFDC66F7039638BCDB357443CA4D89E5A1421412E0EAEB51C196A5728B2EFBA93F5DEF
Malicious:	false
Preview:	2021/03/05-10:04:50.793 1bb4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/03/05-10:04:50.800 1bb4 Recovering log #3.2021/03/05-10:04:50.806 1bb4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	1.1247061729326566
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwZEEV7lzde9D6pf1H1oNJyhLrP:TekLLOpEO5J/Kn7UrE3dDfvoNCLrP
MD5:	EF48BC650B9391BC1F1514D2BAF672C0
SHA1:	C55B1FCCC919DE1CC6F46C85F4AA2A09A1D92859
SHA-256:	BDD9590731B79F3F87E8883E3221826E4FE4B26BDB1882E007D0212E50D1895E
SHA-512:	84A7BEC2C819CE691B8DFA40AB7A5F451A7B32A4521E95EEC124046186E078392DCC27C143B0821BF641F35167808C4BE14C343E6706A7D02F8B92442D637F30
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Entropy (8bit):	0.9736773196074099
Encrypted:	false
SSDEEP:	24:+e9H6pf1H1oNcFqLbJLbXaFpEO5bNmISHn06Uwv8:+bfvoNcFq5LLOpEO5J/Kn7UA8
MD5:	760E77012AC5689C88DF97A7179715E2
SHA1:	C60DCE9D58F1ECEE5CF2C80651388180AA005673
SHA-256:	E41549DA294640398E286FD8C3ADC6D266F6C780001B2FE091DF142BCE39D59A
SHA-512:	0ACC8C2A8A8F8048CCB0C5EC7C0D647E435ECCE4E2932DD6F3D592CBA79704F6ECA5532578DF047223B348D24847433EC6E88D1EC9775AFFE43C3AA7B9F78 29
Malicious:	false
Preview:	.....h.9..... ....

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):	2575
Entropy (8bit):	3.960132494591614
Encrypted:	false
SSDEEP:	48:34wyxXxML7XqRCxzjIFzf+OWEfi/OPfrK1xdSxukxuj:34wI86hvfKOH6
MD5:	63E9FBB24E2A6810E5DAB6C5E5959CC7
SHA1:	8480ACED2D4B0EEFEA0C5F6751C8F6733936B47E
SHA-256:	B57990BE2C43BD738F98AAA23722589886216571E8D9DB200AD49D7078AEA0C2
SHA-512:	709697962EE82A8C6AFB8828236D6B7BC3EE8BD08ABFA556CEC2D283D368563BDA5FCFE901CF7E90A94882AC35846E1F6C176206C1621E22994512A6DB9A9D1 E
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...996e9fa7_4d35_4296_a94f_6ea60aab6351..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....E...file:///C:/Users/user/Desktop/equinitiTicket%2351347303511505986.h tm.....h.....`.....\..`...]..`...8.....P.....E...f.i.l.e.:././/.C.:./.U.s.e.r.s./.j.o.n.e.s./.D.e.s.k.t.o .p./.e.q.u.i.n.i.t.i.T.i.c.k.e.t.%.2.3.5.1.3.4.7.3.0.3.5.1.1.5.0.5.9.8.6...h.t.m.....8.....0.....8..... ....E...file:///C:/Users/user/Desktop/equinitiTicket%2351347303511505986.htm.....

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):	5.1429228771733575
Encrypted:	false
SSDEEP:	6:mxfNCVq2Pwkn23iKKdK8aPrqIFUtpyfpu+gZmwPyfHzSIkwOwkn23iKKdK8amLJ:cNCVvYf5KkL3FUtpMA+g/PMeI5Jf5Kkc
MD5:	FEF02069B3BD97845EFB7707A697BBE6
SHA1:	2220DA854EADEB5AD0CAEC63FFE6951ACB976EF8
SHA-256:	39E1B0CF47A9DD7121855128EFF4AFF7706FDC6C969DB9E29627CE042BCB7BB8
SHA-512:	2412941C9CB434AA5D659864C4B8777D2872AC245D73F9349BFEEE9900E739D59DA922BA49F8F1DF0C0E1DC777D9736CDB0423C90A497DDBFECA4EFF14179C B
Malicious:	false
Preview:	2021/03/05-10:04:43.006 1680 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/03/05-1 0:04:43.007 1680 Recovering log #3.2021/03/05-10:04:43.008 1680 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT: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.....

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):	5.175422588788153
Encrypted:	false
SSDEEP:	6:mxfz6Vq2Pwkn23iKKdK8NIFUtpyfzojgZmwPyfzojIkwOwkn23iKKdK8+eLJ:cz6VvYf5KkpFUtpMzojg/PMzojI5Jf5c
MD5:	AE316B532A7515C91718BB3F2EB9141B
SHA1:	69C96FE66596D9315AB4093DBE241F947C8FA298
SHA-256:	BAF8AB91E05F7571E2401EEFEDC73A2A8D90AE906F3D533EB881D719C351CBF1
SHA-512:	38492F7A42D4737D27FF40D7369A6CC5BA322DB837A6E6730BCF345337D0F552B2B896E824BDB7BECF57DDBA6706445446D58CC8D090DE09897A4F00FD09612
Malicious:	false
Preview:	2021/03/05-10:04:45.366 1be0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/03/05-1 0:04:45.368 1be0 Recovering log #3.2021/03/05-10:04:45.368 1be0 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\comput ed_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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.121829143514594
Encrypted:	false
SSDEEP:	48:tBmw6fUOxJuxaOxzjIQIxWxuOGxdSnw1Ok0ITXUBdsxx7xJKxFxzjInxwxutjYP3:tBClzSwsnITkvub6
MD5:	7EC9336D4CAA09DFAAC70DAA2A49134C
SHA1:	719A3BAD4D04F36456C8A1D7B002B1F3098437D2
SHA-256:	EE7BD11BB811810CA01EEB2B6DF15C4ED3F8169C3CDEAB6A2887BDD6F2D380D3
SHA-512:	26BBF1EAF48F4D815F39442142C94130AFE9BE8B785FC682867F78C5B712B9C34FAC43E62630E2D5A7E39460818E8543968189DBCE04F3BFA46AFF72563C1DC9
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.8116279599340828
Encrypted:	false
SSDEEP:	24:h9rTl+PQOAyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6UwK3n:JuqCBmw6fUR3n
MD5:	22CBE671565C7F0642ED35BEEDAB4BC1
SHA1:	5F26B8872F78FB7D604749782CF29ECD33E4EFD6
SHA-256:	02088B23E1B239E276819BDB352FAA47FA9385579C57AEC8E9107A0FB672D0FC
SHA-512:	CC85627C609608882B0298B9CC847EF36A974E0E8FF5C24D5C7D10344D4E7D3A37252E0BED03360AC7C97C0DC3DDF7FA853DE3ED1119A1FC44D61007EB13B15
Malicious:	false

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.196394589381303
Encrypted:	false
SSDEEP:	6:mxfo/uHxNAVq2Pwkn23iKKdK25+Xqx8chI+IFUtpyfozAgZmwPyfo94AIkwOwknl:c5HxNAVvYf5KkTXfchI3FUtpMqAg/PM8
MD5:	C2593FC539B21196FF688513D703CC7A
SHA1:	331A37D3CF537AE62CA55112DEF1E014F70FFDEF
SHA-256:	62E906905268A33EBFAFC4A2A353AB797F186BFA543EC93419EAA1BF0FBA7199
SHA-512:	DB5B17FA68858CD1D0C9E97D217ED2ECBB0D7B4D1E49FC5EEF83D69B248B4F8FC524E20048CC84814069C4EC22FBFF121C1F1EC0FA2199FB9134AA13B3A015F2
Malicious:	false
Preview:	2021/03/05-10:04:50.600 1bb4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/03/05-10:04:50.601 1bb4 Recovering log #3.2021/03/05-10:04:50.602 1bb4 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):	5.207557054655487
Encrypted:	false
SSDEEP:	6:mxfSYLAVq2Pwkn23iKKdK25+XuoIFUtpyfs8NAgZmwPyf7LAIkwOwkn23iKKdK28:cLAVvYf5KkTXYFUtpMs8NAg/PMPAI5JZ
MD5:	2D05CE98D44265104DC3E78C888DB87E
SHA1:	2F95400F997F6AED66DF7EB74E545B96DDBE378A
SHA-256:	DCCE28470B9A206EB2ADFB8026FA7931EF44107DD38BA113838F57A7E0BA998B
SHA-512:	FD3DF3D2D5BBA8378A712D2079A8C853CB563B5898FD73868FB80B891192E776F617E203C8926A2BDF978F4BF4178FEF845EF1D66AE397BF9A88D78BC1BE35EA
Malicious:	false
Preview:	2021/03/05-10:04:50.574 1bb4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/03/05-10:04:50.576 1bb4 Recovering log #3.2021/03/05-10:04:50.581 1bb4 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):	5.2103880785220085
Encrypted:	false
SSDEEP:	6:mxflt+q2Pwkn23iKKdKWT5g1IdqIFUtpyfKXZmwPyfztVkwOwkn23iKKdKWT5g1L:cOvYf5Kkg5gSRFUtpM6/PMP5Jf5Kkg5i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
MD5:	26B19A7EF1DA983DE24DC25045E2DC53
SHA1:	80328D89C8B42881902FD09652DB76BB63EB8345
SHA-256:	C39B41432B8229CC3AE984B8FA96EEF119DA8D6EA52D273555C1CE2218B52E15
SHA-512:	5C7AD397115BD479F31292D7535A5720D1FC47069F0D183F220C15230217EDFC5DA82198EFFE4B79FDDC310FA2216E2B25374B6CC218BA8F980E7787BD02285(
Malicious:	false
Preview:	2021/03/05-10:04:50.301 1bb8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/03/05-10:04:50.306 1bb8 Recovering log #3.2021/03/05-10:04:50.307 1bb8 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):	0.6416664914895375
Encrypted:	false
SSDEEP:	48:TImxzjIYYUmxJRmxkhmxFx5hmxu8lN/qD+lUd4dbdWhnTxzjIRxHxwxuNxJt+:snKA/GDSl4+gqhnM
MD5:	498BED7D8B85F8D97B56E147D86AAA07
SHA1:	FFEFBC7A435F45C08A323B1ACB93285713806760
SHA-256:	F45A983433EE00344F36AF22AAB4F28FF03CC1A2A96C497F8B97B43D1591C76D
SHA-512:	E506682ED5C2C42474F09795B1A0D9E065C71270337A89AA1F2E0B0BDE0680E76EF499F58CBBCF0FBB3C4D93225E5B0E70DE434F19B107028DFD59CC7E30364D
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.6685058710427985
Encrypted:	false
SSDEEP:	24:wtUTlJVbP3ieTXykp1GPqQv55d/B9KcPcp/NBDOxo7nQBr1xx6MfbS4KfJpo+SHp:wulVbPye2kpgqS5dZ28J1xJO4KfTYHe4
MD5:	17597951BAD38319092F15CB11D5A85E
SHA1:	B923ED0B753E5007B94B6B8E45E9649D48E6713D
SHA-256:	2B56E44C43014BB03F1D3881EC1E3431D2F501AF9E1F237B7F118589260AA0B5
SHA-512:	7EBB69F3A37CF6F3599CF157DDE04521779A7BE9D3DB580DAF27361BAC58E674952FB9213EE0DD4F1DAD24840CD783432EFED9482401C9B7ABD7B21E243FBA4E
Malicious:	false
Preview:	....."......0ffice365..com..common..equiniti..foodtecafrica..https..newman..review..zak..51347303511505986..c..desktop..equinititicket..file..htm..user..users*.....0ffice365.....51347303511505986.....c.....com.....common.....desktop.....equiniti.....equinititicket.....file.....foodtecafrica.....htm.....https.....user.....newman.....review.....users.....zak..2.....0.....1.....3.....4.....5.....6.....7.....8.....9.....a.....c.....d.....e.....f.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....z...:..... .....B.....m..... .....*8https://foodtecafrica.com/common?zak.newman@equiniti.com2.Review: 0ffice365:.

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):	0.11707046864565286
Encrypted:	false
SSDEEP:	12:SMvkvqLBj/v3lA4nMWQASjG9LEOBQZ8fOD:RkvqLBv33f1NJTfm
MD5:	24C2CB9BE39026664E6924BD60CC5724
SHA1:	9B9379FD8773E293F471541F5BAFD9D553CB0FD3
SHA-256:	2355E8A4DBD1E875105A83AAE8BAB8E2D3280AEF0AF5553E723F12CE92D3DEF3
SHA-512:	B423A28411EBB4C286ED8B73D9DC728AA89FDF4F2A515DB95FA703D4076770046A43ABEBCB186C2E516AB27DFAD732D4FB34EAF72259DCA7F3F0440C9050426
Malicious:	false
Preview:	.....E5W..... ....

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):	5.47543660260798
Encrypted:	false
SSDEEP:	48:VZYGe1a7pM58dbkOp+pDbQSefgGzNrS0U9RdiN9s:VEa7pM6dbkwADbQ5fgGhrS0W
MD5:	CE1B91732C53A0822E6E1CF6900F8776
SHA1:	B2D1A1EBD3FA0CE214CE1DD96E943603B944EDEA
SHA-256:	C11036D3CA81FB81B42CF7061BAC9A912600D4213A684AA423C2C367F21C26EA
SHA-512:	241C90602CBEA791A5A80F2C3A9721BABC379B85B75AE1644F428026DB56E6B1B102FB6C78F73FD3850D59A7358F74620185B7F4F99EA7AE73B0A2DE39EEEB83
Malicious:	false
Preview:	.Q.G...*.....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..416265000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-03-05 10:04:52.70][INFO][mr.Init] MR instance ID: 8df6e546-1771-4b67-9356-1c26642f08a3\n","[2021-03-05 10:04:52.70][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-03-05 10:04:52.70][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-03-05 10:04:52.70][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-03-05 10:04:52.70][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-03-05 10:04:52.71][INFO][mr.CastProvider] Query enabled: true\n","[2021-03-05 10:04:52.71][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):	5.201782844575109
Encrypted:	false
SSDEEP:	6:mxfsBM+q2Pwkn23iKKdK8a2jMGIFUtpyfsNXZmwPyfsHpMVkwOwkn23iKKdK8a23:cgM+vYf5Kk8EFUtpMyX/PM2pMV5Jf5KV
MD5:	E9F556BC5460FEB6F52189BD236BF21F
SHA1:	520C8BA55970E73A9589C3F5A1AAE40CF08BD0EF
SHA-256:	CB1DFA5CC7C44E88DF06AF6D9C4B443C642E266AA66AE6C1D67070D7A9577D91
SHA-512:	81DBE57E45E8A0CB02DD97941B7514604315D6E6CDA9F6D47FEA795DE2C4C14E1BBD7AA58F0261ED94FAD20707FAA47B53E062FFA14FF9EB512D00D3E80F43B8
Malicious:	false
Preview:	2021/03/05-10:04:42.780 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/03/05-10:04:42.785 176c Recovering log #3.2021/03/05-10:04:42.788 176c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.170011740723077
Encrypted:	false
SSDEEP:	6:mxf4CVq2Pwkn23iKKdKgXz4rRIFUtpyf6gZmwPyfyIkwOwkn23iKKdKgXz4q8LJ:cTVvYf5KkgXiuFUtpM6g/PMyI5Jf5Kkt
MD5:	E851F92DCDADEA5DB8329057C9ACA18B
SHA1:	68867CDA59696838A93B8046CDAB557ED9CFAB3A
SHA-256:	11822A1F8ACAC1E73BC9D10EAECB02182359F43B0B60BC3BB8D837FAD32C93C7
SHA-512:	0CF65ADFE4EA28746AD480EB1D7B0958C9C728EC855DC03AD9826CA45667458D65892E1F7A41C5C7792F15460DFDF6A05B18B940E7C3EBD0745073EC10F06FA
Malicious:	false
Preview:	2021/03/05-10:04:43.038 1680 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/03/05-10:04:43.039 1680 Recovering log #3.2021/03/05-10:04:43.040 1680 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
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):	5.161337685047875
Encrypted:	false
SSDEEP:	6:mxfguVq2Pwkn23iKKdKrQMxIFUtpyfglCgZmwPyfglCIkwOwkn23iKKdKrQMFLJ:czVvYf5KkCFUtpMtg/PMtl5Jf5KktJ
MD5:	36275AF0B62B463058CB6878E9CE0133
SHA1:	E4CBDC1A5D959F5A51989BE814CFA7ADD95E8A2A
SHA-256:	DE0275CD7B6225F71881E99A3FBE1DB35EA26CB9CD05E49E97BA681E1151235B
SHA-512:	46BE61F41DF218B10E22883B7775E886108C85579E9534BC16F365A9BBFF3E5B03AC1697AE040A76471AC4B815973413351647F6782FB7AFA62B30DB56DDFFA4
Malicious:	false
Preview:	2021/03/05-10:04:42.963 1680 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/03/05-10:04:42.965 1680 Recovering log #3.2021/03/05-10:04:42.965 1680 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):	5.138779836073714
Encrypted:	false
SSDEEP:	6:mxfZ5jyq2Pwkn23iKKdK7Uh2ghZIFUtpyfkCR11ZmwPyfkVRRkwOwkn23iKKdK7w:czyvYf5KklhHh2FUtpM/RX/PMaRR5Jfl
MD5:	89E5A4E30BA0D58D568BFB76F3D09260
SHA1:	677186C94506C712BF169FF5C2B24F77BB9A333C
SHA-256:	781E453A036FB6AA3BCBB68DB543C48361B1A00D1C40261561A5A0A5A411081A
SHA-512:	EDB2007C19CE838C07B1FF6045C3531CF81814287C45DFA27563C190F3BF8200C69D00E1E3F0A83CA0F2B882C896BDC9FACB23C53E33F5DD20A79B16AED3049
Malicious:	false
Preview:	2021/03/05-10:04:42.699 1be4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/03/05-10:04:42.701 1be4 Recovering log #3.2021/03/05-10:04:42.702 1be4 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\5bd75231-5773-48a9-b9fd-f8c53144f5e5.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
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):	5.252083148756653
Encrypted:	false
SSDEEP:	12:cuEVvYf5KkFFUtpMN3g/PMN3l5Jf5KkOJ:e5Yf5KkfgynSJf5KkK
MD5:	F18267AC8F76A6A819D89145680EFD74
SHA1:	B5EBD01A0FA8C7ED1993731824D8A507913844FA
SHA-256:	45182A623C5B76B092A7670C5BC2C3DDFA8A78302C8530D0559923F05ABD4685
SHA-512:	D7D5B7D8D41854764F189367BCE135E4599CFC1C22BEEEBD9D7C5488ED08D455AB93ECFEAF2D60CF510836CCA950A50A4449FBEFB36160D2D4E953AA46B2BB0
Malicious:	false
Preview:	2021/03/05-10:04:42.989 1680 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/03/05-10:04:42.990 1680 Recovering log #3.2021/03/05-10:04:42.990 1680 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.270746883336452
Encrypted:	false
SSDEEP:	12:celM+vYf5KkmiuFUtpMfd6/PMoMV5Jf5Kkm2J:dYf5KkSgGJf5Kkr
MD5:	07AE67F81FC31D385C9FC6A8EA76E2FB
SHA1:	4C3EB262110EC2E4DB3D48DE48AD6E55B92F0CD4
SHA-256:	74E4475E63BC56632F7DA1AF42CC81C732FE892F86104945E43436D2B77BBA82
SHA-512:	EBCB44BB1793BEE73C4006206CAF191A2BA304A0E96D113E38E38E10D2C9F84728EB035C132A702631B9142E1436E2EB6D778916807D45D0E3B5D6DCBD41F53
Malicious:	false
Preview:	2021/03/05-10:04:43.039 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/03/05-10:04:43.045 176c Recovering log #3.2021/03/05-10:04:43.046 176c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.24358772225487
Encrypted:	false
SSDEEP:	12:cewVvYf5KkMFUtpMNDg/PMNDI5Jf5KkTJ:25Yf5KkUgwDLDSJf5Kkl
MD5:	6EB419F5D5C04EF313408585E7F78490
SHA1:	0DD2A7E72405C3C8EE43D035468AE83CBF1A7E52
SHA-256:	30D36FF51DB6ABD0E6A6A031B447AFCAEAED575E742222CAE191EC696B7BE8BB
SHA-512:	C89655ADBC44C06420593720F8039D0AC215379CC1BB8CEF00F508CC140BAA41D07348A081EEF4546A4B0A2BDA019D3B5D0EB74530EA046232D34C442EDBB85
Malicious:	false
Preview:	2021/03/05-10:04:59.276 1be0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/03/05-10:04:59.278 1be0 Recovering log #3.2021/03/05-10:04:59.278 1be0 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\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):	5.17790785433563
Encrypted:	false
SSDEEP:	12:cGVvYf5KkkGHArBFUtpMkg/PMSI5Jf5KkkGHAryJ:n5Yf5KkkGgPgLwSJf5KkkGga
MD5:	BA36201345F117C700F0710139920267
SHA1:	B3113D5EA444CF91EBE470A9F19DF12B1A54209E
SHA-256:	D59FF9901B823FE6632F3A70AE46F87782053CAF1791AF8BF92C810DD1F8D562
SHA-512:	2FEB3F67F407E3D2F98128373FD069B82BC72C9BF33E2E20A9EC873553D719ECBD1BD6AB662DD5CA484B5551F0FF444AB5D24C6DEAB8001382A0815FA0CD773
Malicious:	false
Preview:	2021/03/05-10:04:50.901 1680 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/03/05-10:04:50.903 1680 Recovering log #3.2021/03/05-10:04:50.905 1680 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.161056729791467
Encrypted:	false
SSDEEP:	12:cz2IvYf5KkkGHArqiuFUtpMZX/PM95Jf5KkkGHArq2J:c26Yf5KkkGgCgtJf5KkkGg7
MD5:	519E0033976364AFF1C5C3C88CE21AA6
SHA1:	CF62714FDCFA157BA2603C02230391A9C378E0B3
SHA-256:	1767C3297F737954DD505C8DFAD284EEB80102A8404ADFF712FCFCF52ECFEE75
SHA-512:	122D2EDCC835943418D51007A8042A39A6FF79D3452E75C27D3834E27B261A7CC33BC98020765C09D0691BA793487AD93742B6C54E4F6E37BCF586C2FE46CFB
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Preview:	2021/03/05-10:04:50.904 1530 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/03/05-10:04:50.909 1530 Recovering log #3.2021/03/05-10:04:50.910 1530 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):	5.156694869823573
Encrypted:	false
SSDEEP:	12:cNfVvYf5KkkGHArAFUtpMNHwg/PMNtQSI5Jf5KkkGHArfJ:ef5Yf5KkkGgkgUQ3tjSJf5KkkGgV
MD5:	AC08F012B1DF3ECEF061848DF2509146
SHA1:	3A18BC4657BFDB625F0E360907BEFABD502437FA
SHA-256:	9EBEB83910C446AB5C665056F467A5662D0B7EE796BB79DD9E60CF781128CD89
SHA-512:	75A0D2D0F43A40927723C1D616B373736F3137091DD1EB997D2283FF602AC9712F1DC3EBB1E245CD2F931415FA7B2F397E845A6260D3FCB895887952DD50197A
Malicious:	false
Preview:	2021/03/05-10:05:06.167 1be0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/03/05-10:05:06.168 1be0 Recovering log #3.2021/03/05-10:05:06.169 1be0 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\bafaf7f6-9d61-48b4-b4ed-987c02904db1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.222577474356885
Encrypted:	false
SSDEEP:	6:mxfZRyq2Pwkn23iKKdKpIFUtpyfxH1ZmwPyfiUpRkwOwkn23iKKdKa/WLJ:cZRyvYf5KkmFUtpMxV/PMiER5Jf5KkaQ
MD5:	EF1AB780A48F75D56F9DCBA4647AE261
SHA1:	A13AB11A3BFA1C7AA0776F49A6856C420F2EA2BB
SHA-256:	3FA971481AC74BD83D5DC8F16BE751A064F3F294B9900E35504678EFD091D408
SHA-512:	6735EA08CB85CFB7EE5CB0B115CF9967DB56A786A4BAE2C0C856297A08219C5684266747D783367BF049CED3B5C88A1579B76B3BE4C97F4DACCA3B804846124 C
Malicious:	false
Preview:	2021/03/05-10:04:42.750 1be4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/03/05-10:04:42.758 1be4 Recovering log #3.2021/03/05-10:04:42.767 1be4 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):	5.282312398397875
Encrypted:	false
SSDEEP:	12:cKAvYf5KkkOrsFUtpMTh/PMw5Jf5KkkOrzJ:2Yf5Kk+gc1Jf5Kkn
MD5:	AAB8330EE1EA8391C5DC551FC0D57198
SHA1:	BF85618CCE4ED7D51906DEFE9792CAFF689A0EC0
SHA-256:	0AF72B177054E230B2A929FAC4C002437EA1861A547727B1229ECDF6081759F7
SHA-512:	E39E31907D822276470C8D97252EC99CBABAA42ED8D41568D13B62BB4DBAFB5BDC64D102EF3BAB6AC38557FFFA8496A0B2F3531A76C31B7E62019473FDDB84 F0
Malicious:	false
Preview:	2021/03/05-10:04:52.688 14e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/03/05-10:04:52.689 14e0 Recovering log #3.2021/03/05-10:04:52.691 14e0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.92251475799613
Encrypted:	false
SSDEEP:	3:kTGi9F1qzcGr7j4/T:aB9ODnGT
MD5:	070533F29B5C57A181183E7247EF24C5
SHA1:	A6539FD1BD31F9212788B55AB3CBDC481FC568EB
SHA-256:	414BB0653986358C98A3B7534005B15FF9DBFCAD80226AE1AFD636886C7A10BA
SHA-512:	A6062ECDE4643477FFEA4CE0EE51CEE09C5CFDAC7E6D545C436D5BA37D619AFDD6786F49856C3F656CC205DFFE3896BAC7D696DF8B21ABDB0F2DDCB1BAC 610B
Malicious:	false
Preview:	......W..t.....t..&.j.....Ls..&.....#s.....A.....g.G.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ce99f6bd-cb32-4af0-a8ec-d170a12abf57.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):	5418
Entropy (8bit):	5.153688559120413

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ce99f6bd-cb32-4af0-a8ec-d170a12abf57.tmp	
Encrypted:	false
SSDEEP:	48:YcKkMklilj5M+qALRqpgcBLb2t4lYGlQuoTw09kwrf4MqM8C1Nfct/9BhUJo3KhV:n8Lsk4pgcBHHIVH5k0JCKL8obOTlVuHn
MD5:	5649FC4958958F20ED64E2B603ADB7B7
SHA1:	EC98A2F4584D9738827940941E4271A91C6F7B66
SHA-256:	AC073E119AEF1600E293775BD5F2CFCE1F108562AEC5A4C10A1A545CF2D145FC
SHA-512:	59C6B4CAF25C7C2FA46D6A757AA4847E7E11ABC135D768C0950C3A58747739E0EA3824DC88A2E42FD8246D0C35FD0A8DB732F148C0980576A15484FC6A510A2
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13259408683001031","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.440989542794581
Encrypted:	false
SSDEEP:	3:tUK0fu7unRNAdTyZmwv3yfvRsA7V8syfvRsA7WGv:mxfu7uRNAgZmwPyfJsA7VvyfJsA7tv
MD5:	E02DC61179FCA1736168B70F251CBE49
SHA1:	61DA32AC78E6CAE85AC1CCA4EE75F1703112AF80
SHA-256:	ACDFBFFA7E1E00496556C9B7663D983212649ED0902B5C08D456E7EBEF7C21FB
SHA-512:	B5AF3508A58D80F0127C79DB9BA22851A63387D63AB3D6E7940A1988B8B820595C7EC86E06563B217DA934AEB7643E10072F1F919B1BAF6E32E156094816C833
Malicious:	false
Preview:	2021/03/05-10:04:50.048 1bb4 Recovering log #3.2021/03/05-10:04:50.127 1bb4 Delete type=0 #3.2021/03/05-10:04:50.127 1bb4 Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\db4313c4-f022-41f5-a06b-1111c40781a3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\db4313c4-f022-41f5-a06b-1111c40781a3.tmp	
Category:	dropped
Size (bytes):	1040
Entropy (8bit):	5.571807499746814
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeiXzkq/HeUe8zUej7wUR8RUeiQ:Ym6UUhyKUeiYqPeUekUefwUGUeP
MD5:	005E2B3C51E4B88B00AD0A42CCB595EF
SHA1:	469561C2865CE152AD35D71055D9BE827461EF66
SHA-256:	67D2E085CA80D4B7FE57FF32C9BE70800D6BA84884C5DB4F93A1F45A67EC2B8C
SHA-512:	75429FF2B667E927D4C18842DE93F840E21326BE781756C9C82FA89758045FF8704128FB0B688ADC7E0219D05478FF2FA821C5FC3AA9CA00CBD670F87CC5B8BE
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1646471087.704387,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614935087.70439},{"expiry":1632986995.164829,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e705fee9-51f7-4cd9-bfe4-4c10ed790ab4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e72e0f2c-6e97-4ca9-8d2a-3cc80341ca33.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):	1831
Entropy (8bit):	4.847175553241777
Encrypted:	false
SSDEEP:	48:Y2nzMK6qDHGXCtwWsh7RLshAyv5xOshb3zsh9MHuYhbw:JnzMKxDHGXCOTt+PaGDhM
MD5:	D9895CA6C1889523323C47D95AE3167A
SHA1:	39A939B510828F351EF5F0F8181D34C57AD7B4FB
SHA-256:	269EB994D1391648336E1DD890A21E4E619EF719AF090E3B0C02141553F247B8
SHA-512:	D8B98EDC58E93C143087A497E99474CBBB6E974625CBB88D829423DE9FA620C5B212AF28C98F23F5DDDB635C74487FFCD362C35161BB44E2ED9470302B39ABB4
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13262000687704329","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.182220891024624
Encrypted:	false
SSDEEP:	6:mxfmCYVq2Pwkn23iKKdKfrzAdIFUtpyfmQgZmwPyfmQIkwOwkn23iKKdKfrzILJ:cmCYVvYf5Kk9FUtpMmQg/PMmQI5Jf5KF
MD5:	98217CCC379E47047CC6E1A7B849C005
SHA1:	7A4ECFBC415DBDE0826D557C8C3ED3CA4900FBA6
SHA-256:	CE002D4F82C97F42C2F4C97726516A6C604D5D4DB04C1C50F12EBF11086B2E4D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
SHA-512:	0EADD9E76C988EBA6289DB9518EF4020E99CB8C4C1C7D73FC325E7C63D0BCB9A84CDC7346DF50303722544271F0F7E7BDBF191E38C5DB7D603036C5926D3CB1
Malicious:	false
Preview:	2021/03/05-10:04:50.839 1620 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/03/05-10:04:50.841 1620 Recovering log #3.2021/03/05-10:04:50.841 1620 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\a5f934dd-7288-499b-9f00-1274a2264f98.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):	156978
Entropy (8bit):	6.052357784479004
Encrypted:	false
SSDEEP:	3072:r2VQRlj6UuIX5KN7iW2inex9Oe4jFcbXafIB0u1GOJmA3iuRy:r0QvjfKkW2Xx9OewaqfIlUOoSiuRy
MD5:	D9FABFC07C9BDC7F69E119816AC88F0E
SHA1:	57A4E142FA7C3A6432A64CAB448A5C68DB8853C9
SHA-256:	952DD8EADABD96194F532393B7639130A4E2AA31108DC637DE6004348388ADCE
SHA-512:	27D05BD1CA6FF6FDAD962E40817B86E809D0BE227661471B523709FCDD549D6AC98DF99A69AABE71F2CFC36A550AE4327510D7188421F227DA086CC24F3D5B
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":1.614935085943618e+12,"network":1.614935087e+12,"ticks":305376941.0,"uncertainty":4782826.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBljSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":

C:\Users\user\AppData\Local\Google\Chrome\User Data\d8f70adb-a47f-4c79-b62b-33a4f5e7f79b.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):	156978

C:\Users\user\AppData\Local\Google\Chrome\User Data\d8f70adb-a47f-4c79-b62b-33a4f5e7f79b.tmp	
Entropy (8bit):	6.052357784479004
Encrypted:	false
SSDEEP:	3072:r2VQRlj6UuIX5KN7iW2inex9Oe4jFcbXafIB0u1GOJmA3iuRy:r0QvjfKkW2Xx9OewaqfIlUOoSiuRy
MD5:	D9FABFC07C9BDC7F69E119816AC88F0E
SHA1:	57A4E142FA7C3A6432A64CAB448A5C68DB8853C9
SHA-256:	952DD8EADABD96194F532393B7639130A4E2AA31108DC637DE6004348388ADCE
SHA-512:	27D05BD1CA6FF6FDAD962E40817B86E809D0BE227661471B523709FCDD549D6AC98DF99A69AABE71F2CFC36A550AE4327510D7188421F227DA086CC24F3D5B
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":1.614935085943618e+12,"network":1.614935087e+12,"ticks":305376941.0,"uncertainty":4782826.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":

C:\Users\user\AppData\Local\Temp\4513a782-0670-4335-9c87-3123cd40f752.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\4ac57fed-731f-44c4-a9f5-6e21e97931c8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\51fcfd65-e9fb-46a5-93cd-719e7ccb4fd6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
Malicious:	false

C:\Users\user\AppData\Local\Temp\51fcfd65-e9fb-46a5-93cd-719e7ccb4fd6.tmp	
Preview:	Cr24.....0..''0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..I.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\6960_1256072906\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9669759926795995
Encrypted:	false
SSDEEP:	3:SfvHUTa8URTTH/BXDj6:SXD3TfB36
MD5:	E3EDA33A5C956F4FC9C5BBD91FF10252
SHA1:	182B989E299A3EC306622A9DD45C3B74A4DF6077
SHA-256:	6D7A462B703F1617286B65BFE0116F267328BEFC379812BCE774D8C640289647
SHA-512:	A49FF4979FEC3512C44899840CCF8D112806330C93812C515F09953B9B6DBA6B1DAB1828382D634235CF23E093C983AEFA860B7A75FDCB5F3F98DD928D4F47D
Malicious:	false
Preview:	1.d730fdd6875bfda19ae43c639e89fe6c24e48b53ec4f466b1d7de2001f97e03c

C:\Users\user\AppData\Local\Temp\6960_1327120964\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	66
Entropy (8bit):	3.866533712632772
Encrypted:	false
SSDEEP:	3:SpUCQEd2dq8ebEJW2GnnHR:SXQ5Y88EJeR
MD5:	423CB83A2A3B602B0AA82B51B3DA2869
SHA1:	58BC924AF90A89CE87807919F228FE6C915AD854
SHA-256:	0047059C732D70AF8C2F407089237F745838A0FE4F75710ABF1E669B81243E9C
SHA-512:	F80E9B5D544894A667F74CFD0A4D784311299DB080CA6793AABD93B95CF1E2870F74AD38A6386D862580220047F828457240577335C565B7F38B0C6677811660
Malicious:	false
Preview:	1.ffd1d2d75a8183b0a1081bd03a7ce1d140fded7a9fb52cf3ae864cd4d408ceb4

C:\Users\user\AppData\Local\Temp\6960_1590743133\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.8184870675314144
Encrypted:	false
SSDEEP:	3:SSgdRQtXPjnQVLX4I2LNyzXdn:SSgdRQxPjnQ14tAzXd
MD5:	DE50A5B093F2233B688C710F12E2816D
SHA1:	2E0EDDCCB2E6144A5E640AD9ED92B4D27A88B9C9
SHA-256:	505E9F362B6BDCCF6AA007C4F5228D999B6CFB553980BAE38CF3204D6DF872AA
SHA-512:	B455D4C22B21D779544816F1B505C6AC701A159BECBC84AD535F60EC8CDA0CE1FDEB16B1E41407C47D456F161EF8D01288E40F15FA778CD4B820BC286F95B7A
Malicious:	false
Preview:	1.7d315645c6a7a98c8c88c51eaaa64575081d492ae50f58e686b8119864023087

C:\Users\user\AppData\Local\Temp\6960_2102678167\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363

C:\Users\user\AppData\Local\Temp\6960_2102678167\manifest.fingerprint	
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\c70014d7-3d49-48ea-954f-6b86d5c18738.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\4513a782-0670-4335-9c87-3123cd40f752.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Preview:	{.. "10189845614885205 17": {.. "message": "....."..},.. "12139579827238759 20": {.. "message": "..... ... .?"..},.. "12827687646031907 5": {.. "message": "..... ..."..},.. "14284488690781267 31": {.. "message": ".... ....."..},.. "15221406833188603 51": {.. "message": "..... ...."..},.. "15509040647108289 58": {.. "message": "...."..},.. "16366867476874943 76": {.. "message": "... ..."..},.. "18027627465894571 77": {.. "message": "..."..},.. "18503975003120203 88": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\ar\messages.json	
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0IprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "155090406471082895 8": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:lPswlWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ... .".. },.. "155090406471082895 8": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "18027627 46589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\ca\messages.json	
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7ADB
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "1522140683318860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\de\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djIV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "......... ....".. },.. "1428448869078126731": {.. "message": "......... .....".. },.. "1522140683318860351": {.. "message": "........ ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "........ .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146CI
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71E EEE
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas describe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB1120272356
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "152140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\fa\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF371
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "1282768764603190 75": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A5261952050
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "1522140683318860351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromecastisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\fil\messages.json	
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C8202343738 91BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C00
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "128276876460319075": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-smooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51B
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Se fige".. },.. "1213957982723875920": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "1428448869078126731": {.. "message": "Fluidit. de la vid.o".. },.. "1522140683318860351": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "1550904064710828958": {.. "message": "Fluide".. },.. "1636747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Votre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\gu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\hi\messages.json	
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "....."‥ },.. "1213957982723875920": {.. "message": "..... ... .?"‥ },.. "128276 876460319075": {.. "message": "..... ..."‥ },.. "1428448869078126731": {.. "message": "..... ....."‥ },.. "1522140683318860351": {.. "message": "..... ...."‥ },.. "1550904064710828958": {.. "message": "....."‥ },.. "1636686747687494376": {.. "message": "....."‥ },.. "1802762746589457177": {.. "message": "....."‥ },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15507
Entropy (8bit):	5.290847699527565
Encrypted:	false
SSDEEP:	192:Pdapr6h85tRwVQgkvJryLkla5Kfndg/V6c8TEKdl:Arwot2Q7BryVce/V6uml
MD5:	3ED90E66789927D80B42346BB431431E
SHA1:	2B061E3271DF4255B1FFC47BDB207CDEC0D9724F
SHA-256:	0B41E3C42414F72C9A12C05F8772597F9685115366A774C66018467AD4B71A74
SHA-512:	92BE43F1FFC8EFBF5BBC50573AC4C65F6104416A5B6CD04404C3A9854CA3DCF2A43A4044C168590CDF83887D2344958435723 31ADCD5B020D2E48A3956F3C16
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Zamrzavanje"‥ },.. "1213957982723875920": {.. "message": "Koje od sljede.eg najbolje opisuje va.u mre.u?"‥ },.. "128276876460319075": {.. "message": "Otkrivanje ure.aja"‥ },.. "1428448869078126731": {.. "message": "Ujedna.enost videoreprodukcije"‥ },.. "1 522140683318860351": {.. "message": "Povezivanje nije uspjelo. Poku.ajte ponovo."‥ },.. "1550904064710828958": {.. "message": "Glatko"‥ },.. "16366867 47687494376": {.. "message": "Savr.ena"‥ },.. "1802762746589457177": {.. "message": "Glasno.a"‥ },.. "1850397500312020388": {.. "message": "Vidite li svoj Chromecast u $START_LINK$aplikaciji Google HomeEND_LINK? $START_SPAN$*END_SPAN",‥ "placeholders": {.. "END_LINK": {.. "co ntent": "$1"‥ },.. "END_SPAN": {.. "content": "$2"‥ },.. "START_LINK": {.. "content": "$3"‥

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15682
Entropy (8bit):	5.354505633120392
Encrypted:	false
SSDEEP:	192:CCEAproS9fZv+JwkDMrC2NSxoSgbV6c8TEKdl:5r5VZv+RDMrazoV6uml
MD5:	8E9FF7E49473C5734A2F6F0812E12EB3
SHA1:	A4F10DDD1580582533D5EB59EDF6D8048F887C81
SHA-256:	6CDD2FB39ADECE00E88B989E464B05ED1414092D0492F6D0AE58D549BFD1A46A
SHA-512:	E9A4AF31B1A276F395599BB620A3164CABF3459F3C102DD3F57DFEA734510BD985DE65CB409E1975559ACCC615075439A08E1DEBE22C90A0ABCAA3CAFEE79A C7
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Lefagy"‥ },.. "1213957982723875920": {.. "message": "Az al.bbiak k.z.l melyik jellemzi legjobban h.l.zat.t?"‥ },.. "128276876460319075": {.. "message": "Eszk.zfelfedez.s"‥ },.. "1428448869078126731": {.. "message": "Vide. folyamatoss.ga"‥ },.. "1522140683318860351" : {.. "message": "Sikertelen kapcsol.d.s. K.rj.k, pr.b.lja .jra."‥ },.. "1550904064710828958": {.. "message": "Folyamatos"‥ },.. "1636686747687494376": {.. "message": "T.k.letes"‥ },.. "1802762746589457177": {.. "message": "Hanger."‥ },.. "1850397500312020388": {.. "message": "L.tja a Chromecastot a $STA RT_LINK$Google Home alkalmaz.sbanEND_LINK? $START_SPAN$*END_SPAN",‥ "placeholders": {.. "END_LINK": {.. "content": "$1"‥ },.. "END_SPAN": {.. "content": "$2"‥ },.. "START_LINK": {.. "content":

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15070
Entropy (8bit):	5.190057470347349
Encrypted:	false
SSDEEP:	192:GsprMtChjkWfrEWL0KRCnEOWV6c8TEKdl:9rtAEr3LTRuWV6uml
MD5:	7ADF9F2048944821F93879336EB61A78
SHA1:	C3DA74FB544684D5B250767BB0CB66FFB7C58963
SHA-256:	3630947E1075E3663AD3E4824D0BE42CB47C0D615D8053E83B9595047C8BA9BE
SHA-512:	1F28BB80E1839C5581106BEA3AE2501C7618249D7E3115819F5A9A87771D59F5DE346C1B9C87F7FFC390604D5B9888CE738E25F2F04A094002A0FB3B22CBEC95
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Membeku"‥ },.. "1213957982723875920": {.. "message": "Dari berikut ini, manakah yang paling mendeskripsikan jaringan Anda?"‥ },.. "128276876460319075": {.. "message": "Penemuan Perangkat"‥ },.. "1428448869078126731": {.. "message": "Kelancaran Video"‥ },.. "1522140683318860351": {.. "message": "Sambungan gagal. Coba lagi."‥ },.. "1550904064710828958": {.. "message": "Lancar"‥ },.. "1636686747687494376" : {.. "message": "Sempurna"‥ },.. "1802762746589457177": {.. "message": "Volume"‥ },.. "1850397500312020388": {.. "message": "Bisakah Anda melihat Chromecast di $START_LINK$aplikasi Google HomeEND_LINK? $START_SPAN$*END_SPAN",‥ "placeholders": {.. "END_LINK": {.. "content": " $1"‥ },.. "END_SPAN": {.. "content": "$2"‥ },.. "START_LINK": {.. "content": "$3"‥ },..

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15256
Entropy (8bit):	5.210663765771143
Encrypted:	false
SSDEEP:	192:lYprk52dAaykVza8rE0QWBKD9+vq0hKEV6c8TEKdl:qrlA8r6DalV6uml
MD5:	BB3041A2B485B900F623E57459AE698A
SHA1:	502F5EA89F9FB0287E864B240EA39889D72053A4
SHA-256:	025737EF8FA06706B3F26D0F52B4844244A6D33DAE1D82FEF2931A14C003D57E
SHA-512:	BA51784073BEF82F3A116B33DA406FDB10EC823B9EE74375C46036DAD8BDCB4141F60845DE141ABE42CEEF9251572F6AB287CA5FC7669C60E4F68071D5AB8C D
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Si blocca".. },.. "1213957982723875920": {.. "message": "Quale delle seguenti definizioni descrive meglio la tua rete?".. },.. "128276876460319075": {.. "message": "Rilevamento dispositivi".. },.. "1428448869078126731": {.. "message": "Uniformit. video".. },.. "1522140683318860351": {.. "message": "Connessione non riuscita. Riprova.".. },.. "1550904064710828958": {.. "message": "Fluido".. },.. "1636686747687494376": {.. "message": "Perfetta".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Riesci a vedere il tuo dispositivo Chromecast nell'$START_LINK$app Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6960_1292274319\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16519
Entropy (8bit):	5.675556017051063
Encrypted:	false
SSDEEP:	192:nkprPhQdxkRWrZe1wYpMR5wnAV6c8TEKdl:YrLRWri65wAV6uml
MD5:	6F2CC1A6B258DF45F519BA24149FABDC
SHA1:	8A58C7880C6D22765DCBB6BCE22A192C1B109AE1
SHA-256:	42ECFEE727CFC4F2845FEFDACE5EDC2E0A40AFAD69973A3B950CE653A7633342
SHA-512:	F7454F0E14301C59CC54361ACC0A1C6D072EF9BDF5DEA60646FB90B1CE47612785938C784A4CF1DE3E62648A14420374933B5F5DA43907BC00D3799FF163A3D
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "...".. },.. "1213957982723875920": {.. "message": "...".. },.. "128276876460319075": {.. "message": "...".. },.. "1428448869078126731": {.. "message": "...".. },.. "1522140683318860351": {.. "message": "...".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": "$START_LINK$Google Home ...END_LINK. Chromecast .....$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".

Static File Info

General

File type:	HTML document, ASCII text, with no line terminators
Entropy (8bit):	4.674634473245847
TrID:	• HyperText Markup Language (31031/1) 100.00%
File name:	equinitiTicket#51347303511505986.htm
File size:	120
MD5:	07a72696ec306e32bd82c97adecb0a00
SHA1:	56ce4d5adf0e27e63c4a2a4d4e6f3e0340bf23a7
SHA256:	ff12c57b1e82a05c56405df0f9a31f57057d2dca3522b5a5 aaf7915eccfe0c68
SHA512:	57838c350f43dd01ba1ca2892800e92dbdd3e50c9746cfd 876a6cc27f14e8c0c085afb456bddf99dee288f3309bdb0 edc0fc1c7f2a3db6f555c6960f6ddd68b5
SSDEEP:	3:gnkAqRAdu6/GY7voOkADYnKn4HELPIhOLcXUQM4 c7b:7AqJm7+mYnK4HExcXUQM4Yb
File Content Preview:	<script type="text/javascript">window.location.href="https://foodtecafrica.com/common?zak.newman@equiniti.com";</script>

Network Behavior

Network Port Distribution

Total Packets: 103

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 10:04:47.575459957 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.576133966 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.627089024 CET	49736	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.747462034 CET	443	49734	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.747643948 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.747957945 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.748037100 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.748130083 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.748378038 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.791640043 CET	443	49736	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.791822910 CET	49736	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.797103882 CET	49736	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.910434961 CET	443	49734	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.910461903 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.913502932 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.913536072 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.913564920 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.913674116 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.914547920 CET	443	49734	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.914597034 CET	443	49734	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.914628983 CET	443	49734	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.914783001 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.944610119 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.945292950 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.945343018 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.945441008 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.945625067 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.959170103 CET	443	49736	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.961091995 CET	443	49736	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.961122036 CET	443	49736	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.961147070 CET	443	49736	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:47.961185932 CET	49736	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:47.962326050 CET	49736	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.118077040 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.118092060 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.118099928 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.118172884 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.118442059 CET	443	49734	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.118458033 CET	443	49734	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.118465900 CET	443	49734	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.118473053 CET	443	49734	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.118484020 CET	443	49734	207.174.215.254	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 10:04:48.118499041 CET	443	49734	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.118531942 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.118566036 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.118573904 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.118580103 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.118585110 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.118590117 CET	49734	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.118686914 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.129112005 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.129137993 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.140418053 CET	443	49736	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.140448093 CET	443	49736	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.140486002 CET	443	49736	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.140517950 CET	49736	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.168715954 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.179704905 CET	49736	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.320780039 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.427192926 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.435003996 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.597410917 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.917702913 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:48.958942890 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:48.963928938 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:49.135937929 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:49.144040108 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:49.154997110 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:49.368855953 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:49.736387968 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:49.736427069 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:49.736449003 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:49.736469030 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:49.736481905 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:49.736493111 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:49.736507893 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:49.736514091 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:49.736573935 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:49.741028070 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:49.903076887 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:50.326324940 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:50.326361895 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:50.326384068 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:50.326405048 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:50.326428890 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:50.326446056 CET	443	49735	207.174.215.254	192.168.2.4
Mar 5, 2021 10:04:50.326499939 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:50.326548100 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:50.373820066 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:50.374300957 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:50.374666929 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:50.375019073 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:50.375488043 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:50.378957987 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:50.378978968 CET	49735	443	192.168.2.4	207.174.215.254
Mar 5, 2021 10:04:50.378979921 CET	49742	443	192.168.2.4	172.217.23.33
Mar 5, 2021 10:04:50.421205044 CET	443	49742	172.217.23.33	192.168.2.4
Mar 5, 2021 10:04:50.421360016 CET	49742	443	192.168.2.4	172.217.23.33
Mar 5, 2021 10:04:50.421587944 CET	49742	443	192.168.2.4	172.217.23.33
Mar 5, 2021 10:04:50.463625908 CET	443	49742	172.217.23.33	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 10:04:33.835834026 CET	54531	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:33.885459900 CET	53	54531	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 10:04:35.163121939 CET	49714	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:35.209239006 CET	53	49714	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:36.075161934 CET	58028	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:36.121195078 CET	53	58028	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:37.533006907 CET	53097	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:37.579123020 CET	53	53097	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:38.845556021 CET	49257	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:38.891413927 CET	53	49257	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:40.662105083 CET	62389	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:40.712528944 CET	53	62389	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:41.893055916 CET	49910	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:41.942950010 CET	53	49910	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:47.372301102 CET	51726	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:47.388333082 CET	56794	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:47.389909983 CET	56534	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:47.390358925 CET	56627	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:47.436072111 CET	53	51726	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:47.453483105 CET	53	56627	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:47.453610897 CET	53	56534	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:47.568147898 CET	53	56794	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:47.863605976 CET	56621	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:47.917911053 CET	53	56621	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:48.048057079 CET	63116	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:48.116677999 CET	53	63116	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:50.295495987 CET	51255	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:50.360754013 CET	53	51255	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:52.288100958 CET	61522	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:52.334594011 CET	53	61522	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:53.557212114 CET	52337	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:53.752566099 CET	53	52337	8.8.8.8	192.168.2.4
Mar 5, 2021 10:04:59.601769924 CET	50601	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:04:59.651964903 CET	53	50601	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:00.989644051 CET	53157	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:01.038420916 CET	53	53157	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:01.815690041 CET	60875	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:01.863709927 CET	53	60875	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:04.282404900 CET	56448	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:04.329617023 CET	53	56448	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:05.381145000 CET	59172	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:05.427206039 CET	53	59172	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:06.326328993 CET	62420	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:06.376398087 CET	53	62420	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:07.582745075 CET	60579	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:07.630038023 CET	53	60579	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:08.565567017 CET	50183	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:08.615163088 CET	53	50183	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:08.812133074 CET	61531	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:08.863439083 CET	53	61531	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:09.743740082 CET	49228	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:09.789658070 CET	53	49228	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:11.551647902 CET	59794	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:11.597768068 CET	53	59794	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:12.470850945 CET	55916	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:12.516592026 CET	53	55916	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:16.343097925 CET	52752	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:16.392216921 CET	53	52752	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:27.895245075 CET	60542	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:27.984052896 CET	53	60542	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:28.616050959 CET	60689	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:28.708343029 CET	53	60689	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:29.142839909 CET	64206	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:29.197127104 CET	53	64206	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:29.637300014 CET	50904	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:29.729091883 CET	53	50904	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 10:05:29.802232027 CET	57525	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:29.863831997 CET	53	57525	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:30.280249119 CET	53814	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:30.370214939 CET	53	53814	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:31.027757883 CET	53418	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:31.090688944 CET	53	53418	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:31.759109020 CET	62833	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:31.811006069 CET	53	62833	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:32.956269979 CET	59260	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:33.015208960 CET	53	59260	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:33.807398081 CET	49944	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:33.853156090 CET	53	49944	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:34.268217087 CET	63300	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:34.359623909 CET	53	63300	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:37.102011919 CET	61449	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:37.148143053 CET	53	61449	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:43.133182049 CET	51275	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:43.187552929 CET	53	51275	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:44.227173090 CET	58945	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:44.274354935 CET	53	58945	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:47.281740904 CET	60779	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:47.332772970 CET	53	60779	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:47.471338034 CET	64014	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:47.517467976 CET	53	64014	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:47.645232916 CET	57091	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:47.701663017 CET	53	57091	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:48.766330957 CET	55904	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:48.815517902 CET	53	55904	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:59.499402046 CET	52109	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:59.550532103 CET	53	52109	8.8.8.8	192.168.2.4
Mar 5, 2021 10:05:59.696835995 CET	54450	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:05:59.754672050 CET	53	54450	8.8.8.8	192.168.2.4
Mar 5, 2021 10:06:15.804142952 CET	49374	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:06:15.850083113 CET	53	49374	8.8.8.8	192.168.2.4
Mar 5, 2021 10:06:15.976152897 CET	50436	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:06:16.022489071 CET	53	50436	8.8.8.8	192.168.2.4
Mar 5, 2021 10:06:18.008177042 CET	62605	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:06:18.055953979 CET	53	62605	8.8.8.8	192.168.2.4
Mar 5, 2021 10:06:20.523441076 CET	54256	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:06:20.594660044 CET	53	54256	8.8.8.8	192.168.2.4
Mar 5, 2021 10:06:57.377254009 CET	52189	53	192.168.2.4	8.8.8.8
Mar 5, 2021 10:06:57.439659119 CET	53	52189	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 10:04:47.388333082 CET	192.168.2.4	8.8.8.8	0x4bd3	Standard query (0)	foodtecafrica.com	A (IP address)	IN (0x0001)
Mar 5, 2021 10:04:50.295495987 CET	192.168.2.4	8.8.8.8	0x7d54	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)
Mar 5, 2021 10:04:53.557212114 CET	192.168.2.4	8.8.8.8	0x1efa	Standard query (0)	foodtecafrica.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 10:04:47.568147898 CET	8.8.8.8	192.168.2.4	0x4bd3	No error (0)	foodtecafrica.com		207.174.215.254	A (IP address)	IN (0x0001)
Mar 5, 2021 10:04:50.360754013 CET	8.8.8.8	192.168.2.4	0x7d54	No error (0)	clients2.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 10:04:50.360754013 CET	8.8.8.8	192.168.2.4	0x7d54	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.33	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 10:04:53.752566099 CET	8.8.8.8	192.168.2.4	0x1efa	No error (0)	foodtecafrica.com		207.174.215.254	A (IP address)	IN (0x0001)

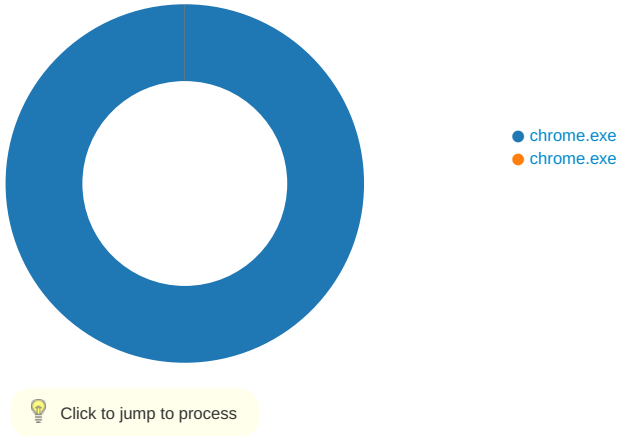
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 10:04:54.228199005 CET	207.174.215.254	443	192.168.2.4	49755	CN=cpcontacts.foodtecafrica.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Feb 22 15:12:28 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun May 23 16:12:28 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 10:04:54.305960894 CET	207.174.215.254	443	192.168.2.4	49756	CN=cpcontacts.foodtecafrica.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Feb 22 15:12:28 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun May 23 16:12:28 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6960 Parent PID: 1072

General

Start time:	10:04:41
Start date:	05/03/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'C:\Users\user\Desktop\equinitiTicket#51347303511505986.htm'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

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

Analysis Process: chrome.exe PID: 5684 Parent PID: 6960

General

Start time:	10:04:43
Start date:	05/03/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,15388751358428902676,16190953219467586011,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1800 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly