ID: 452149
Sample Name: Convert HEX uit phishing mail.htm
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 21:58:32
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

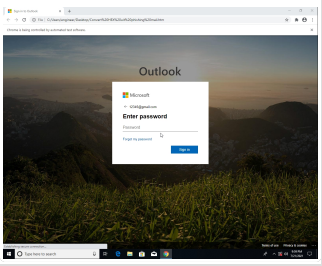
Windows Analysis Report Convert HEX uit phishing mai…

Overview

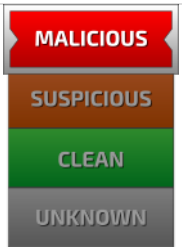
General Information

Sample Name:	Convert HEX uit phishing mail.htm
Analysis ID:	452149
MD5:	bdcd079a5d19d6..
SHA1:	2564b052fc982da.
SHA256:	0a3ad129462284..
Infos:	

Most interesting Screenshot:



Detection



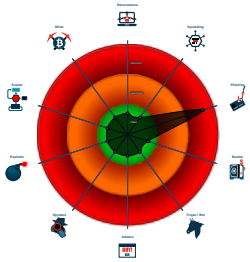
HTMLPhisher

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

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- Invalid 'forgot password' link found
- Invalid T&C link found
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3520 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\Convert HEX uit phishing mail.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6036 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1632,14357687303338385437,9119543046795049864,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Convert HEX uit phishing mail.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

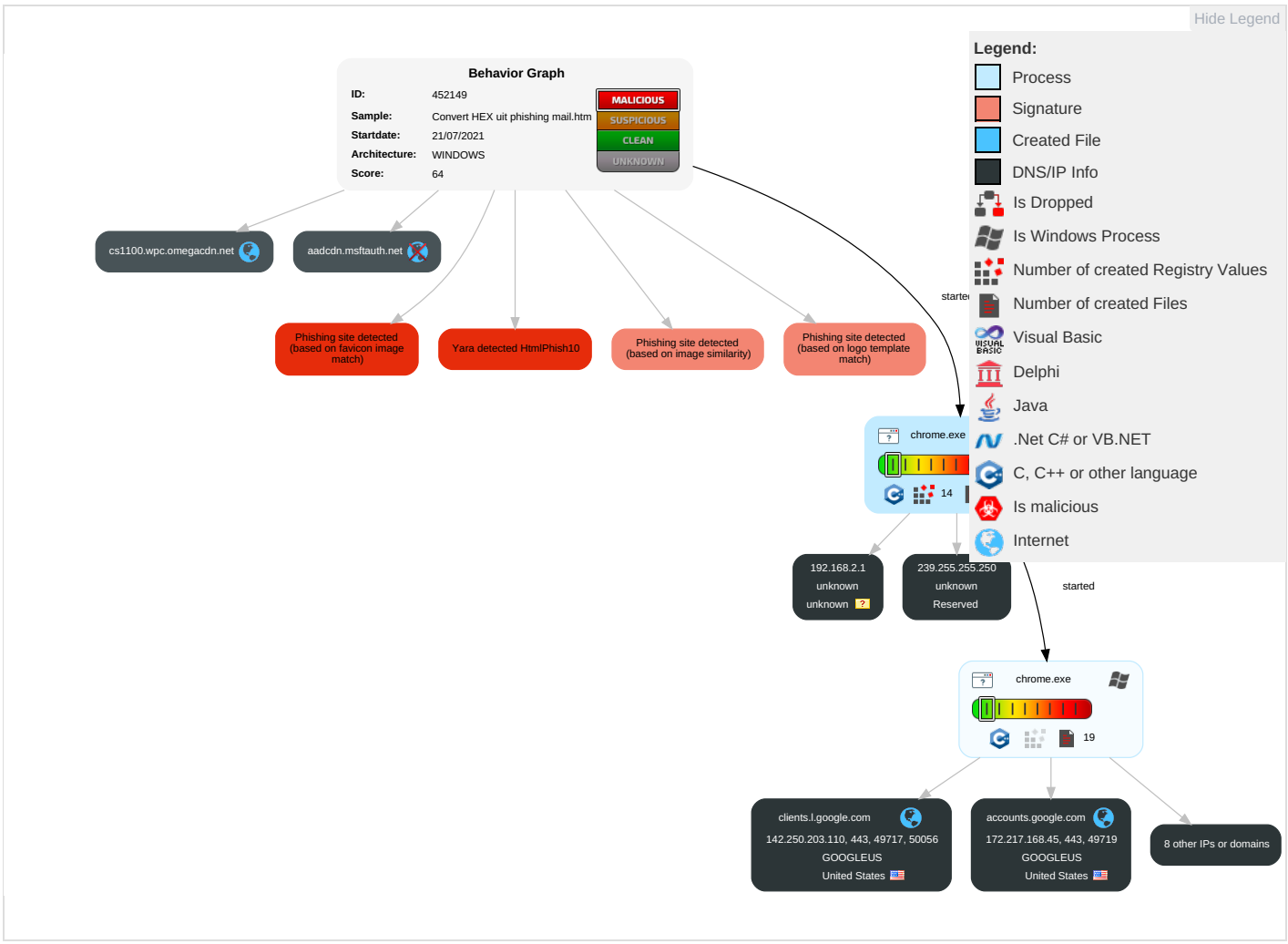
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

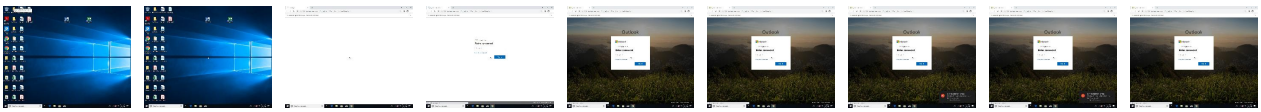
Behavior Graph

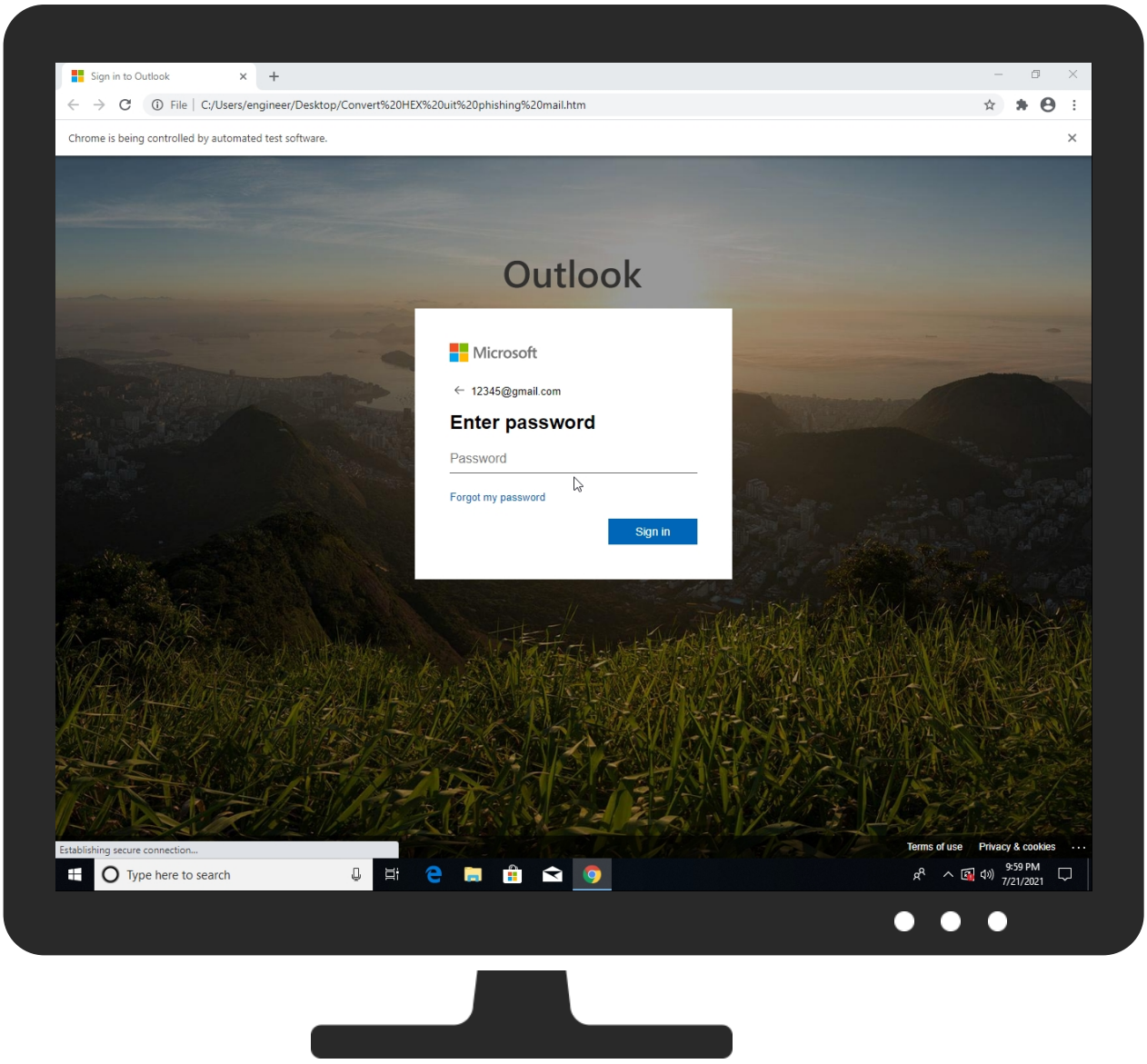


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
ipv4.imgur.map.fastly.net	0%	Virustotal		Browse
aadcdn.msftauth.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png	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://dns.google	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b588ad73.	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net	0%	URL Reputation	safe	
http://https://divisaoeletrica.com.br/sn/fresd.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	172.217.168.45	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.65	true	false		high
ipv4.imgur.map.fastly.net	151.101.12.193	true	false	• 0%, Virustotal, Browse	unknown
clients2.googleusercontent.com	unknown	unknown	false		high
i.stack.imgur.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/Convert%20HEX%20uit%20phishing%20mail.htm	true		low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.12.193	ipv4.imgur.map.fastly.net	United States		54113	FASTLYUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.65	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452149
Start date:	21.07.2021
Start time:	21:58:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Convert HEX uit phishing mail.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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.winHTM@36/178@6/8
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm
Warnings:	Show All

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	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	
	Unisys.com_Fax-Message.htm	Get hash	malicious	Browse	
	192-3216-Us.gt.com.html	Get hash	malicious	Browse	
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	
	banload.msi	Get hash	malicious	Browse	
	Enclosed Business Proposals From 4 Square Services.html	Get hash	malicious	Browse	
	Invoice-Message-500.htm	Get hash	malicious	Browse	
	IPVrDRKfYj.exe	Get hash	malicious	Browse	
	_VM_1064855583.HtM	Get hash	malicious	Browse	
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	
	Pbogart.htm	Get hash	malicious	Browse	
	ATT93916.HTM	Get hash	malicious	Browse	
	Pbeesley-PAID-ACH-SJOJFB-30488393-Comtact.htm	Get hash	malicious	Browse	
	Cx9ER7vYGi.exe	Get hash	malicious	Browse	
	Emilemercier ProtectedCall.htm	Get hash	malicious	Browse	
	INV #95000987.html	Get hash	malicious	Browse	
	Joelle#310712.html.txt.html	Get hash	malicious	Browse	
	ATT07509.HTM	Get hash	malicious	Browse	
	Pointids.ca_Fax-Message.htm	Get hash	malicious	Browse	
	ATT74992.HTM	Get hash	malicious	Browse	
151.101.12.193	VenusLocker_exe.exe	Get hash	malicious	Browse	• i.imgur.com/rSFPH6m.jpg
	VenusLocker_exe.exe	Get hash	malicious	Browse	• i.imgur.com/rSFPH6m.jpg
	http://tftpd32.jounin.net/tftpd32_download.html	Get hash	malicious	Browse	• i.imgur.com/RcdmOWL.png
	http://https://sway.office.com/g4Q55GF1SHkKtpyO?ref=Link	Get hash	malicious	Browse	• i.imgur.com/removed.png
	ACH-4843-93c5-cd20973689-9113.pdf	Get hash	malicious	Browse	• i.imgur.com/EzHd2p1.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ipv4.imgur.map.fastly.net	INV #95000987.html	Get hash	malicious	Browse	• 151.101.112.193
	VUBuRErqKh.dll	Get hash	malicious	Browse	• 151.101.112.193
	XFfw6uDKna.exe	Get hash	malicious	Browse	• 151.101.112.193
	HUCGOYy2oO.exe	Get hash	malicious	Browse	• 151.101.112.193
	qET1iJuly 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 151.101.12.193
	July 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 151.101.12.193
	#Ud83d#Udd0ajs_msg_ 3pm.html	Get hash	malicious	Browse	• 151.101.112.193
	Kay Supply, Inc. REQ 009046.html	Get hash	malicious	Browse	• 151.101.112.193
	Deepspacesystems Signed Waiver .html	Get hash	malicious	Browse	• 151.101.112.193
	deepspacesystems_fxdocstub-jwuKfDGIIoVteWuSsmBhNalGOOjkUsDfVISBHLFvYbMhqYpqCi.HTM	Get hash	malicious	Browse	• 151.101.12.193
	INV_289553.html	Get hash	malicious	Browse	• 151.101.112.193
	#Ud83d#Udd0aMsg_ 3pm.html	Get hash	malicious	Browse	• 151.101.112.193
	aAKihPRSNV.exe	Get hash	malicious	Browse	• 151.101.112.193
	RevisedSpreadsheet.xlsx	Get hash	malicious	Browse	• 151.101.12.193

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RevisedSpreadsheet.xlsx	Get hash	malicious	Browse	• 151.101.112.193
	Invoice-Message-7784002.html	Get hash	malicious	Browse	• 151.101.112.193
	Invoice-Message-4821881.html	Get hash	malicious	Browse	• 151.101.12.193
	Payslip070620219359636Z.html	Get hash	malicious	Browse	• 151.101.112.193
	VM52MC9YQDUO0P.html	Get hash	malicious	Browse	• 151.101.112.193
	PO # 2367.html	Get hash	malicious	Browse	• 151.101.112.193
cs1100.wpc.omegacdn.net	192-3216-Us.gt.com.html	Get hash	malicious	Browse	• 152.199.23.37
	voice mail.html	Get hash	malicious	Browse	• 152.199.23.37
	New Working C0D377B99993939393939939.htm	Get hash	malicious	Browse	• 152.199.23.37
	20210714_110346.html	Get hash	malicious	Browse	• 152.199.23.37
	qET1iJuly 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 152.199.23.37
	July 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 152.199.23.37
	It.servicedesk_FAXit.servicedesk@ovolohotels.com.html	Get hash	malicious	Browse	• 152.199.23.37
	Globalfoundries#Scanned-thomas.caulfield.html	Get hash	malicious	Browse	• 152.199.23.37
	Deepspacesystems Signed Waiver .html	Get hash	malicious	Browse	• 152.199.23.37
	deepspacesystems_fxdocstub-jwuKfDGIIoVteWuSsmBhNalGOOjkUsDfVlSBHLFvYbMhqYpqCi.HTM	Get hash	malicious	Browse	• 152.199.23.37
	It.servicedesk.html	Get hash	malicious	Browse	• 152.199.23.37
	20210714_110346.html	Get hash	malicious	Browse	• 152.199.23.37
	HSBC_Payment_slip_for Outstanding 001005l.htm	Get hash	malicious	Browse	• 152.199.23.37
	dez.htm	Get hash	malicious	Browse	• 152.199.23.37
	Voice0033pm.htm	Get hash	malicious	Browse	• 152.199.23.37
	AhyARattach.html	Get hash	malicious	Browse	• 152.199.23.37
	attach.html	Get hash	malicious	Browse	• 152.199.23.37
	Cmh_Fax-Message-3865.html	Get hash	malicious	Browse	• 152.199.23.37
	attach.html	Get hash	malicious	Browse	• 152.199.23.37
	Ovolohotels-BAD-LINK.html	Get hash	malicious	Browse	• 152.199.23.37

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EDGECASTUS	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.21.175
	192-3216-Us.gt.com.html	Get hash	malicious	Browse	• 152.199.23.37
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.21.175
	banload.msi	Get hash	malicious	Browse	• 152.199.21.175
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.21.175
	voice mail.html	Get hash	malicious	Browse	• 152.199.23.37
	New Working C0D377B99993939393939939.htm	Get hash	malicious	Browse	• 152.199.23.37
	qET1iJuly 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 152.199.23.37
	July 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 152.199.23.37
	RemitSwiftxlsx.htm	Get hash	malicious	Browse	• 192.229.221.185
	It.servicedesk_FAXit.servicedesk@ovolohotels.com.html	Get hash	malicious	Browse	• 152.199.23.37
	Globalfoundries.htm	Get hash	malicious	Browse	• 152.199.21.175
	Globalfoundries#Scanned-thomas.caulfield.html	Get hash	malicious	Browse	• 152.199.23.37
	Deepspacesystems Signed Waiver .html	Get hash	malicious	Browse	• 152.199.23.37
	deepspacesystems_fxdocstub-jwuKfDGIIoVteWuSsmBhNalGOOjkUsDfVlSBHLFvYbMhqYpqCi.HTM	Get hash	malicious	Browse	• 152.199.23.37
	INV_289553.html	Get hash	malicious	Browse	• 152.199.21.175
	It.servicedesk.html	Get hash	malicious	Browse	• 152.199.23.37
	gsskema.html	Get hash	malicious	Browse	• 152.199.21.175
	HSBC_Payment_slip_for Outstanding 001005l.htm	Get hash	malicious	Browse	• 152.199.23.37
	dez.htm	Get hash	malicious	Browse	• 152.199.23.37
FASTLYUS	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 151.101.1.195
	boysLove.dll	Get hash	malicious	Browse	• 151.101.14.132
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 151.101.65.195
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 151.101.65.195
	converter_1626796202.dat.dll	Get hash	malicious	Browse	• 151.101.1.44
	SKM_C258201001130020005057R1RE.jar	Get hash	malicious	Browse	• 185.199.108.154
	recognizerCryptolocker.dll	Get hash	malicious	Browse	• 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	recognizerCryptolocker.dll	Get hash	malicious	Browse	• 151.101.1.44
	INV #95000987.html	Get hash	malicious	Browse	• 151.101.112.193
	soa-032119.exe	Get hash	malicious	Browse	• 185.199.108.153
	PandaOCR.Pro.exe	Get hash	malicious	Browse	• 185.199.108.133
	PandaOCR.Pro.exe	Get hash	malicious	Browse	• 185.199.108.133
	Software updated v2.6.0.exe	Get hash	malicious	Browse	• 185.199.109.133
	product samples.exe	Get hash	malicious	Browse	• 151.101.1.211
	XFfw6uDKna.exe	Get hash	malicious	Browse	• 151.101.112.193
	cheat.exe	Get hash	malicious	Browse	• 185.199.110.133
	TIJYYIYJpv.exe	Get hash	malicious	Browse	• 185.199.108.133
	another.dll	Get hash	malicious	Browse	• 151.101.1.44
	borderCurr.dll	Get hash	malicious	Browse	• 151.101.1.44
	asdsad.dll	Get hash	malicious	Browse	• 151.101.1.44

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
b32309a26951912be7dba376398abc3b	IPVrDRKfYj.exe	Get hash	malicious	Browse	• 151.101.12.193
	_VM_1064855583.HtM	Get hash	malicious	Browse	• 151.101.12.193
	INV #95000987.html	Get hash	malicious	Browse	• 151.101.12.193
	ATT74992.HTM	Get hash	malicious	Browse	• 151.101.12.193
	5cksYFGC2g.exe	Get hash	malicious	Browse	• 151.101.12.193
	ATT59696.HTM	Get hash	malicious	Browse	• 151.101.12.193
	ATT59696.HTM	Get hash	malicious	Browse	• 151.101.12.193
	jYzWBKTsxE.exe	Get hash	malicious	Browse	• 151.101.12.193
	ATT25402.HTM	Get hash	malicious	Browse	• 151.101.12.193
	ATT62725.HTM	Get hash	malicious	Browse	• 151.101.12.193
	WAdStf9Llw.exe	Get hash	malicious	Browse	• 151.101.12.193
	RemittanceAdvice617492.html	Get hash	malicious	Browse	• 151.101.12.193
	qET1iJuly 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 151.101.12.193
	July 16, 2021, 092847 AM.HTM	Get hash	malicious	Browse	• 151.101.12.193
	Statement & Remittance advice 07.13.21 - Copy.htm	Get hash	malicious	Browse	• 151.101.12.193
	07xufnlKWd.exe	Get hash	malicious	Browse	• 151.101.12.193
	Machine Service.xlsx	Get hash	malicious	Browse	• 151.101.12.193
	Machine Service.xlsx	Get hash	malicious	Browse	• 151.101.12.193
	#Ud83d#Udd0ajs_msg_ 3pm.html	Get hash	malicious	Browse	• 151.101.12.193
	Kay Supply, Inc. REQ 009046.html	Get hash	malicious	Browse	• 151.101.12.193
37f463bf4616ecd445d4a1937da06e19	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.23.37
	192-3216-Us.gt.com.html	Get hash	malicious	Browse	• 152.199.23.37
	N41101255652.vbs	Get hash	malicious	Browse	• 152.199.23.37
	FILE_2932NH_9923.exe	Get hash	malicious	Browse	• 152.199.23.37
	RDlkHCLRxE.exe	Get hash	malicious	Browse	• 152.199.23.37
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.23.37
	Swift_Fattura_0093320128_.exe	Get hash	malicious	Browse	• 152.199.23.37
	SecuriteInfo.com.Variant.Graftor.981190.24096.exe	Get hash	malicious	Browse	• 152.199.23.37
	IPVrDRKfYj.exe	Get hash	malicious	Browse	• 152.199.23.37
	11.docx	Get hash	malicious	Browse	• 152.199.23.37
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 152.199.23.37
	Wcqwghjdefrkaiamzhtbgtpbmolvfnoxik.exe	Get hash	malicious	Browse	• 152.199.23.37
	Wcqwghjdefrkaiamzhtbgtpbmolvfnoxik.exe	Get hash	malicious	Browse	• 152.199.23.37
	BoFA Remittance Advice-2021207.exe	Get hash	malicious	Browse	• 152.199.23.37
	8rbuJ8Ycv1.exe	Get hash	malicious	Browse	• 152.199.23.37
	DRQxZrK.dll	Get hash	malicious	Browse	• 152.199.23.37
	DRQxZrK.dll	Get hash	malicious	Browse	• 152.199.23.37
	lpaBPnb1OB.exe	Get hash	malicious	Browse	• 152.199.23.37
	nZdwtTEYoW.exe	Get hash	malicious	Browse	• 152.199.23.37
	unJLhL75HG.exe	Get hash	malicious	Browse	• 152.199.23.37

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\22a972eb-d9e4-45de-82c6-1bb701bf0051.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):	368988
Entropy (8bit):	6.028936777522827
Encrypted:	false
SSDEEP:	6144:Ce98KWPnuw15QgBBDG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinT:CY4j1igBBDGNPUZ+w7wJHyEtAWW
MD5:	9782D1BB3311EEBDBFACBD43902CF91A
SHA1:	0C0DE94C5A4541941BAB60BDDBB51B5A912F07E3
SHA-256:	90A3B84743956A788173EFD10992D3A64CCF75A531A6ACA363E2A46633747952
SHA-512:	90D110153440C7C1C6BB670E0A2352063E6E4995563B9B382108478D489CB958204E13761945DF8AFFD1F0E5D7C0DA62F1E91DB92A694B1C90971B569024CEBA
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626929969265992e+12,"network":1.62689757e+12,"ticks":6861895878.0,"uncertainty":4398782.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488503367"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\264ead9f-6097-4a7e-8ca4-f709d0d0fd98.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):	368537
Entropy (8bit):	6.028225475414381
Encrypted:	false
SSDEEP:	6144:Te98KWPnuw15QgBBDG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinT:TY4j1igBBDGNPUZ+w7wJHyEtAWW
MD5:	48BB1679ACFA8654C87CDAFD657DEA96
SHA1:	EE4A813D842D40D948426B647F5E5AA724A76845
SHA-256:	E71A8EFE04876A77445502DBDAFA7908A31B38324F924E900570E608E434D5EE
SHA-512:	2CBD8EBB8074FC2E145AEDE22D875FD0C9132C48DD319B8A4E6B559A246A63120FDB3C3D6EB14ED6E0F33C4094C9FF3B2322BB50249A1E4FFD8C4B557FEC228

C:\Users\user\AppData\Local\Google\Chrome\User Data\264ead9f-6097-4a7e-8ca4-f709d0d0fd98.tmp	
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626929969265992e+12,"network":1.62689757e+12,"ticks":6861895878.0,"uncertainty":4398782.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488503367"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\38c9683a-e416-486e-b057-a6e67a02992f.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):	368704
Entropy (8bit):	6.028459398255349
Encrypted:	false
SSDEEP:	6144:8e98KWPnuw15QgBBDG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinT:8Y4j1igBBDGNPUZ+w7wJHyEtAWW
MD5:	7B147AA69857111BC060B4340251C991
SHA1:	B8B6AE6BAAF86BDB71D2A418D57651907026C928
SHA-256:	DA55B8BD80BEE638B69A8717BE31369BF1A8E7EF5B9A469BB3C8A24E42014371
SHA-512:	688821BE7D5B61287159FB9B548BACD1F07A688C4117C23406913781705BB1E4DD526A6D365CC04CD36B8ED7B5ABD3B0EE75E36E17DF60CEE1EF2F40BB810DD
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626929969265992e+12,"network":1.62689757e+12,"ticks":6861895878.0,"uncertainty":4398782.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488503367"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\409d4fe4-6a5f-424a-a2c5-47a12f644b13.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7444501860432515
Encrypted:	false
SSDEEP:	384:VrMTbJW0hZ15V1X/mNfr8vLR30zN0HdQGwPrK1T7xMtpRori/mqurWB/b30OV1jn:QqatdChvUcernZVMvrupKnhLpJ
MD5:	2CEDCB2A48B5496C1719DEF09C93C7A3
SHA1:	F31CF802F65B9AB21785EADF3E673101304FFCF9
SHA-256:	39C52F0D71D5D2C680539E124E870F8600C93D39B9EF51EC0760C51C409A974D
SHA-512:	BC151A1EE672DBA4D8886E45CBB3C7F4168BE79FCF096310CF22B432229D86B7B7917D02423C0274737B9CE1CB57E35EADEDED1440BE25CD722444736749955E2
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...d@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\464516d9-00fc-45ec-a739-f82b3f146da2.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):	376995
Entropy (8bit):	6.049362200545819
Encrypted:	false
SSDEEP:	6144:Ee98KWPnuw15QgBBDG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinT:EY4j1igBBDGNPUZ+w7wJHyEtAWW
MD5:	A2F29A867FD61367801426C78F98A9B2
SHA1:	CA9E4378E0375A99ADAB96C3B767B749658B80E8
SHA-256:	CA619CEED432A6E573C3C89086A03D486DEB4D761D1AF3198829A86DDEE97A13
SHA-512:	05398FD1C8A5D6E7EDCB29D2FB501DC848C27F1A704553EDE68C7E2A9F6D78C245D6E0B3E4F75986D341F8EEF8C2BDC94505A6BE00D39601909AAB7D7227279

C:\Users\user\AppData\Local\Google\Chrome\User Data\464516d9-00fc-45ec-a739-f82b3f146da2.tmp	
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626929969265992e+12,"network":1.62689757e+12,"ticks":6861895878.0,"uncertainty":4398782.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\70fa48f6-5a32-43ff-ab3c-eb857debf6ca.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):	376995
Entropy (8bit):	6.049361820190589
Encrypted:	false
SSDEEP:	6144:me98KWPnuw15QgBBDG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinT:mY4j1igBBDGNPUZ+w7wJHyEtAWW
MD5:	6E275F3C45D9F658D6A5911DE6D7E9CF
SHA1:	265C90F19312487704812CFB744ECDED9AF733F5
SHA-256:	E2FB05CB019771A2F07D0F04A0C99A8F181A8CD456CFAC2AA2F3F41546795E34
SHA-512:	3DF1B807F4312D49405F41B211B2C07D06F8F9F180C3B7BD204945F2D06E87A12BCBD06EC55831B706E31793E0A3400BE3416919ACEB71CCFCD2C0B0F999A43
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626929969265992e+12,"network":1.62689757e+12,"ticks":6861895878.0,"uncertainty":4398782.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488503067"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\98fbf5ab-09cd-4555-a8c8-2b07d3aaa1fd.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):	368894
Entropy (8bit):	6.028766327770171
Encrypted:	false
SSDEEP:	6144:+e98KWPnuw15QgBBDG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinT:+Y4j1igBBDGNPUZ+w7wJHyEtAWW
MD5:	9B872EE9A84A68E0FED5CFA18A682084
SHA1:	BA45E342522F17FBFCD9803706725C743CA1BDBE
SHA-256:	69DECD4F53A946E95ABBD03299BAC66598E0142B825870969647AD8DF9523EAF
SHA-512:	6842CA1158D2EB478DA30F0FE26D4249CB8A7180EA6B1EF5CC5DD63EAC52FA87C26E4F7FB888A60495754ED60D920E7502AE327B05718AC6BBAAAB958C26AEB9
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626929969265992e+12,"network":1.62689757e+12,"ticks":6861895878.0,"uncertainty":4398782.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488503367"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\9d8edceb-84f7-4f48-9684-2ffcb5ea27c1.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):	376995
Entropy (8bit):	6.049362200545819
Encrypted:	false
SSDEEP:	6144:Ee98KWPnuw15QgBBDG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinT:EY4j1igBBDGNPUZ+w7wJHyEtAWW
MD5:	A2F29A867FD61367801426C78F98A9B2
SHA1:	CA9E4378E0375A99ADAB96C3B767B749658B80E8
SHA-256:	CA619CEED432A6E573C3C89086A03D486DEB4D761D1AF3198829A86DDEE97A13
SHA-512:	05398FD1C8A5D6E7EDCB29D2FB501DC848C27F1A704553EDE68C7E2A9F6D78C245D6E0B3E4F75986D341F8EEF8C2BDC94505A6BE00D39601909AAB7D7227279

C:\Users\user\AppData\Local\Google\Chrome\User Data\9d8edceb-84f7-4f48-9684-2ffcb5ea27c1.tmp	
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626929969265992e+12,"network":1.62689757e+12,"ticks":6861895878.0,"uncertainty":4398782.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHGftEwozZHGftEwozZHn:+EwozZHGVEwozZHGVEwozZHn
MD5:	4829695F153A750ADF50C6E979E8E8F3
SHA1:	2F697EF207460D03671E4B59670BC73328D60D6E
SHA-256:	1AACF1304FD42C84FF41DDD2F2252E5C0EDE7362352661B7957648F2EA4C2683
SHA-512:	6D16A6EF4BB20B25B1B14757C475E9F8C3A40D6181F718D563A628BA41DA9426E1B586C472D4F8729FD65FCA014151B7D46FBFAAE171BFF9A6D937DB7A7A2C02
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0accabc9-fa60-4f65-a7ea-7d9b5d1c5d84.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22594
Entropy (8bit):	5.535614665888027
Encrypted:	false
SSDEEP:	384:2O7t7LlQ31Xg1kXqKf/pUZNCgVLH2HfDorUuHG6nToI0iv4c:RLliRg1kXqKf/pUZNCgVLH2HfkrUeG6t
MD5:	6F482BD6FACE3258A113DEAA699F1CFC
SHA1:	CCA1660627BA1B5C4F174665A43F3B311A414D7F
SHA-256:	7FCDBD037ECEB1E692EE3CAA91B9867D9297E076E009A21310812A40E99BA4A0
SHA-512:	A5310CEAAD0E3DD37ADB2E794DBDA64A8994828FFB0B2AAE1385584278FC1F1B90945B92F1F7191241F8070C66D8917CF7F19198112CC9EED6BC245B5E2A0E97
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13271403564401538","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\65e5e673-e0b6-42f0-9fae-90f9fde41682.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\65e5e673-e0b6-42f0-9fae-90f9fde41682.tmp	
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7e1ea8e6-047d-4d44-ae73-a07efc9b2feb.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):	874
Entropy (8bit):	5.555125829425211
Encrypted:	false
SSDEEP:	12:YmZ6Hk3O+UAnIvcJeJrNgmh4r+UAnIEJScNnYj+UAnIEORY1R7N+UAnIO0cVWFKg:Yc6H0Uhc4G1KUe4aUeR7wUpm3RUeHQ
MD5:	CEE8313DD4CF4769D0498A0E2EF9FA00
SHA1:	7B97F46BD4F24C9DFBA3D8F1DF3DE0116697C862
SHA-256:	1522E4F2F13436274B57A4ED1D2BB26645831F87E1330DF71E9E9C805147B2F3
SHA-512:	BAA4E066F978CBC298F140F8291DC4E98DCEA93E1E4B1E33DDE1C1F0852DE1BB5B7B0B2874ED8B9EAEBB6E9370602D4319D9E37CA5B640A10047D229DD130B60
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.52056},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.455726},{"expiry":1658465969.286412,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626929969.286418},{"expiry":1633015352.814139,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.814142}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\941d0dfd-3fac-4374-912f-e90d6b0483de.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.53566550959919
Encrypted:	false
SSDEEP:	384:2O7tCLlQ31Xg1kXqKf/pUZNCgVLH2HfDorUuHGRnToO0L/v4G:YLliRg1kXqKf/pUZNCgVLH2HfkrUeGRm
MD5:	396C5A2090C777FF10B8FDD9765B411F
SHA1:	CBBCA26906CF6F40475C8E66F3B60AE20988B877
SHA-256:	2100DEA3C75D3FC725529CDC4BC2BA37A55628500F0F92F1AF12E617577772D4
SHA-512:	B7AEBE0F432B9A3ACD48EF7F33D1940F374776257F59AB148EA9E2E7AF455CD5C963244FD5C9AF938DF21C2BD8A04D465661AF79106D6BB80B5E07F33C7F5B34
Malicious:	false
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13271403564401538","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9dfe1fee-4a66-4581-83f1-c3e0e326be03.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):	2371
Entropy (8bit):	4.8921682885389925
Encrypted:	false
SSDEEP:	48:YALteBdpNntwTCXDHzM7sgeRLsKKOcsqqSgsAyKsa3zsU5MHRYhbG:2lNnOTCXDHzMTetKO1VD5G+hS
MD5:	E7021E72FB2B6B1B6276D1223DD8F824
SHA1:	76BEF692E837F9915DA561DEA0D6DD053AC364F3
SHA-256:	CAED59E367CDEA137FB80394DD9707D8A21DCC63CDDF7333AD6514CFE0286EFD
SHA-512:	27AB4C40F36E7CD53C4742372D8CFB8901F3C1A2A5924762B7F5EC3710F7E43096E573F579FC3200821C2124DC39E9BAF234B3CF26E87BB29F0EAC8E7EAC2CD
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9dfe1fee-4a66-4581-83f1-c3e0e326be03.tmp	
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://i.stack.imgur.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273995569286292","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ac

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):	340
Entropy (8bit):	5.19775566691528
Encrypted:	false
SSDEEP:	6:m3lVL+q2PN723iKKdK9RXXTZIFUtpgIiZmwPgI1E1zkwON723iKKdK9RXX5LJ:1F+vVa5Kk7XT2FUtpli/PlO1z5Oa5KkT
MD5:	342BA6B4B57BAF8A119EE64AE6A1A465
SHA1:	BC02D5ACA82FC4FE8F36097CDFC0F3908FF8E32B
SHA-256:	9D7EB036BB26569F6855A5E4B6125F0F1EE4A479758EA225436635552AC62417
SHA-512:	0D60BC0992D018D1443AEC55511A6F027C377406E95A84460E22A414CC6EDA0A9E37D83EB000EF50BA2DE0ED8B4E6C26100682EA8A703281933389FB6F32714
Malicious:	false
Preview:	2021/07/21-21:59:30.279 1a44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/21-21:59:30.281 1a44 Recovering log #3.2021/07/21-21:59:30.285 1a44 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):	324
Entropy (8bit):	5.196207428436287
Encrypted:	false
SSDEEP:	6:m3lpq2PN723iKKdKyDZIFUtpgIrbZmwPgIvQkwON723iKKdKyJLJ:1pvVa5Kk02FUtplrb/PlvQ5Oa5KkWJ
MD5:	F832DEA9FAADAFAC5EA3314E851AD777
SHA1:	3881E9C73EB4A0A3EE0FC023F5687B626CAED0A6
SHA-256:	2FD329B189525734B1B7DFFA1932597F8867D6BE1D0C46D6E9803AD4327E9F5E
SHA-512:	D5EA03635B9D51FEEFE3F5E2A92FFFDDBFBC51520741A4CCEA6B2353C48A6914A0E6C52EDC35D678C0CD2C889598472361009CC887DEA7229A0471F9D1FA689
Malicious:	false
Preview:	2021/07/21-21:59:30.258 1a44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/21-21:59:30.259 1a44 Recovering log #3.2021/07/21-21:59:30.261 1a44 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):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
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):	0.964125969137907
Encrypted:	false
SSDEEP:	24:wpIvJn2QOYiUG3PaV3qLbJLbXaFpEO5bNmISHn06UwEt8:wpIvZXC/aFq5LLOpEO5J/Kn7Upt8
MD5:	F2B95811E123F5D82235FBEAF39BE94F
SHA1:	07B9457C4E96AA9D8AB3682B16DBF6E5D139535D
SHA-256:	8E3587B8420C43201B7E1DC760495449C0562DB7C49C297541AAF633198FCA33
SHA-512:	FEBE89C1362F2ABE75986E106DBBE2396564DF2AC4D7B6CCA69418F1EB33AA2B7B4292EE3BA46AC429F42BA811A7EC508926A15DA340D6F62E0DBE61538A030B
Malicious:	false
Preview:	.....i..... ....

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):	1633
Entropy (8bit):	3.462594782987131
Encrypted:	false
SSDEEP:	24:34S7lrlo6Ot+lo74ZHBKLWw9QE5L1YYMbxUt+lo6lLlL:34gxo6plJ+ZT1FAFlHRL
MD5:	E9775EE57B9C1C798060AD1FAEBA564F
SHA1:	E593E81FA79186E02CD8C5CE9C79CDE04D3EBA68
SHA-256:	FBC5B89873A731DE6364FB4E3D85D5827250AC9E390929F265344854FF73458F
SHA-512:	0BE3E0A88369B02887C32111A0008E6CC0ABB87DCBEA0DE428C721B34E4F1ADC319E869FBBA11307AEA841E5A88FCC9C8724BDBDCBA7D2DCA61FE47D29D9760
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...21b9bd21_d110_4b5b_a345_ea84b22ba3f0.....F..... .....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....K...file:///C:/Users/user/Desktop/Convert%20HEX%20uit%20phishing%20mail.htm.....S.i.g.n. .i.n. .t.o. .O.u.t.l.o.o.k.....h.....`.....m/.&....n/.&.....0.....K...f.i.l.e.:././.C.:./.U.s.e.r.s./.e.n.g.i.n.e.e.r./.D.e.s.k.t.o.p./.C.o.n.v.e.r.t.%.2.0.H.E.X.%.2.0.u.i.t.%.2.0.p.h.i.s.h.i.n.g.%.2.0.m.a.i.l...h.t.m.....8.....0.....8..... P.....p.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.158900823176991
Encrypted:	false
SSDEEP:	6:m3fLYq2PN723iKKdK8aPrqIFUtpgfLQRU9ZmwPgfLQRUPkwON723iKKdK8amLJ:oLYvVa5KkL3FUtpYLEk/PYLEE5Oa5Kkc
MD5:	5F08731336EB0096BA1A8B6E3A4F223F
SHA1:	8DFF93F4980F4F6D87F575687A1F686F9601C4B6
SHA-256:	1D3062BAB840CF62F9315556F516F745361AF4E75AEBF8010792C5ECAE55A2A0
SHA-512:	846D83F79320129B36E74F60756A66C1DC0E679FFB86AA667EF9FB078026EAA02BE61AC0967F028F1B8A1E740BDCAB636D4E9CE23C1813E251879301742BCB2E
Malicious:	false
Preview:	2021/07/21-21:59:24.903 1414 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/21-21:59:24.905 1414 Recovering log #3.2021/07/21-21:59:24.905 1414 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Preview:	.f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f. 5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5.. ....f.5...............f.5...............f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.170412900338023
Encrypted:	false
SSDEEP:	6:m3TLamq2PN723iKKdK8NIFUtpgTLoUy9ZmwPgTLblFkwON723iKKdK8+eLJ:kLamvVa5KkpFUtpULJi/PULP5Oa5KkqJ
MD5:	844FE2D86791000ADE89E7F6D467BD5D
SHA1:	1F2CE78A613AB94F2F120DE797D0285391549E14
SHA-256:	79516E0541049A5FE71814368D5E0A3B28433A4AF0717E19DBC3D2BC5504B501
SHA-512:	A579104AEDA9E7153F7256970353E9CCDE9ABBA62C969DFCB911F063F9917788F0B32B6F79D5814063B9524275D559C707A79F5C0B6B9A1CBB5FDF2C12E2941
Malicious:	false
Preview:	2021/07/21-21:59:28.902 1414 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/21-21:59:28.904 1414 Recovering log #3.2021/07/21-21:59:28.907 1414 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F

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=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","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=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.213670822655231
Encrypted:	false
SSDEEP:	24:LLwxh0GY/l1rWR1PmCx9fZjsBX+T6Uwpat+loYGIT5ktsaDc90R4snrwTnNGKt+v:yBmw6fU4tlAitjI90R4uEG9lyo
MD5:	4BFB1AC19A4FC376A5A281284CFF5154
SHA1:	62802EF6A8F87EE79BC92519A48ACA0B330BAC3E
SHA-256:	29E90CE963F52917EB909F5D4882B61657563C55307EBAD9E496ABD6C0B5EC84
SHA-512:	8202A2037F6A388CA2DCDB75602CEE48E3AB08ED90244C6CD9700D2BA8CA62A04F3C5536C477865BB923CDBA37AFBD494D051B19DE8A47E5E1EE4378C20CDF3
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):	0.7778275776771448
Encrypted:	false
SSDEEP:	24:yFicDSsEtnyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwcAt3n:yFicDSsEtndBmw6fUjAt3n
MD5:	843DE133BB10F3F8837E97CC449EF377
SHA1:	76ACE866606DDEEFD17211D126E90595D36EF93A
SHA-256:	DEBC049027D162412B98D425443ADA65FFEE1C2CFD838C33EB19EA65FDF943B2
SHA-512:	CFFCE7942A0FB38B503286D2B7D14BF9D1F823B5B03B1DFCD3E46FA81AE5F600F67DBA8A571582748885AA1E9DFCE165966C6A7420D354901F16207B18AA08A
Malicious:	false

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.188276022826069
Encrypted:	false
SSDEEP:	6:m3lDd1Iq2PN723iKKdK25+Xqx8chI+IFUtpgIfjZZmwPgIrFkwON723iKKdK25+M:1DovVa5KkTXfchI3FUtplf9/PlrF5Oak
MD5:	E68B2F098E1B658FD474FCA35F998DC2
SHA1:	6C3092631DD040959B334F400B8B061CCA68ACBD
SHA-256:	1B7916F0F0DC783ED567C756273EE199D2264DF9188AAE06C2688AF5E466E8BE
SHA-512:	64B190C11A9AB8903A48E5DA6B34DC9B1CF55649B49911AD4575146B8BB5C033C6F0E88B919594A5B1DA824C21E89A97D41633484E48676F238FD9A99C223F71
Malicious:	false
Preview:	2021/07/21-21:59:30.172 1a44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/21-21:59:30.222 1a44 Recovering log #3.2021/07/21-21:59:30.224 1a44 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):	364
Entropy (8bit):	5.174740148964058
Encrypted:	false
SSDEEP:	6:m3l2Sq2PN723iKKdK25+XuoIFUtpgI9XZmwPgIzVkwON723iKKdK25+XuxWLJ:12SvVa5KkTXYFUtplZ/Plp5Oa5KkTXHJ
MD5:	33FF9DEC5FC58EB9BE9D6E0AFF72D94B
SHA1:	B2F9284AFB5FE408710EDCCEE47A38EC113F4DF0
SHA-256:	0A95BD0C396E88D3DDC462B24B3B01C77639C3F08D31BADD9B65285AAF48A708
SHA-512:	518DF1B6E4DFE9D87E2F5A6EAC70AA82A6EF524767E9D9BDDF7A353E5F2BC95CF2DF18A13EDB37EE19A3627C45F46B44F36DC2EB707A88BDC1A7A4A82EAA7C77
Malicious:	false
Preview:	2021/07/21-21:59:30.139 1a44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/21-21:59:30.154 1a44 Recovering log #3.2021/07/21-21:59:30.156 1a44 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):	336
Entropy (8bit):	5.1889920990694
Encrypted:	false
SSDEEP:	6:m3lcOq2PN723iKKdKWT5g1IdqIFUtpgIn49ZmwPgIn4PkwON723iKKdKWT5g1I3e:1tvVa5Kkg5gSRFUtpll/PlQ5Oa5Kkg5i
MD5:	CBC1BDCE9F62FD0555B46504826341AB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
SHA1:	1CF7C4654E6DE80A0ED46861F59C710CB24B9969
SHA-256:	2F7B9A237DD8BA1E92332C34CF1C241114DDEF3DC795F00A2E0F5CCE13605F44
SHA-512:	B21158789E7E834B69E46ED2AB43F40C66D1512DA27047FEC8AC2E03000F8DBFF2A3F35031CBD10A74E0869D1A9266128D74FD7AD62E1CE248ABBB215A96B6E D
Malicious:	false
Preview:	2021/07/21-21:59:30.038 1a44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07 /21-21:59:30.041 1a44 Recovering log #3.2021/07/21-21:59:30.041 1a44 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\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):	0.1336289838858557
Encrypted:	false
SSDEEP:	12:TL+A/Z73Bv+oIohxBENuQOCGI/gBv+oIoz:TLxZ73t+lohxBwurt+loz
MD5:	704AE2D164911ED4F815D924DBFBB645
SHA1:	3560330137FCD9B8B0CFCF0E9C66B1E039C13095
SHA-256:	9214469229522427CECAD07F32695C0779FFB52F622264C0840C3A39D6715D54
SHA-512:	E3AB6BF4ED67816767FDEDCF876CE51821FB4755C72F1A31EEFE9F4B214E0BF0A9DE7368CC0332B4ECBB9CD16E14E4166CD8094C3D3BDB1B4C73DF4ABA323 28F
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):	807
Entropy (8bit):	5.287678024362349
Encrypted:	false
SSDEEP:	24:nxCJ21mIk6zPxY+sEBdEY78BJgskfa9yBDOxo73t+loYeBl:nx4286Px/SUQl3El
MD5:	046910D72F6653E1C605CFD29C881C0A
SHA1:	D628F6A3A0DE26816D9A6BC57137F92EC6B11D89
SHA-256:	3445D426DC2F6E9001DA6474BD1B6322A7A5653B1EB4CE53D92D544138225D13
SHA-512:	04431D1C6B9F55AD8B25EB07DD3297B6E51FBFF31BDF2BEBC2FC32CA630C35CD231E5CB883EEE8C5B3642F1F04B70D7B8CEBB4054AC336B7870206B5DFB44 B16
Malicious:	false
Preview:	....."d....c..convert..desktop..user..file..hex..htm..in..mail..outlook..phishing..sign..to..uit..users*.....c.....convert.....desktop.....user.....file.....hex.....htm.....in.....m ail.....outlook.....phishing.....sign.....to.....uit.....users..2.....a.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r..... .....s.....t.....u.....v.....x...:.....B..... .....*Kfile:///C:/Users/user/ Desktop/Convert%20HEX%20uit%20phishing%20mail.htm2.Sign in to Outlook:.....J....."*.2;@.....

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):	0.11673154630529205
Encrypted:	false
SSDEEP:	12:2ivPp6l22fogD+WqLBj/KQh+3lf4nMWQfy9L0BQZ8fOi:2iHp6l2FgDpqLBLh+3CtN0TfX
MD5:	0FAE05CA477E5E7622D8E23DE16740FF
SHA1:	396EFE303C04AB8893741830F38A57DB455A4BC2
SHA-256:	F5B34645F230C93DE3E89A8677CB0FA4BD49E333B7E02F8045E044022735F464
SHA-512:	3484082B701D34FFB7B9E1EAA7FCB367860B472EA47C84FCE313BE123AEF311843B9BE434B9C82B5AA40C0E89C4A8CC2F69A515CF65E60F6A3ED2B70CC1A4E AE
Malicious:	false
Preview:	.....-..... ....

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):	5.480384023939533
Encrypted:	false
SSDEEP:	48:Ng3Gbev2rKa7LKM3n+8db/nVncXcXbQSefgGNYNrS0U9RdiN9ua:WzOrKa7LKM3Vdb/VncXcXbQ5fgG6rS0r
MD5:	C98F33131416210D7AC040410188291A
SHA1:	0EA0A49426386F8C25A15124653257FB8BDE5D59
SHA-256:	9BD25FA461C8DBF8E68EF991B106FD49F6B3E7E5C36407EB3E676A06D2B8A7A7
SHA-512:	31059783CC727AE7E3E9D35337EF7D7EC58F4616AE0B6CE85DEF4BFB1C0C1FE000E236C299717D9CFAC9915A38785EF2B227CE8D93B54979DB85F3C4B5AB2F7
Malicious:	false
Preview:	.....*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService:.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..761346000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-21 21:59:32.95][INFO][mr.Init] MR instance ID: 7f09217b-7880-48ec-b3f9-9a8c2e804e6e\n","[2021-07-21 21:59:32.95][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-21 21:59:32.95][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-07-21 21:59:32.95][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-21 21:59:32.95][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-07-21 21:59:32.96][INFO][mr.CastProvider] Query enabled: true\n","[2021-07-21 21:59:32.96][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):	338
Entropy (8bit):	5.185053562348859
Encrypted:	false
SSDEEP:	6:m3fL/uRSQ+q2PN723iKKdK8a2jMGIFUtpgfL5/pgZmwPgfL7BQVkwON723iKKdKw:oL23+vVa5Kk8EFUtpYL5e/PYLOV5Oa5i
MD5:	191297BF7EA7F7A1B838F49F97BFB8A0
SHA1:	E625CC60FF3A2700DADDDFFCC56531B7CEF2E6BE
SHA-256:	E947040715C25E31AA9055853AAA9234BF1B72961E91C04607E7814C5FF1C23B
SHA-512:	D2460B524A52F6C7D3D38AAEF619978F0C4FFBA4D780A6121D10DF391F85F5E95A51CDB395F57DAD8D8ED61D3A7D22DB56FE48AF9726E87205ED81ABD7A289E
Malicious:	false
Preview:	2021/07/21-21:59:24.543 13dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/21-21:59:24.545 13dc Recovering log #3.2021/07/21-21:59:24.547 13dc 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):	337
Entropy (8bit):	5.219527894983063
Encrypted:	false
SSDEEP:	6:m3fL6jM+q2PN723iKKdKgXz4rRIFUtpgfLtZZmwPgfLRMVkwON723iKKdKgXz4qG:oLIM+vVa5KkgXiuFUtpYL//PYLRMV5O6
MD5:	BA80B1482A3622B9F4B008D3E5A0DA69
SHA1:	BDDDC9BDC4C8DCC5812558697F8C1C66C0E9708F
SHA-256:	4084401F9392C1248883782C774A36726A20261A6737C3144A631445B53FB430
SHA-512:	001E7A1B6AEA65005B370950F8D1EDEDA3273C42844BF88B148144045D731C7DBAF0AE00D447D6C02D1AD2782525F08FE20B5CF21C822502C30D52D855D3D8A
Malicious:	false
Preview:	2021/07/21-21:59:24.939 f8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/21-21:59:24.942 f8c Recovering log #3.2021/07/21-21:59:24.943 f8c 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:	3:5ljljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
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):	323
Entropy (8bit):	5.190348228750443
Encrypted:	false
SSDEEP:	6:m3fLW9q2PN723iKKdKrQMxIFUtpgfLwYZmwPgfLwAkwON723iKKdKrQMFLJ:oLW9vVa5KkCFUtpYLd/PYLv5Oa5KktJ
MD5:	13299FD71C7B45CD749CD07BF58FE838
SHA1:	6951ED345358C32CEDE4020B764CD585258929C7
SHA-256:	B27B5FBC3D34C9F87E6E24049D1471EB294EF344ABB1E2D5C2A992A869C948DB
SHA-512:	40BE25888667F28D8D0BA90EBB91880CA55C2BF279078A753DE01C59DB78E72771EC3877EAF2A443E07CD0F65F39EC1EB9E6E6111BC1AA5B568ED64F547A99E
Malicious:	false
Preview:	2021/07/21-21:59:24.861 ad4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/21-21:59:24.863 ad4 Recovering log #3.2021/07/21-21:59:24.863 ad4 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):	351
Entropy (8bit):	5.15035662030105
Encrypted:	false
SSDEEP:	6:m3fLA+q2PN723iKKdK7Uh2ghZIFUtpgfL2tXZmwPgfLZRFkwON723iKKdK7Uh2gd:oLA+vVa5KkIhHh2FUtpYL2Z/PYLvF5Ox
MD5:	5779A5440CBA020358335E6D29762A9F
SHA1:	FDC857A095309B099DE3F41F5261FF42F0B74E0E
SHA-256:	E495FF9866DEFBF32ED426A5437D55E633596D69D49EBC58E1880EB20945E443
SHA-512:	EBE112776D7AB5BC4944E639A30878686F78033821F2ECEC57D3D0D0BF9C6EEEBBC9E1FAAD47F7C00EC39157C545988DBB0CE658482C5653A79B311EB8838E2
Malicious:	false
Preview:	2021/07/21-21:59:24.445 2d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/07/21-21:59:24.454 2d4 Recovering log #3.2021/07/21-21:59:24.457 2d4 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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	436

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Entropy (8bit):	5.260392236294803
Encrypted:	false
SSDEEP:	6:m3fLFOq2PN723iKKdKusNpV/2jMGIFUtpgfLvkZmwPgfL5kwON723iKKdKusNpV0:oLFOvVa5KkFFUtpYLvk/PYL55Oa5KkOJ
MD5:	1D6876887F95489248812C35101ADECD
SHA1:	BFE317F1685C28800B22DC89318F601CADC8CDFE
SHA-256:	4CEBC69CAFDA2D42CC37D0AD835D0C57B84458691C893B0DBA80E7BAAF89FA2D
SHA-512:	33492FC6044FCFA58AB17605033BCD54E781E439696431DE6BB82EE0317502F398C757AD0CB34A18BB70F09123AE673AA9C2E89FDC3BA4FB0E9E7DC949FA3227
Malicious:	false
Preview:	2021/07/21-21:59:24.877 1414 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/07/21-21:59:24.878 1414 Recovering log #3.2021/07/21-21:59:24.879 1414 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):	435
Entropy (8bit):	5.291228970896051
Encrypted:	false
SSDEEP:	12:oL/VvVa5KkmiuFUtpYLBnwg/PYLJI5Oa5Kkm2J:oLBVa5KkSgyL0LkOa5Kkr
MD5:	7703C7DDBD95F46F7662AE61E4952F39
SHA1:	D323D0BC81DC420CCA1D1A7FE8EE8C6FAB3D4FF5
SHA-256:	E8BCA227ACBA52BE9A3F8A8D1BC0B237C618DDDD5DC8AFC05CA5BF68500D1733
SHA-512:	E28E442C1CAB28B714C2B8724488BE0F47AC7C843B5DA54626B8B2DD27FA762DD0ADC44202D2E030ECD50FD58CF1CE0EF37D4A90747472BDC8D5FA92C8FB9C9
Malicious:	false
Preview:	2021/07/21-21:59:24.951 8b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/07/21-21:59:24.952 8b8 Recovering log #3.2021/07/21-21:59:24.953 8b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.2499897530985
Encrypted:	false
SSDEEP:	6:m3vb+q2PN723iKKdKusNpZQMxIFUtpgvKsZmwPgvs3VkwON723iKKdKusNpZQMFd:Eb+vVa5KkMFUtp0Ks/P0s3V5Oa5KkTJ
MD5:	F0177FFE860EFD123A524713D8410344
SHA1:	7AA247CA72C4D27687266EFAED1752CEFFF56B31
SHA-256:	44217F7209331CCB667B9F73356B0E9A5016006AD75F606764930D9CC77EA888
SHA-512:	376427247B881A18DF931D3A2B0534D935F26C1A31E348F3AEDBCBE21EB222DDA17819E4C9991A945BB88163052E7DFDF65406767E14515535106962F21358A8
Malicious:	false
Preview:	2021/07/21-21:59:42.797 b4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/07/21-21:59:42.799 b4c Recovering log #3.2021/07/21-21:59:42.800 b4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\da36ed04-88c5-40a4-b059-eb9836bd7189.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):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.191542474325605
Encrypted:	false
SSDEEP:	12:10vVa5KkkGHArBFUtplG/PlY5Oa5KkkGHAryJ:1+Va5KkkGgPgj2COa5KkkGga
MD5:	AFF5E604F0683C9593EEB63C209CBAAF
SHA1:	31256CF8202A56C53BD606957CE60F185DA53EBE
SHA-256:	99B2E85390F51E6250F97A16CC9DBF5C8F62D6D99058CD7A7B95AE2A3376379D
SHA-512:	C9B5ACE6C2C069927F6D97173E49ED71F5E48A5894D7ACD6082AD2CA1FD64560F63F6F77900D65D7354A6369C99B4DC38C7CD602E6AA5C3C3786C437C2EC3A6
Malicious:	false
Preview:	2021/07/21-21:59:30.619 1414 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/07/21-21:59:30.625 1414 Recovering log #3.2021/07/21-21:59:30.630 1414 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):	435
Entropy (8bit):	5.2238589592684415
Encrypted:	false
SSDEEP:	12:1B+vVa5KkkGHArqiuFUtplRZ/PlMV5Oa5KkkGHArq2J:12Va5KkkGgCgjB2Oa5KkkGg7
MD5:	A94D257316CFAB8E02EE14F07388AB4B
SHA1:	13561E4D52FD5EC055C1F1F260C9107271CC7706
SHA-256:	5D6258C184EDB3F96955AA55C6159C7713D5AAF4E691E8D1D37F1BA35D6F2A76
SHA-512:	80000CD7F5E6E35FF4562BF4970EBB185283EFD08B1DAD7F500DEDAC70788552AA6BA73F69916D074FF1B6E6FAD9004E5A0463F5590E45FFAA9237D650A010D
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Preview:	2021/07/21-21:59:30.623 b4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/07/21-21:59:30.632 b4c Recovering log #3.2021/07/21-21:59:30.639 b4c 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):	421
Entropy (8bit):	5.21667329679836
Encrypted:	false
SSDEEP:	12:A3xSN+vVa5KkkGHArAFUtpwja/PwPV5Oa5KkkGHArfJ:A3dVa5KkkGgkgatPOa5KkkGgV
MD5:	5955B2630AB505368F6083FB73770DB7
SHA1:	DB05509F9FF7074E944BB2B7F5136E0EAA3E19D0
SHA-256:	4E94ACE10E0E5168A6FA429EDE5299CD084D10EBD86F9CEAA1FA46CA61DC2397
SHA-512:	A6A59BC606245323BBA2AAA45D741EC75479497EC8219E3E5F1E541603DE50856903A31487441EA8E36BF866E80A8DA3D78BB84372F687F87E08E1E689BD1DC5
Malicious:	false
Preview:	2021/07/21-21:59:46.196 b4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/07/21-21:59:46.198 b4c Recovering log #3.2021/07/21-21:59:46.199 b4c 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\d4ab6060-f37d-4ea2-905c-eec3c17613f6.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):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A0
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","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):	330
Entropy (8bit):	5.240883518108279
Encrypted:	false
SSDEEP:	6:m3fLAW+q2PN723iKKdKpIFUtpgfLwa9XZmwPgfLSVkwON723iKKdKa/WLJ:oLAXvVa5KkmFUtpYL5X/PYLq5Oa5KkaQ
MD5:	542DFE28FCF30F71644497D486863388
SHA1:	5F5C0C1D955DD8D6DD204587B3C8E004A8BB43D9
SHA-256:	89634383C37CA263272E16FFC73E90DDB7A915012D58E7AD0E285658F1D431E7
SHA-512:	1DA6589AA014F534AD4B59311B83DAB445326F2658C4F8354B6A3C261CC32859B25FE89266B69AE7DE4DA939F82E0C016EC359962CBF3DDB8BCFC2455F3DB5(F
Malicious:	false
Preview:	2021/07/21-21:59:24.445 10b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/21-21:59:24.452 10b8 Recovering log #3.2021/07/21-21:59:24.453 10b8 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):	405
Entropy (8bit):	5.284226306131903
Encrypted:	false
SSDEEP:	12:14Z3+vVa5KkkOrsFUtpI4iSZ/Pl4IV5Oa5KkkOrzJ:16MVa5Kk+gj/WfOa5Kkn
MD5:	FA12C5DD01C56C95426F41BE1EE1A7D1
SHA1:	ACAB134C3A515657C24589FC5229E8DD3D0936D6
SHA-256:	9E8513E92F8F355AC607B6B4E0BB0825E16E6852924413CC4BED873C063459C7
SHA-512:	AA895DF4CD3AEF08063A28C3DCC079EA595D43B5F4B95126EFCE951D87214E84785878A04E02E542CB9817C09A254B572333805BAE95EA16DA58C6459A39C0C
Malicious:	false
Preview:	2021/07/21-21:59:32.929 b4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/21-21:59:32.932 b4c Recovering log #3.2021/07/21-21:59:32.933 b4c 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):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:uT:I
MD5:	2E68462D1918112E95BC6F32448A0D7F
SHA1:	A0265C3A408652502035F09183E47689A940E2B9
SHA-256:	D9A9877E9AB61485A32CD4C0196A8E2FF3EA89B9705214DC2682E51EDCF845F7
SHA-512:	9D3093E66080767760E62CF96E2D08CAF98302BC8D03174064D1E260F8CEA1D6A7955C705EE2F5BF0EE8A092906FF9EB63B4E3E83B54AAEA226EB285332C023
Malicious:	false
Preview:	.....v..Z`..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bf224988-4cd5-46fb-8249-c6138b8a037d.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):	5479
Entropy (8bit):	5.177646279078697

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bf224988-4cd5-46fb-8249-c6138b8a037d.tmp	
Encrypted:	false
SSDEEP:	96:nnXb8yAMDQqpDoaAKIW9xk0JCKL8rNbOTQVuwn:nnXbWMsi89wP4KsV
MD5:	0AC39DFB8A4A502E3C1AB6CE9A3B4B0C
SHA1:	BA7B839456DE1908B50529C0CA7751E4CFB7A35E
SHA-256:	31754D9BE7570E79AE0C000F92630AB47ECF1E8F9B77354D5C5F0AA6295C3B9B
SHA-512:	E31B70611C629043980D554309012BB3C73BFDFF0E0572084FA04C2EE0F2A242473D7D6DA8E96632EB05237BBB9BE245DB033D12777276A08CAC539831D0DBE
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271403564894759","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bffa793b-8dbe-405c-a4b4-dd7f82599cb4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5453
Entropy (8bit):	5.173771440890694
Encrypted:	false
SSDEEP:	96:nnXb8PAMDQqpDoaAKIW9xk0JCKL8robOTQVuwn:nnXbZMsi89wP4Ksa
MD5:	BC0A0BF50DDCCBF14799EC4F55B88EE3
SHA1:	D092457E460EB3711FAA71B0E535BFDC59D972A1
SHA-256:	4C97E50F6307180B20AE0771620BA810628F0741F17687D505FC9438188702C8
SHA-512:	FBB6FFD2E9DBBD77930AA7683F03E002C7D1853D0A15F163444E3C2F8D2CB3F67C0E8F17CD6C5D36943E4C8B042ED4A040B5EE1D94D74EA146BD2CAD0DC41 27
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271403564894759","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c318a30d-36fe-4354-b4ee-4378f131e789.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Preview:	.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
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):	4.562884756327839
Encrypted:	false
SSDEEP:	3:tUKCJc9acSRyZmwv3gJcIFdQ0V8sgJcJL1O0WGv:m3GacXZmwPgFQ0VvgUxO0tv
MD5:	58654A6010100A49966E7A0F4D38F157
SHA1:	1507079D5F7B35942E045E3B89BD520D5271ED55
SHA-256:	F818CC794CD0688E61A4AC21D2F9E9EEFA4EA04E0BCA2D616EF1F5483C2EA528
SHA-512:	5EA768F6D822C4D64CFA96369E4B070BFCE08BE1AC38F2B5321ECD0A9FB04463BE703D659A9BB241A4B94EB91A0D076B6F09673A06D5A99EA9AC3F1D5308EF C0
Malicious:	false
Preview:	2021/07/21-21:59:29.866 1a44 Recovering log #3.2021/07/21-21:59:29.926 1a44 Delete type=0 #3.2021/07/21-21:59:29.927 1a44 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\e1af0235-8458-479f-ab1c-98a50fe17144.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5453
Entropy (8bit):	5.173771440890694
Encrypted:	false
SSDEEP:	96:nnXb8PAMDQqpDoaAKIW9xk0JCKL8robOTQVuwn:nnXbZMsi89wP4Ksa
MD5:	BC0A0BF50DDCCBF14799EC4F55B88EE3
SHA1:	D092457E460EB3711FAA71B0E535BFDC59D972A1
SHA-256:	4C97E50F6307180B20AE0771620BA810628F0741F17687D505FC9438188702C8
SHA-512:	FBB6FFD2E9DBBD77930AA7683F03E002C7D1853D0A15F163444E3C2F8D2CB3F67C0E8F17CD6C5D36943E4C8B042ED4A040B5EE1D94D74EA146BD2CAD0DC41 27
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271403564894759","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	341
Entropy (8bit):	5.214355646673319
Encrypted:	false
SSDEEP:	6:m3I+2M+q2PN723iKKdKfrzAdIFUtpgI+/ZmwPgI+HXMVkwON723iKKdKfrzILJ:1+2M+vVa5Kk9FUtpl+//Pl+3MV5Oa5KF
MD5:	52B1C7C82063E7B2F2A9821A49A6186D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
SHA1:	7136C43A260D078CC947B65F0F75FBD3B0AEBE17
SHA-256:	613D065C9F5A4DC447FB5E962541DF3B4AF87D76A38F2BCD614365F0E2474C68
SHA-512:	5980F08F6E87412AEE91E92ACBD859CF3C611610CF57F3418682BF26AFCCFF63E0B4F7FEF9B3AA21C0A481259AF55379DF07C5D904C58707CDA9C325209D68B
Malicious:	false
Preview:	2021/07/21-21:59:30.723 f8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021 /07/21-21:59:30.727 f8c Recovering log #3.2021/07/21-21:59:30.728 f8c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_d b\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir3520_2140828001\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	186784
Entropy (8bit):	4.915957886381836
Encrypted:	false
SSDEEP:	3072:bl35PHEWQyoghJbTloZq6L45c7wbMn5nezpiKmneSxCgWCCkHjuhjMQBJXS:R3NKghJbTl96BXTChW
MD5:	E4ED6CE0DB78ED18701755E5FF177B82

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir3520_2140828001\Ruleset Data	
SHA1:	7D660E76CE91C05FC52FE1AD54C28EAD7E4A04B6
SHA-256:	BBA545E82F5720A1AD3BCB3743EB27BB1F015CB2E1222615CB880DA40CE42C20
SHA-512:	F49A4487C245DE86158EE6BD675BF70C74D8FE7164A5AA5D71469AFA94071FD4C06BB09E88E06B1CCDE9ADE6C124C957E45179C25891E12BD7C9FD419B7EBF72
Malicious:	false
Preview:	.....$...(.....\.....p.....P.....,.....geips..... /.....lgoog.....6.....ozama.....onwod.....Hi..(.....g.bat.....<q..@.....uotpo.....w..X.....ennab.....S..p.....nozam.....E..h...^.....t.....L.....$.....x.....|...l...h...d...`...\...X...H...P...L...H... ...@.....4...0...,..(...$... .....h.....(.....\|.....t...p...l...h...h...`...H...X...T...$...L...H...D...@.....8.....,..(...$... .....p.....4.....|...x...t...p...l...h...d...`...\...X...T...P...L...H...

C:\Users\user\AppData\Local\Google\Chrome\User Data\a43b77ed-0b77-4cb4-a694-e0cc5571ec94.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7444259938311952
Encrypted:	false
SSDEEP:	384:TrMTbJW0t1q/mNfr8vLR30zN0HdQGwPrK1T7xMtpRori/mqNWB/b30OV1jNa13eK:katdChsUcernZVMvrupKnhLpc
MD5:	3A58663620C57967FDB70FF5394492F7
SHA1:	F41DD66DDF1B0C61338FBA3F35B3383E4798E6DA
SHA-256:	C867A7059CF51125A055258542261F04CCEC5FA5079AAE319B903FD5A8D3898C
SHA-512:	CAB308C66CCEFB9E181FD7A41C501A90C83B6825C0FB79FEE5574FECBB8B0E51219A1E54F983D69594E8B442296C471BDB34965F2440908E84C150D7B9CC97E3
Malicious:	false
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...d@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\ab94c602-583b-4ea3-84e8-bf77c1d9965c.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):	368537
Entropy (8bit):	6.028225475414381
Encrypted:	false
SSDEEP:	6144:Te98KWPnuw15QgBBDG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinT:TY4j1igBBDGNPUZ+w7wJHyEtAWW
MD5:	48BB1679ACFA8654C87CDAFD657DEA96
SHA1:	EE4A813D842D40D948426B647F5E5AA724A76845
SHA-256:	E71A8EFE04876A77445502DBDAFA7908A31B38324F924E900570E608E434D5EE
SHA-512:	2CBD8EBB8074FC2E145AEDE22D875FD0C9132C48DD319B8A4E6B559A246A63120FDB3C3D6EB14ED6E0F33C4094C9FF3B2322BB50249A1E4FFD8C4B557FEC228
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626929969265992e+12,"network":1.62689757e+12,"ticks":6861895878.0,"uncertainty":4398782.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488503367"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\d6bf2ebe-3934-457d-8dc9-da5a4eda7bcb.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):	368790
Entropy (8bit):	6.028575277595983
Encrypted:	false
SSDEEP:	6144:+e98KWPnuw15QgBBDG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinT:+Y4j1igBBDGNPUZ+w7wJHyEtAWW
MD5:	46A839608F64C65CE549718026684F1B
SHA1:	DD48ED5E8FA4751D307900BB1EB7F3C3672595E2
SHA-256:	9F1AFE7626E31F317DE9BE633CC66F4E9F685FB12C9E00A5EA34001926F245C6
SHA-512:	65852309F65DC15889D2765FFC42ECC13E541DC5D8C961B0322603A3FBEFE307C30469FA7069C435529E655FCAAA5B3C24B6B7FB5F806484E1711F391BCBCE6
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\d6bf2ebe-3934-457d-8dc9-da5a4eda7bcb.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626929969265992e+12,"network":1.62689757e+12,"ticks":6861895878.0,"uncertainty":4398782.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488503367"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\ee2ee447-5780-4abe-9e57-20af04770158.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.744750194956465
Encrypted:	false
SSDEEP:	384:lrMTbJW0hZ15V1X/mNfr8vLR30zN0HdQGwPrK1T7xMtpRori/mqNWB/b30OV1jNf:AqatdChsUcernZVMvrupKnhLpf
MD5:	9703CCF104BEEF905203E6AD47B5C7A6
SHA1:	26A8ED500A0A4F24AB1408006EA43C2BC2A30762
SHA-256:	B30BB5566061BEDF15D1A2A5BD160FE1A40DDE35C76D41E14918E82A5919A092
SHA-512:	3E3F6A52BF6A5028EFFE6B8D766EC885ECEBE1E11CD34CF4F9A105113FB91DEACF922B76EAEBE3367F299D6BEADC28B6FFC2CBC2895CBA00386EABC9F0BA39F1
Malicious:	false
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...d@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\1d4aece2-b9aa-43b7-85f1-c53daee2ae69.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.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\3520_1374344680\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):	3.9555383032528804
Encrypted:	false
SSDEEP:	3:SQVHFCSAGd2cpXa2WkBUGfg9aRD:SQVnJpK2Woll
MD5:	09C536CD77C00468F2161B9F7A49B716
SHA1:	8705F0371E8AD2E34636ADDE7ED20BC34270A6AB
SHA-256:	81F1F7132F3999597E910FCDBB413A6BED4CE6870FF1858B6602391A9379E62B
SHA-512:	4CE9D9ED2C80D106AA338F60767CCD914679949825D400C340615FBD6EA5CED793F56305476CED45DB0975FCB848C6E19C132793AE6C1A87FBFE6F4223E2E7
Malicious:	false
Preview:	1.5347b8d5fcb6fe52675d2707ccdec8de9ae2fc40413bad18aff220c66a11f44f

C:\Users\user\AppData\Local\Temp\3520_1754930635\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators

C:\Users\user\AppData\Local\Temp\3520_1754930635\manifest.fingerprint	
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\3520_43638511\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.9570514164363635
Encrypted:	false
SSDEEP:	3:SVCBGERJd9WaHpYx4eiXoA:SVCwERJdVMiXd
MD5:	C6ABF42CB5AF869629971C2E42A87FD5
SHA1:	6EB0FAE28D9466E76FA12E31FE6CDADD3ACCE4D1
SHA-256:	D281AFDA759075F4CB7D7CEEC4A3CB2AF135213B4D691F27090E13F238486AD1
SHA-512:	EDDF7E4883E82718743C589E8F2E48BEAD948428E730231FEFADAD380853343332BC56C9DC61C963B3F537CD4865B06FF330CEF012B152CEA35F8A0AA2C7B5D
Malicious:	false
Preview:	1.fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace

C:\Users\user\AppData\Local\Temp\3520_482233905\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.866533712632772
Encrypted:	false
SSDEEP:	3:SpUCQEd2dq8ebEJW2GnnHR:SXQ5Y88EJeR
MD5:	423CB83A2A3B602B0AA82B51B3DA2869
SHA1:	58BC924AF90A89CE87807919F228FE6C915AD854
SHA-256:	0047059C732D70AF8C2F407089237F745838A0FE4F75710ABF1E669B81243E9C
SHA-512:	F80E9B5D544894A667F74CFD0A4D784311299DB080CA6793AABD93B95CF1E2870F74AD38A6386D862580220047F828457240577335C565B7F38B0C6677811660
Malicious:	false
Preview:	1.ffd1d2d75a8183b0a1081bd03a7ce1d140fded7a9fb52cf3ae864cd4d408ceb4

C:\Users\user\AppData\Local\Temp\3520_663501212\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):	3.9265057735423707
Encrypted:	false
SSDEEP:	3:Scy/szkTqhKDKVXGWjGd5n:ScCPqhYKVFK5
MD5:	72AC97F196EAA5A1E6C61113B4931B84
SHA1:	B23CC7C005A3BC6AD1517B9B1CB86E4451E92021
SHA-256:	A51A8D5EF5856EDD33EBDBD68AE67B9F0BDDB6FD3C0256637EA688429C36525D
SHA-512:	3F60837DACB8B20A8E87E432A61D0C59E9D39152167AE2C6D0FFC3CA9DE25C4CC9ECAB4A7FF1762B27F2C53FFD8AFD5B8F519CC8B242E2DD801AC29822275C4
Malicious:	false
Preview:	1.91ee417000553ca22ed67530545c4177a08e7ffcf602c292a71bd89ecd0568a5

C:\Users\user\AppData\Local\Temp\3f04c794-8089-432e-947c-00aced599f90.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\3f04c794-8089-432e-947c-00aced599f90.tmp	
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\50ad4809-31c0-4a3c-9c8b-469f5d2620b1.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\7eca31ac-bd15-435d-ad41-c55750ca56de.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir3520_1534545062\1d4aece2-b9aa-43b7-85f1-c53daee2ae69.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

C:\Users\user\AppData\Local\Temp\scoped_dir3520_1534545062\1d4aece2-b9aa-43b7-85f1-c53daee2ae69.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.....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_dir3520_1534545062\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:	{.. "1018984561488520517": {.. "message": ".....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir3520_1534545062\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
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_dir3520_1534545062\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": "..... .. .., ...".. },.. "1550904064710828958": {.. "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_dir3520_1534545062\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir3520_1534545062\CRX_INSTALL_locales\bn\messages.json	
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:lPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ... .".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir3520_1534545062\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
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_dir3520_1534545062\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_dir3520_1534545062\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

C:\Users\user\AppData\Local\Temp\scoped_dir3520_1534545062\CRX_INSTALL_locales\da\messages.json	
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?".. },.. "1282768764603190 75": {.. "message": "Enhedsregistrering".. },.. "14284488690781267 31": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "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_dir3520_1534545062\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
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "1282768764603190 75": {.. "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",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir3520_1534545062\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_dir3520_1534545062\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:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir3520_1534545062\CRX_INSTALL_locales\en\messages.json	
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chromecast 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_dir3520_1534545062\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:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71EEEE
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_dir3520_1534545062\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:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB11202723566
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".. },.. "1522140683318860351": {.. "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_dir3520_1534545062\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:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF37195
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_dir3520_1534545062\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 21
Malicious:	false
Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "152214068331886 0351": {.. "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_dir3520_1534545062\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
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wIJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C00 0
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-s mooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smoot h".. },.. "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_dir3520_1534545062\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:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51 B
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".. },.. "163 6686747687494376": {.. "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": {..

Static File Info

General	
File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	4.660023280384529
TrID:	• HyperText Markup Language (15015/1) 30.63% • HyperText Markup Language (11501/1) 23.46% • HyperText Markup Language (11501/1) 23.46% • HyperText Markup Language (11001/1) 22.44%
File name:	Convert HEX uit phishing mail.htm
File size:	5215
MD5:	bdcd079a5d19d6e7770c3ed82d71d772
SHA1:	2564b052fc982da1f2baed9c19953f38da140406
SHA256:	0a3ad129462284db86e44bb0ce8d12317915c8fe79d7301f77d774110654461b
SHA512:	67203bc03096bd3cff1b21d223f8a1de8c954e7c91b5edb03574f036f84228ad2504ff014c1d6bdd82df56a461013b89314fd5d569ae3147688c22d53d5fe52e
SSDEEP:	96:sYXGGgG2F850fVpwXFy1mfJYN8+9yTp66yFKb7R:1gG2F850fk0s+N271bl
File Content Preview:	<!DOCTYPE html>..<html lang="en">..<head>.. <meta charset="UTF-8">.. <meta name="viewport" content="width=device-width, initial-scale=1.0">.. <title>Sign in to Outlook</title>.. <link rel="shortcut icon" href="https://aadcdn.msftauth.net/ests/

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 21:59:28.593970060 CEST	192.168.2.6	8.8.8.8	0x7bd8	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Jul 21, 2021 21:59:28.597615957 CEST	192.168.2.6	8.8.8.8	0xc378	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 21:59:28.605595112 CEST	192.168.2.6	8.8.8.8	0x4b40	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 21:59:28.607547045 CEST	192.168.2.6	8.8.8.8	0xad8f	Standard query (0)	i.stack.imgur.com	A (IP address)	IN (0x0001)
Jul 21, 2021 21:59:29.983815908 CEST	192.168.2.6	8.8.8.8	0x1aa4	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 21, 2021 21:59:31.415635109 CEST	192.168.2.6	8.8.8.8	0x1f51	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 21:59:28.618657112 CEST	8.8.8.8	192.168.2.6	0x7bd8	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 21:59:28.618657112 CEST	8.8.8.8	192.168.2.6	0x7bd8	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Jul 21, 2021 21:59:28.628645897 CEST	8.8.8.8	192.168.2.6	0xc378	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 21:59:28.628645897 CEST	8.8.8.8	192.168.2.6	0xc378	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 21:59:28.629623890 CEST	8.8.8.8	192.168.2.6	0xad8f	No error (0)	i.stack.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 21:59:28.629623890 CEST	8.8.8.8	192.168.2.6	0xad8f	No error (0)	ipv4.imgur.map.fastly.net		151.101.12.193	A (IP address)	IN (0x0001)
Jul 21, 2021 21:59:28.642524958 CEST	8.8.8.8	192.168.2.6	0x4b40	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 21, 2021 21:59:30.010767937 CEST	8.8.8.8	192.168.2.6	0x1aa4	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 21:59:30.010767937 CEST	8.8.8.8	192.168.2.6	0x1aa4	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.65	A (IP address)	IN (0x0001)
Jul 21, 2021 21:59:31.428306103 CEST	8.8.8.8	192.168.2.6	0x1f51	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 21:59:31.428306103 CEST	8.8.8.8	192.168.2.6	0x1f51	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 21, 2021 21:59:28.684952021 CEST	151.101.12.193	443	192.168.2.6	49718	CN=i.stack.imgur.com, O="Imgur, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Oct 19 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Nov 20 00:59:59 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jul 21, 2021 21:59:31.483025074 CEST	152.199.23.37	443	192.168.2.6	49734	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 21, 2021 21:59:31.513005972 CEST	152.199.23.37	443	192.168.2.6	49735	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 21, 2021 21:59:31.586890936 CEST	152.199.23.37	443	192.168.2.6	49736	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 21, 2021 21:59:31.655193090 CEST	152.199.23.37	443	192.168.2.6	49737	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 21, 2021 21:59:31.716618061 CEST	152.199.23.37	443	192.168.2.6	49738	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 3520 Parent PID: 3940

General

Start time:	21:59:23
Start date:	21/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\Convert HEX uit phishing mail.htm'
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 6036 Parent PID: 3520

General

Start time:	21:59:25
Start date:	21/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1632,14357687303338385437,9119543046795049864,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes

MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Disassembly