ID: 452646
Sample Name: Payment Copy for Inv ps-7 -USD 24,806.PDF.htm
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 17:19:52
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

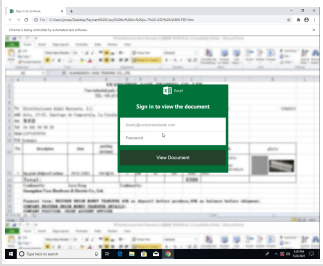
Windows Analysis Report Payment Copy for Inv ps-7 -U…

Overview

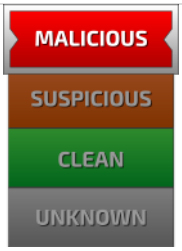
General Information

Sample Name:	Payment Copy for Inv ps-7 -USD 24,806.PDF.htm
Analysis ID:	452646
MD5:	49132b4f0d2418a.
SHA1:	619827a6c71125..
SHA256:	24405ff6000d280..
Infos:	

Most interesting Screenshot:



Detection



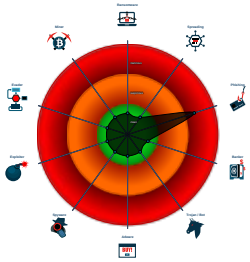
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Yara detected HtmlPhish10
- 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…
- None HTTPS page querying sensitiv…
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6740 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'C:\Users\user\Desktop\Payment Copy for Inv ps-7 -USD 24,806.PDF.htm' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6896 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,11699132993908980424,10170989427665474543,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Payment Copy for Inv ps-7 -USD 24,806.PDF.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

AV Detection:

Multi AV Scanner detection for domain / URL

Phishing:

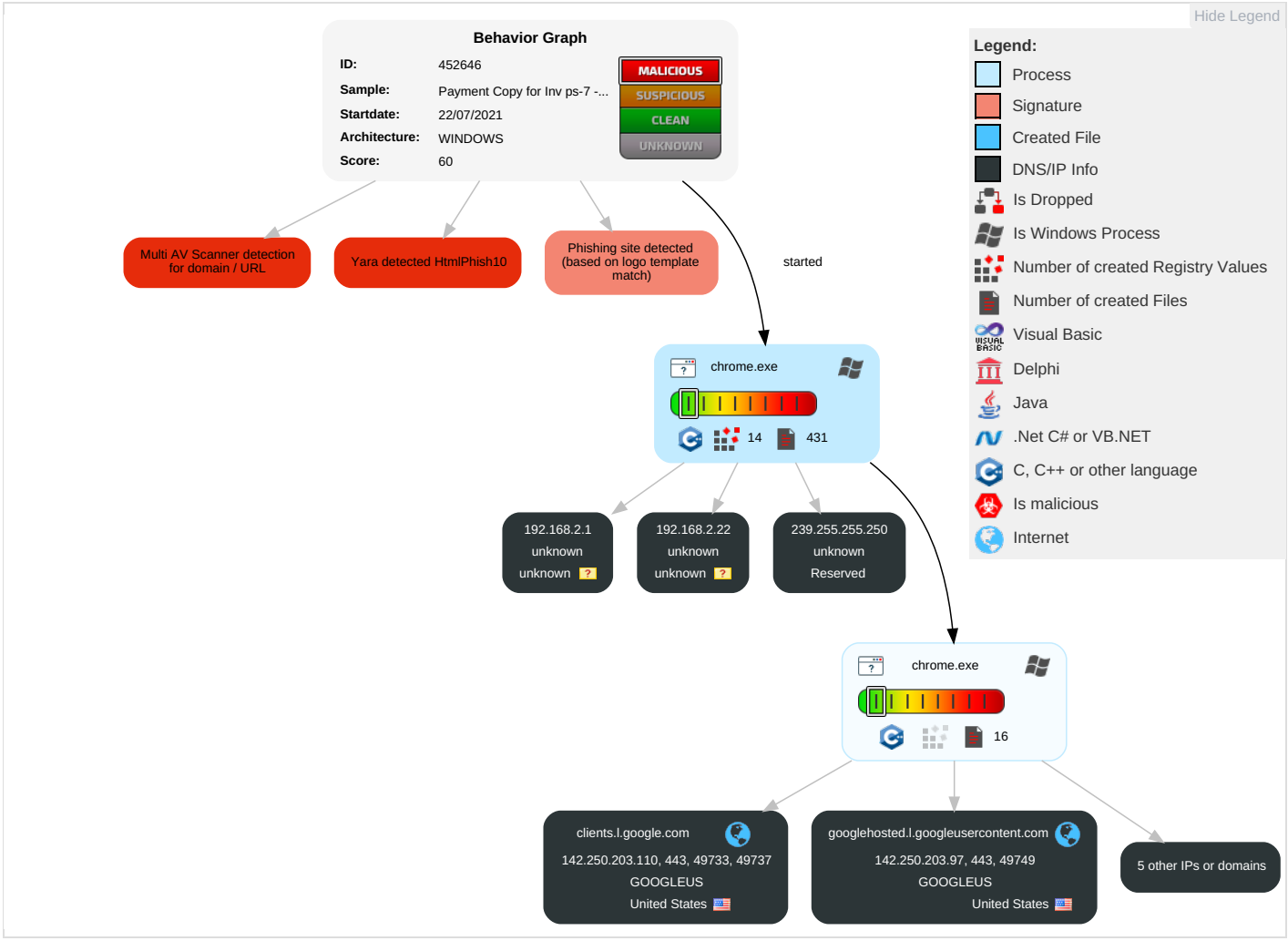
Yara detected HtmlPhish10

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

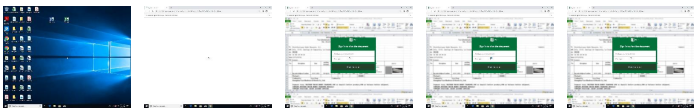
Behavior Graph

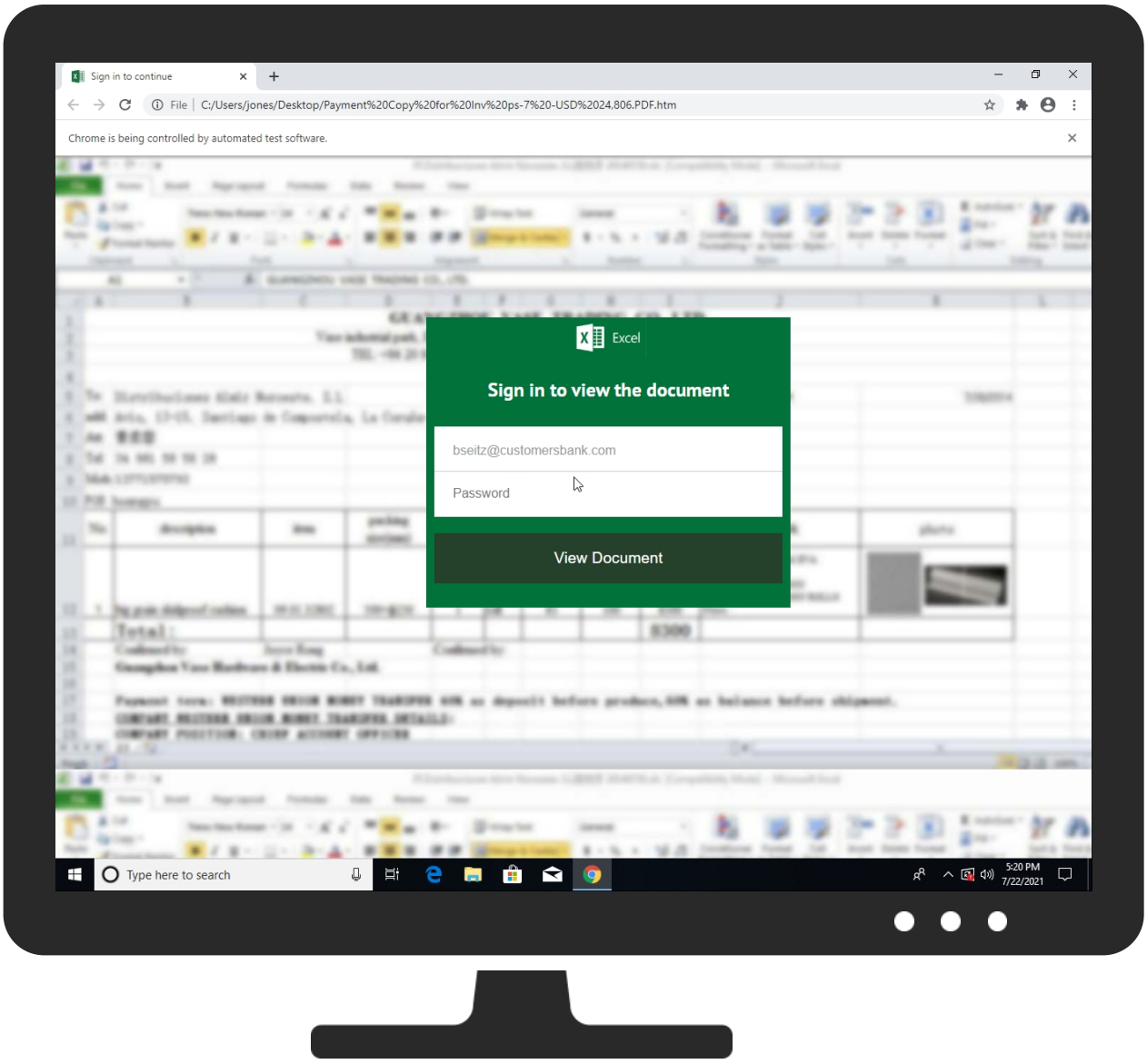


Screenshots

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

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://erandibermudez.com/wp-content/themes/opo.php	8%	Virustotal		Browse
http://https://erandibermudez.com/wp-content/themes/opo.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
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	142.250.203.97	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/Payment%20Copy%20for%20Inv%20ps-7%20-USD%2024,806.PDF.htm	true		low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
192.168.2.4
192.168.2.22
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452646
Start date:	22.07.2021
Start time:	17:19:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Copy for Inv ps-7 -USD 24,806.PDF.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:	mal60.phis.winHTM@33/175@3/8
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	MD9ymCl9vY.exe	Get hash	malicious	Browse	
	DCBR.msi	Get hash	malicious	Browse	
	#U00e2_#U00e2_Play _to _Listen.htm	Get hash	malicious	Browse	
	Westernunionreceipt711 ___vaw.html	Get hash	malicious	Browse	
	Remittance.html	Get hash	malicious	Browse	
	DHL Documents.html	Get hash	malicious	Browse	
	2DAAD8278E0DDD4D247303ACED4B1D41C75CE94BE3A9E.exe	Get hash	malicious	Browse	
	Convert HEX uit phishing mail.htm	Get hash	malicious	Browse	
	#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	

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\0768db86-36ba-4991-8d3b-54d53143fc73.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):	166088
Entropy (8bit):	6.049965612449309
Encrypted:	false
SSDEEP:	3072:l9WW4u2Vl2CViqRnjUkQJUwYMrwjYUEDt5HCzSFFcbXafIB0u1GOJmA3iuRx:8zH2aHRnjOJYMrw8LCzSzaqfIlUOoSic
MD5:	77B3774DBC7447A0109A62DE5A64C487
SHA1:	7EC237AEADAFCF204E189019CEFE132B03534255
SHA-256:	F3A57377878C5AF08E2B375F51DFE92B8AAE5B429194B0BA4BC142F6EB1026A7
SHA-512:	F420B93F8785760CEEFFF1E32B626455ED117E710FCAB1113EDBADE0E5C96A802C8B944FEB70FE41BD04A5B270A8A754F4BAE457828836A4648E19F611DBA34C
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626967244619998e+12,"network":1.626967247e+12,"ticks":4769258237.0,"uncertainty":3937570.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715636091"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\27ca25fd-a596-4fde-bb03-bce2c5baf858.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):	166182
Entropy (8bit):	6.050241783957279
Encrypted:	false
SSDEEP:	3072:19WW4u2Vl2CViqRnjUkQJUwYMrwjYUEDt5HCzSFFcbXafIB0u1GOJmA3iuRx:MzH2aHRnjOJYMrw8LCzSzaqfIlUOoSic
MD5:	458F22F975FE8D7E372FE7980CFFD182
SHA1:	0843DCBC13598BB2442D009BF81BBA9FC1A8364C
SHA-256:	97DD73A265AA789DEDED82578D0AEBF87BE07805FFC4F903C500889155C4B966
SHA-512:	A2D0BEB5AABE67436F018392949CD545A13DDC5763023C4BBECB676434E1DD288034F9A08A6416D17D66B69A7E465E235E7F470CD60C04B5522A87321B378B3
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626967244619998e+12,"network":1.626967247e+12,"ticks":4769258237.0,"uncertainty":3937570.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715636091"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\3100b87c-c6c1-44b4-88aa-2603b8e5487f.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):	174555
Entropy (8bit):	6.079389433967097
Encrypted:	false
SSDEEP:	3072:zv09WW4u2Vl2CViqRnjUkQJUwYMrwjYUEDt5HCzSFFcbXafIB0u1GOJmA3iuRx:LhzH2aHRnjOJYMrw8LCzSzaqfIlUOoSf
MD5:	DB767EE36AB529E071ED9B5EC99455F5

C:\Users\user\AppData\Local\Google\Chrome\User Data\3100b87c-c6c1-44b4-88aa-2603b8e5487f.tmp	
SHA1:	0E892DDFD7763CA7B9029BEBA7027115FEE551FE
SHA-256:	2646646CE798BD2A9AF2AB55A95FF7EF362DA7EFDBEDD4F4224FD8F0F466F8F9
SHA-512:	0068A3070F2968043F6510DFA41FBF5150E739CC6ECB171138CFB54AEB74DD721BB997E1F70B543D57F577A82404A38A93A6229738D08E32D8EF0657C21D74C7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626967244619998e+12,"network":1.626967247e+12,"ticks":4769258237.0,"uncertainty":3937570.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\4a508aa4-a246-4e2d-88b3-0b5f7c1356fb.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):	174555
Entropy (8bit):	6.0793879489467635
Encrypted:	false
SSDEEP:	3072:Sv09WW4u2Vl2CViqRnjUkQJUwYMrwjYUEDt5HCzSFFcbXafIB0u1GOJmA3iuRx:qhzH2aHRnjOJYMrw8LCzSzaqfIlUOoSf
MD5:	D52DE4413A0763111E85DB2D71DA58FB
SHA1:	0298A04FFD6225D25A94BC2B05749834DE099116
SHA-256:	C82E22C17CE4ECFBFA8073A6D45F3CC8818B16774B3C9CDEFC8B752DBFD7A9A6
SHA-512:	2E8066941642A83995F919BFDA0F1B837565B630744DD04D23F84912772CC0B8077A17FBF836844BAC3DA9BD15475ACF77C1533517342A6395FFA43553401B68
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626967244619998e+12,"network":1.626967247e+12,"ticks":4769258237.0,"uncertainty":3937570.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715636091"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\53963be9-2789-4f9a-93b0-dc9338857ce8.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):	174555
Entropy (8bit):	6.079388634999904
Encrypted:	false
SSDEEP:	3072:z4E9WW4u2Vl2CViqRnjUkQJUwYMrwjYUEDt5HCzSFFcbXafIB0u1GOJmA3iuRx:cxzH2aHRnjOJYMrw8LCzSzaqfIlUOoSf
MD5:	115A21FCE2DBF59D36AEF64CF1725EC7
SHA1:	64A94D1E35953DAA2B9829738300E1B0B799F72F
SHA-256:	54848192DE6D1FAC4FC48FD760B64B0922D6E429EB861C940CDBB1639939CF4B
SHA-512:	390FCE61485EBCBB40507EFEA43486F9D2D13350025DB51ABE00574CD7FB76093C48DA796B0EDA35E4DCA9BFE050E7147D47147B0E2B616F918E23DFE2E9F29
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626967244619998e+12,"network":1.626967247e+12,"ticks":4769258237.0,"uncertainty":3937570.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\609af24a-6e8d-4152-ab17-9ebc8259ecc9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7434171232364073
Encrypted:	false
SSDEEP:	384:x3ReWoLRc70KVDlqNNGrDvai3py8BHMpGdErf8agxRMQEzrLamHMPMuuSNOUAuNj:5emxpy8dVgeXsGYofX2SKkCOhH
MD5:	0EA45A0262018D1EE4EACD8B14F3C7C3
SHA1:	7BD31E15325235A1B10E7CA64298505742B54ECE

C:\Users\user\AppData\Local\Google\Chrome\User Data\609af24a-6e8d-4152-ab17-9ebc8259ecc9.tmp

SHA-256:	AD39D510C9AF7565EE436EEB25DEE948B7AACB8D8E4D089F94EDD817B0877970
SHA-512:	F1C408F28EA7BA407F1B11AE18AE4439EB6C4FF0A9BC66774AD0DC59F72DC70EFF9B974C741A5E9985D1C0A71CE06EA1FE4F4979CDBD817CD94D195ED21AA3CD
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...o@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\86a38742-6bdc-4202-93a2-9407ddf9034f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.743019451231429
Encrypted:	false
SSDEEP:	384:33ReWoLRA0jqNNGrDvai3py8BHMpGdErf8agxRMQEzrLamHMPMuuSNOUAuNP1ena:7mxpy8dVgeXsGYofX2SKkCOhJ
MD5:	9152D483D9AE990A4B81018679FCF2E0
SHA1:	76B3168A72CCF4CF271F0AE6F135AA88D86A2B68
SHA-256:	D51574C27C3330261873494C12E2BFB9543CBF980A83211B68896A4287E7E605
SHA-512:	18B0BE276C43CE271E795F47F13D2291F218E2D40CB6C908E5429822861AE8866E6C7487CA307DF7A4E57B355E3CCB9B8D66EA0B8F85B05A7A1C2790A001A8D
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...o@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\Crashpad\settings.dat

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ce4c3f7-b691-4228-b575-f5998eda2cea.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ce4c3f7-b691-4228-b575-f5998eda2cea.tmp	
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3605cfde-f1d0-441c-95dd-901d085239dc.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):	19010
Entropy (8bit):	5.5672942685221845
Encrypted:	false
SSDEEP:	384:GDEtzLlejXP1kXqKf/pUZNCgVLH2HfD0rUrHGsh84J:pLlAP1kXqKf/pUZNCgVLH2HforU7GC82
MD5:	E5DE7FEBABA35AA81ABBDBE28CF26123
SHA1:	214BE1EA7C1FBF7E8151A6EBA1FDCB3143CC65EA
SHA-256:	8E9043B10983A99AE6541EFA876D62FAFBDF9B816F4D195F4541CC60CC047EDA
SHA-512:	0134062DE917E0D670845EE9706AE5AB3AE93A1AB6F449DC6CC0B1DFEA2EAC6562E5DFD88AB6FAE20F1F6EDDC58FDDA8D512DFAEB1767019C17FBEA0F641 7A6
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":"13271440841678315","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ae11929-9a83-46c4-95cc-340980071b9f.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):	5464
Entropy (8bit):	5.148606729554996
Encrypted:	false
SSDEEP:	48:YcPkKSChkligqArdqx58oQQf2H4lYGlQKHoTw0Orf4MqM8C1Nfct/9BhUJo3KhmR:nHLn4MxXQgIKIw5k0JCKL8bbOTlVuHn
MD5:	CB9A1678E8C84C88C619E707F334868E
SHA1:	5558C42A96EA9310754A6AFC9F3DAE53B3CAA031
SHA-256:	8E4EAA8EF6F40EBB55CE38D9C09BF9E1DAFCEE3BE9424EA54B4975CD608696E3
SHA-512:	727F1AD7152A5E2BE366C55A19D35DA408A7A6E6C218F6F9D7F29FEB01945225816B8E63B622FFB9BB3D1A503C18DA1FE3FEC0C173B95CC295CD92E97453CE D
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271440841945842","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4b52a989-4339-4a29-af16-872aba1db11d.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):	1040
Entropy (8bit):	5.572670458459364
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSTG1KUeiXzkq/HeUe8zUe7V7wU+LpRUeiQ:Ym6UUhyKUeiYqPeUekUeZwUQPUeP
MD5:	11D4EB883417582388A1E6F2EBAA58B1
SHA1:	C81064B3394172356887E9FC0A3397EC466253A6
SHA-256:	99FFC1C139E90684AAA0E8EBE509387D5F588D8D09F1539B6E7E909F9C4E86EF
SHA-512:	1E71F787FBF94D3642F6940D4BC26EF41A8448AE610096B73815131B3C5CD019F3EBD36E75671E689261AF0F3BE06C5E3AC684A4BD924ED1BFFE749F31D7457
Malicious:	false
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1658503245.984746,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626967245.98475},{"expiry":1632986995.164829,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\54874e1c-cb5f-407d-9af9-e7eb805591f8.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):	1756
Entropy (8bit):	4.851237683614485
Encrypted:	false
SSDEEP:	48:Y2nzMK6qDHGXCtwWs9RLs1AyKsd3zs5MHHOYhbw:JnzMKxDHGXCODdooGDhM
MD5:	2C305D6C282AE97FBF0C4CCC44D0BD1E
SHA1:	B5D4183BE166F3565C6EC2BFA13C73CF70357C90
SHA-256:	D8C5CC822DFA1A29C38AED08698BB2117FB888319BC70F6DA68C713257D8DB7C
SHA-512:	1225F274DABDB82A7175CC62F9852E3C5D5F096A2FBA00FB73FAD6342FA054406EB354959392B6886A123D9575298EC9C5FDFCE0BFA1000E7771C17571AB9EC
Malicious:	false

Preview:

{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13274032845984631","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6b6894c5-25ba-4a10-99c1-e53a5fbc0a1e.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):	5490
Entropy (8bit):	5.152178217717677
Encrypted:	false
SSDEEP:	48:YcPkKSChkliJMzqArdqx58oQQf2H4lYGlQKHoTw0Orf4MqM8C1Nfct/9BhUJo3K/:nHLz4MxXQgIKIw5k0JCKL8wbOTlVuHn
MD5:	F28C0EC45B658756F0EDE0C8BA36F57F
SHA1:	5B5CF842B62AC4F87F6098D278D76A663C9D66FA
SHA-256:	9A30B96C6214EFD55752C98391203F7C0FF8E58EAD005F6025B9381AE76DC0A4
SHA-512:	31F312874067272285C8A7745A52CCB219C2060AB658EEB21FD3AC15CCEB8F48DD887378D3BC94608E339CCEB4C56542965B29C841CB6B7FCDE71B6A5EF2C6C
Malicious:	false

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13271440841945842","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\82436d81-54a7-42df-8b43-1577f2b8998f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22602
Entropy (8bit):	5.536341798637953
Encrypted:	false
SSDEEP:	384:GDEtCLlejXP1kXqKf/pUZNCgVLH2HfD0rUrHG4nZ6B84U:4LlAP1kXqKf/pUZNCgVLH2HforU7G4nD
MD5:	CFCDA7102A917BCAF1E48E6CB934AC2B
SHA1:	54E03A502C87664B6764DCDE9F5064F66701B784
SHA-256:	96F46E3415EBA64ACF28E4408CA4C6514B2942FF5CD6EC8D6AE2157C1A454E60
SHA-512:	DD1F573BC1FB3F7B9D3FDD3624856EDA6DC9D9F23A43547A411C73F21C66E19B1282BABF3E5331F3AFCF6D357DBC0F69AED828E984F4D4754F9E666764B8637
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":"13271440841678315","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\841ae51d-8533-4c0b-9724-3c789d6eb6cf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22601

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\841ae51d-8533-4c0b-9724-3c789d6eb6cf.tmp	
Entropy (8bit):	5.5363702548281
Encrypted:	false
SSDEEP:	384:GDEtCLlejXP1kXqKf/pUZNCgVLH2HfD0rUrHGfnZ6Z84u:4LlAP1kXqKf/pUZNCgVLH2HforU7Gfn5
MD5:	F7267162FD290FD8A0392778D3962492
SHA1:	6A78D09C0DEF2776840C08A3F4EEF5A2C09BCF3B
SHA-256:	37A46BED8E697E34978D8F5CE88E84B95402559C390A4D5C188FE9DDB1C844C8
SHA-512:	65AC59E7302B856DD6740092029C8953A47D4B1069360AB98C6B2AE3A2204B6E93C85586B4C9AA340BCA872FBA4689DD3D9F231CCA90E323772E4BFF0DD9361
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":"13271440841678315","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.192635466546377
Encrypted:	false
SSDEEP:	6:mBdypQL+q2Pwkn23iKKdK9RXXTZIFUtpcdd+fG1ZmwPcdd+fQLVkwOwkn23iKKdi:MIpQ+vYf5Kk7XT2FUtpcfmG1/PcfmQVz
MD5:	485543C3101F99746255316FF1D5FAA9
SHA1:	AA5E45B54EE92F71115DFB81EF51BD8BA4C17D74
SHA-256:	3762C86421B1F1182F9EA10A285890283DADAF700EE699FA1B55ADE994FB13F5
SHA-512:	EEAE99167BFAAA189763F85CC3AB7BC45D21C6867BCA58BE8C30A805B2827F97EA6233C893ACF8F376D3AFCA9D91EF18597BFAFF04DAC06812C0EA3282048661
Malicious:	false
Preview:	2021/07/22-17:20:51.877 1a9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/22-17:20:51.882 1a9c Recovering log #3.2021/07/22-17:20:51.882 1a9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.230590181602155
Encrypted:	false
SSDEEP:	6:mBdRv9+q2Pwkn23iKKdKyDZIFUtpcdGxJZmwPcXe39VkwOwkn23iKKdKyJLJ:MTv9+vYf5Kk02FUtpciJ/PcY9V5Jf5K1
MD5:	3AED8F508C063B03071EDFB0C26A4CBE
SHA1:	BCB6418067D4DDE165169C3F64091EEF69D6FDCF
SHA-256:	6DBD66D33D4B975D426937D457BD6E433838BACD7D742A5212679283AC152B4D
SHA-512:	849002FE80B3004522E9E6F0E6B61704B6B0622BE7BA694FA1AF89FF4DC3FB0012F23128EC9ACA6812016ED1FBD76E6E6590652CB37381FDBC28F4D453555940
Malicious:	false
Preview:	2021/07/22-17:20:51.842 184c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/22-17:20:51.852 184c Recovering log #3.2021/07/22-17:20:51.946 184c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9737335394851427
Encrypted:	false
SSDEEP:	24:ae9H6pf1H1oNvaqLbJLbXaFpEO5bNmISHn06UwW8:abfvoNSq5LLOpEO5J/Kn7Uh8
MD5:	AACAF9957471B76CFF9477D5871EEEA8
SHA1:	A3E1DC3C27859E5A8F60B584EBA8E95A3CCA864E
SHA-256:	479E89EA6649DC1CC0EBF3B4C71251B56C0CF0FE5B3A9896599AB832558596D2
SHA-512:	B164588BB1321CDE759927C3F81828E53E578610271CD3232B09EB858583026D1E6EC98E49D83F2192E30F4B550063FA37D3C9F168CDEB9667E72601F075768E
Malicious:	false
Preview:	....

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):	2427
Entropy (8bit):	3.5981112564460083
Encrypted:	false
SSDEEP:	24:34SkHvxlrlJlpwXNlYnqssgpwXOxpwXrH07Zn1UqssFCLrGKPwlY6jb6bpwXOF/:34xjxpGNan5GEGrUzUbrltNGA
MD5:	612579D0DDEB013CD95696A2DC01C36A
SHA1:	587A84EF465FD6F4DF633ECBA32DF0609C64906C
SHA-256:	BCD222E719F6E157B3AEA520C3EEBC8003D824C25E2166E2A8207FC67A13E102
SHA-512:	AA858C83EB8EEE6B52993EF438346248391001DB05CD1743EACD5992A4DF9D2C350E978353C7080EA24A4BC766A28A2203E71A12BFAF668940D8A7797B09C334
Malicious:	false
Preview:	SNSS.....!.....1.,.....$...b6299f93_1cef_4a2a_b050_9ba44b908f5e.....|..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....X...file:///C:/Users/user/Desktop/Payment%20Copy%20for%20Inv%20ps-7%20-USD%2024,806.PDF.htm.....h.....`..... .....X.....p.....X...f.i.l.e.:././/.C.:./.U.s.e.r.s./.j.o.n.e.s./.D.e.s.k.t.o.p./.P.a.y.m.e.n.t.%.2.0.C.o.p.y.%.2.0.f.o.r.%.2.0.I.n.v.%.2.0.p.s.-.7.%.2.0.-.U.S.D.%.2.0.2.4.,.8.0.6...P.D.F...h.t.m.....8.....0.... ...8..... .....X...file:///C:/Users/user/Desktop/P

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.206307547580614
Encrypted:	false
SSDEEP:	6:mNYklL+q2Pwkn23iKKdK8aPrqIFUtpKm1ZmwPKwLVkwOwkn23iKKdK8amLJ:cIvYf5KkL3FUtph1/Ph5Jf5KkQJ
MD5:	3AE373B82609560497DDB45AE2F9607D
SHA1:	A4D6F917C57DED0426E00C34AF1B4D127E186C3A
SHA-256:	FFFD3E12F93C01B6C63402EB7F57C5D4843D84FF77015746D0EF5A1E14575A40
SHA-512:	F664BC9BE012EBFFB60A810326CD78761ADCD6FDD0A7C1C5FF682E07CC852F1135A2C39C70D95C018621291B5A7C5673048587CD70416124AA0ADEC1177551
Malicious:	false
Preview:	2021/07/22-17:20:41.952 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/22-1 7:20:41.953 1a98 Recovering log #3.2021/07/22-17:20:41.953 1a98 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.191182449016886
Encrypted:	false
SSDEEP:	6:mX/4q2Pwkn23iKKdK8NIFUtpkJZmwPEIvDkwOwkn23iKKdK8+eLJ:u4vYf5KkpFUtpkJ/PEIvD5Jf5KkqJ
MD5:	A92A052CCA43BEC8447CDFEBEC227049
SHA1:	EB463AFBC22A9A2870A9A1487418E1B263205B21
SHA-256:	3EF150A4CCA5D9A398DBCC8E43E78FE129F7E663B817B9BC02C02827B66F5C1D
SHA-512:	62D4BCBBC608B4C7259EA298F6F98A1FACCD2D0F673CFE2F03DD434190454170427EB8068177671FAC6F18FC43CEBFBA91F0A7C1D8B84FE5E1B6177033507C 7
Malicious:	false
Preview:	2021/07/22-17:20:44.353 1b20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/22-1 7:20:44.355 1b20 Recovering log #3.2021/07/22-17:20:44.356 1b20 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","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:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	174080
Entropy (8bit):	5.627924866637524
Encrypted:	false
SSDEEP:	3072:vHBbzmh7SW8r5tIvQzHu+Cgt/TzIr7Ss1aZRtuvQ/VuECc:vHFo+VtIvmO+CgtLM+satuvCUECc
MD5:	1B62FB35F8E884CFD0FBD3EA6801A66B
SHA1:	3622D836BAC4A1C6CF6A230CB9946E87F8408897
SHA-256:	064A165CB5B03E89E0C26BC021F5090AD63E049887B1ED94E8A561EA3DF533C7
SHA-512:	16AC4726585C7746CD9BF47DAD3170398EE1416BA18C374C038D2B1FDB34CD6721ED26B7FFB4475676236DC594EB9B8FA099CD36BE61C87DF9310926E316A19
Malicious:	false
Preview:	....qSSsIQtkgAxbO/L6gtEEBSVIIii2AZ6sVvtc69nztzxjL0MOnfOnMnMnFnv9Lnd1263btvlitJAu3SjtrIj4K644Ya7LSpEksIEUsv7mz8qBYFmSareSqrq/XzO6QayFMkTTleah+/vKQEAAADYA2uu3Li6f7y0a6nNWtMqJe0kxyfpkw5PVEr+6Ed/ccN/lQQAALCQ9IsAAAAA2N3at1xyYP/4zlZNo1lrbZWkXZPTMpFltdQkSSlyAgAAYPFRoAMAAECPam3eNPDQttFj+8pku6Y0a2qrpLQzNnZEJyXJVFleRQUAAECPUKADAADAYrf5/P612/rX9qXRqiXtpDaTtLaPbj2hUdKomTonL3FWDgAAQG9ToAMAAMAiMv38eielnU5tlIJadTSnp2RpdUsOAAAAT0uBDgAAAAvQ+jdevGJsYPLYvtpp1ZR2LaVZaj0lY2OHdqYvyUtRmQMAAMBeUKADAADAfLb5/P612waP7yudZk1pTT+/PpGJExs15dHn16uqHAAAAGZLgQ4AADzxJorN65eMl6bnUZp1U7ajZJmHU0rpTM0VY8ryQEAAGAuKdABAABgHzv6Tecf0OjrP6mm0ay1tmopzdR6WpnIqk4pSU12/QEAAADYhxToAAAAMEfab2gvuX/ZquOmn1+v6bRLSjPJMZ2aRytyz68DAADA/KBABwAAgC5Yc+XG1f3jpV1LbdaaVqOkuSU5qZHO4PTz62XXXjkAAAAwPynQAQAAYC+sfcslB/aP72xNP79eknYnObVMZKSWXRflnl8HAACABUmBDgAAAE+itXnTwEPbRo/tK5PtmtKsqa2S0s7Y2BGdlExX5DVxVw4AAACLhAIdAACA3rZpU9/aIx88qi+N1vTz66WkvX106wmNkkbdVY97fh0AAAAWPwU6AAAAPWP6+fVOSjud2iyltGq2np6UpTWPPb8OAAAA9CYFOgAAAIvO+jdevGJsYPLYvtpp1ZR2LaVZaj05Y

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

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):	19552
Entropy (8bit):	0.734638530918797
Encrypted:	false
SSDEEP:	24:cyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6UwmC6JXN5lglQgN4:cCBmw6fUl7qR4
MD5:	118C2245D040D92584D89EC63DFEF8DE
SHA1:	E95A68AA97AE5CB87C3E3185BF772C765FC79091
SHA-256:	D29CC2FD81B4FF2F8C339A2DA2F7BA086E94DE28AFA43A4AFB00F22761AC146D
SHA-512:	B589BAC0CD0024628AEA93DC02F2948E56E24BAA55242FCCDBC4A5C2DADA19CF92DA4D70835E6CC10A961C00B8C7A6A1C6DBCFC65CE5B96A4E95758D9700EE3
Malicious:	false
Preview:	.....E:.....SQLite format 3.....@ .....C.....g....._.c...~.2.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.255881374598068
Encrypted:	false
SSDEEP:	6:mBdqpQL+q2Pwkn23iKKdK25+Xqx8chI+IFUtpcdTJsG1ZmwPcdTDQLVkwOwkn23U:MuQ+vYf5KkTXfchI3FUtpcPsG1/PcNQy
MD5:	BDF396424D701FF198D1E270C9B917BC
SHA1:	A34F016853382BEEEF4792F74417146BF24F525B
SHA-256:	59AB3340BE2584C3B94E03E40FD772497FF9666988DC7FE448BC3956D2115996
SHA-512:	F821E6EF38EF32691C7432994FCD3CBC06A29DA1850BAD0ABD0C2FBB6447BE1E3A401C38BA20D310564837F28DAE495D398DE08503E44F289409ED03BDDBA7D
Malicious:	false
Preview:	2021/07/22-17:20:51.859 1a9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/22-17:20:51.866 1a9c Recovering log #3.2021/07/22-17:20:51.867 1a9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.2032380061102055
Encrypted:	false
SSDEEP:	6:mBdXyiQL+q2Pwkn23iKKdK25+XuoIFUtpcd7cpG1ZmwPcdtQLVkwOwkn23iKKdKl:MbQ+vYf5KkTXYFUtpcqpG1/PcLQV5JfR
MD5:	0B627EF76B968A9C0D748EAFAE6D3A88
SHA1:	BECE3E6F33E33AB09BBBBD1940DBF8578F3F0729
SHA-256:	5465009DD8C9ED667AC5D4D2125B503D6160CEA91485DEAE01AE0403AE68A3F5
SHA-512:	281C1F2DD29A6710238080D4478BA90E6D3A97712A8863C36C849B2658A80172F8A9DBEFC1763A987A657040158509E0F8209199A444A860F243B0391FBED1DD
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Preview:	2021/07/22-17:20:51.825 1a9c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/22-17:20:51.835 1a9c Recovering log #3.2021/07/22-17:20:51.836 1a9c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.224773095469653
Encrypted:	false
SSDEEP:	6:mBQ39+q2Pwkn23iKKdKWT5g1IdqIFUtpcSNJZmwPch9VkwOwkn23iKKdKWT5g1Iu:Mi9+vYf5Kkg5gSRFUtpcQJ/Pch9V5Jfz
MD5:	D7CED7AB4069FED6B9225BA72256DDC3
SHA1:	8099697E33BB5740D6AEEB0125CA1FBC2522FE16
SHA-256:	9A19EB1F1D64D0B4E8EAA982D277B3E8F1805E864743868EA389A9696EFCC913
SHA-512:	7375C43858EE568077DA802ABC6AD8E399B74B3D120C4B27F58BDCE889C254DFF5B4A5E17F24600B51AF683E3341FDEFDA56C194BCC7BE4347109E64FD7559E A
Malicious:	false
Preview:	2021/07/22-17:20:51.706 184c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/22-17:20:51.731 184c Recovering log #3.2021/07/22-17:20:51.732 184c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.14543492070777359
Encrypted:	false
SSDEEP:	12:TL+A/gyBfwXRwlxNvHNuQuGI/2n6CBfwXRwn:TLxgypwXExxtuu6CpwXG
MD5:	329CF6685694677BCB95B9DF2D1916E0
SHA1:	0F987421EBB0F393DF9F10B445B096F2158E3014
SHA-256:	67A8594682E392F9DFAC7A0728C52B03B2BAD44473E175D09C493B17CF210B49
SHA-512:	831C2A79918E0E607356E6ACD90620F1E409459953EA7139C255253AA1ADF9D1AF0B9AF927CD214C6C760BE56DC424F03D2C457A794CF5615506940BBFCEB1D
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):	978
Entropy (8bit):	5.337752391096668
Encrypted:	false
SSDEEP:	24:PbQMOnTTQpN4t9e8fs7McyoBK7uGY78BJgskfa9yBDOxo7nQBrxzkcDpwXnaBl:zQvnTE/6XfsioVQU8JF7GaBl
MD5:	1179EB6DF624264F9C06AA832855DA7F
SHA1:	2B8CEC11DDA87F3CEB436C19246E7C825EF64CF1
SHA-256:	5EA3509352D8C4A0B2A6EF22DA6692AFD1803BBAF72E212D93088341E812A4F8
SHA-512:	EF1DCBF686AF4AC8BCBA0A9F9BACF2570CBE9DE70EE08480897544A8886F060E93C61CBB2BDE5557DC963FAC5729C8EA447B2E77D0C86F5A405670B4FF9C902
Malicious:	false
Preview:	....."q....24,806..7..c..continue..copy..desktop..file..for..htm..in..inv..user..payment..pdf..ps..sign..to..usd..users*.....24,806.....7.....c.....continue.....copy.....desktop.....file.....for.....htm.....in.....inv.....user.....payment.....pdf.....ps.....sign.....to.....usd.....users..2.....,.....0.....2.....4.....6.....7.....8.....a.....c..... .d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....y....:..... .....B..... .....*Xfile:///C:/Users/user/Desktop/Payment%20Copy%20for%20Inv%20ps-7%20-USD%2024,806.PDF.htm2.Sign in to continue:.....J.....',047:>EI.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Entropy (8bit):	0.11677519904524104
Encrypted:	false
SSDEEP:	12:ccyqLBj/5r3lCTq4nMWQASjG9LKbBQZ8fOC:uqLB93Yrf1NKbTf3
MD5:	90F675224FFC0B9E307B628337C9657E
SHA1:	D4B75B2F2AB250BBF21CE71CA8384A60B06EAC58
SHA-256:	3AB875D88C4E53BDCC449B186686BA7C5939174BE77F9BA780DCA0E9F2C4BCF0
SHA-512:	3F119EBC1A3FBE731FAF21EA74BF7D2EBA75B74F183AEF765ED28FBA307AF59FDB5BCE972FCD9F27DD787615864E6F36FC829F7A1E8B024DD6AA744F0759F46C
Malicious:	false
Preview:	.....37..... ....

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):	5.458726967963783
Encrypted:	false
SSDEEP:	48:xEDCG0Va7jMi8dbJLbGbQSefgGrNrS0U9RdiN9k:Pa7jMhdbJLbGbQ5fgGZrS0+
MD5:	44BDB351CD11FDA5B3C061F46F6C7D6E
SHA1:	BC1A70AF3BFB4D041FEDB1280001D8AC915F3FFB
SHA-256:	E1330B1552647F834DF6F41D0590D3FEAED3DD6E22A27CB59342F8BCA772F9DF
SHA-512:	82B9091E618909576451CB70E9E7B0C8FDBAFB1ABD1402CFF32E90D25BB9C2B6D6837840D73DEA2077ACB51ADD79A12B9158148FED0482444DA619943A55A8D3
Malicious:	false
Preview:	91.....*.....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..822446000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-07-22 17:20:53.60][INFO][mr.Init] MR instance ID: beee9845-accd-4a3a-a77b-9a15503d3b43\n","[2021-07-22 17:20:53.60][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-07-22 17:20:53.60][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-07-22 17:20:53.60][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-07-22 17:20:53.60][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-07-22 17:20:53.60][INFO][mr.CastProvider] Query enabled: true\n","[2021-07-22 17:20:53.60][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.133946875733089
Encrypted:	false
SSDEEP:	6:mD5q2Pwkn23iKKdK8a2jMGIFUtpEj4XZmwPEvEjzkwOwkn23iKKdK8a2jMmLJ:05vYf5Kk8EFUtpEcX/PE8P5Jf5Kk8bJ
MD5:	409FFDD102F6FB218C68E965B4AE622F
SHA1:	B85D84452811D843F06EE8688CC1140C4B5A444C
SHA-256:	6D0435067E48ACEE9305EA33F3AD8BD693F599A40ECFFE6E1E26BC74B6234595
SHA-512:	CAFBE91388C36AB46502FFE04C17AE53C526D815FEC573C4A2E794ABA80A2C91DC3059A162DA28F11D3E8183A7BE58975C92BDBC19C8D22BFF9BEAC0F5BEDB69
Malicious:	false
Preview:	2021/07/22-17:20:41.728 1ac4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/22-17:20:41.733 1ac4 Recovering log #3.2021/07/22-17:20:41.737 1ac4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.247127054058229
Encrypted:	false
SSDEEP:	6:mNUFLROq2Pwkn23iKKdKgXz4rRIFUtpKSFRZmwPKHkwOwkn23iKKdKgXz4q8LJ:xpMvYf5KkgXiuFUtplR/Pa5Jf5KkgX2J
MD5:	188C8793BD1F331EC457D0231E7485D5
SHA1:	11797A0D76CC52D995DD8539926E3AE4E0500141
SHA-256:	E93392D0730C4F858065A5996ABA06A5BE1E03BDF85EDD77958F5C9CA5C53024
SHA-512:	8BBA7A4E423F7CAF1166848379AE6CAD75F6E0F7813E5538A69AE1204B7C579B91CA0B0B51497D7877A1DB36E138483E8D53951E114412CCB89D3787C3B6F65F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Malicious:	false
Preview:	2021/07/22-17:20:41.983 1b14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/22-17:20:41.985 1b14 Recovering log #3.2021/07/22-17:20:41.986 1b14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.011144941877655
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoE:wIElwQF8mpcSJ2YK1
MD5:	0C37B3BED260DFDF816B387B6B5D3B1D
SHA1:	2679C26D397FD0813C0DBBF21F6E1E8F4BEDA4C1
SHA-256:	867163649F1E30853E866BEA126C2B07EC69D00FC3723D29EF898E36C712061B
SHA-512:	E4B9B833521E5DAE79CE6B94AF1B7ACB4C9F1EFFE7C896E900CE768F0F3CB1FDD8161BE0344DF057518C71E8543D5D3DDC42CC3DD2008DAD9CA42D962A4CC18
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8264578357809998
Encrypted:	false
SSDEEP:	48:QoqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUP6:QohIElwQF8mpcS+
MD5:	B7C5BAA974747684F5E8E22ED8C9EB73
SHA1:	674653AF3D244A1864339053D6AC23B8E497213E
SHA-256:	B7A3CB99FD0A0A657FE84A5AE1349ECC520C099F097E82489B7EBADAFC23941D
SHA-512:	897F0C8CBD9B5B4F3A752FB4E6FFDC1C54ADA3F4ACA2F591E395FBB000A2993F753D26C818BB910D4ADC11A42A7D1DAFF1BB2BF24370D5F3435D36EBFAC88CEE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.145157173548239

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Encrypted:	false
SSDEEP:	6:mNPHlL+q2Pwkn23iKKdKrQMxIFUtpKid11ZmwPKidjLVkwOwkn23iKKdKrQMFLJ:eIvYf5KkCFUtpf1/Pv5Jf5KktJ
MD5:	205FBA9C1EE2203EC3BFC926CC878B04
SHA1:	84B34E6941997E3510533644B3149D2FB621D58E
SHA-256:	D317E457AD72FBD69BFC40E2AA4CD9A4FE436086BC7D688AA4D1E83A35A77447
SHA-512:	4632DB331133BA434EDFA3210E9E3AEA69744C1027D2520EA0E70FFD69C7DF4DBC8A3759B98141F85977614C9CFB11001A37141F6F7FE5A93A2735F87C108B3C
Malicious:	false
Preview:	2021/07/22-17:20:41.932 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/22-17:20:41.933 1a98 Recovering log #3.2021/07/22-17:20:41.933 1a98 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.125094797496074
Encrypted:	false
SSDEEP:	6:mDELGFL+q2Pwkn23iKKdK7Uh2ghZIFUtpEB1ZmwPEJEFLVkwOwkn23iKKdK7Uh2w:0EmyvYf5KkIhHh2FUtpEL/PEJEFR5JfI
MD5:	81F70E939CB53D714033484562E3CF25
SHA1:	BA03E58D467640BFB6E691FB2F80AA68FCF0BD29
SHA-256:	8CF02314CB8A27BD092D066BD29004E50D7F7FA3F44CDF84B8E7D56D5FD5C374
SHA-512:	91A2B9DBC3CD3B2CCA4A383D1E0661F054130123F3A1FAD1508DC3182EFAB0E20FE2073910625AE417E325ECDFDD8B388A7D852D6582CB84CCC859FB73A030A1
Malicious:	false
Preview:	2021/07/22-17:20:41.718 1ac8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/07/22-17:20:41.729 1ac8 Recovering log #3.2021/07/22-17:20:41.731 1ac8 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\27285b39-9e5d-48ad-9660-5276ab5edac0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.21979755593409
Encrypted:	false
SSDEEP:	6:mNCFUHkN+q2Pwkn23iKKdKusNpV/2jMGIFUtpKEFWZmwPKEoVkwOwkn23iKKdKux:8l+vYf5KkFFUtptY/PtoV5Jf5KkOJ
MD5:	A0059FF27C2AC96BF236BE2B51B70A20
SHA1:	9C13E5998BA71F8DCFF109FC8FB977E87A45668C
SHA-256:	E95C313F9E82649CF11F15BC4A5A4160026CDA70B62C13D84D4389BE8EBA580B
SHA-512:	1A7EC6EE28BCC556C1B6B10341533E89BFCACE99BFB30EA7CFED66DD2EFB4B54F78F0AC7E872439F89091F1769013DCA7C4A174AD0CD366662364C737EBD6 1C
Malicious:	false
Preview:	2021/07/22-17:20:41.927 1b0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-17:20:41.928 1b0c Recovering log #3.2021/07/22-17:20:41.928 1b0c Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.256502275043329
Encrypted:	false
SSDEEP:	12:pUf4vYf5KkmiuFUtpBsJ/PfD5Jf5Kkm2J:pUfKYf5KkSg0FVJf5Kkr
MD5:	05C43F068A386C46D57CCEF6D1B9E133
SHA1:	86B4BF7F56D4B7AFAF3BC839F3231613FE3FAD78
SHA-256:	165704BAACA17B44C3067738A01AAB3D5F6B1AF46B4629F2094E686CBF9C0A70
SHA-512:	A86A04FC0CB06E082FB40CE0696302B88FA8ED3108DA771DDEEB4CB30C983BC5CC70FB97A4181D4DF44E0C1D523376AAE3047B2013EDFAF4CBB25F74C99BC 004
Malicious:	false
Preview:	2021/07/22-17:20:41.981 1b20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/07/22-17:20:41.983 1b20 Recovering log #3.2021/07/22-17:20:41.984 1b20 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.240549639987825
Encrypted:	false
SSDEEP:	6:mhdSL+q2Pwkn23iKKdKusNpZQMxIFUtp2z1ZmwPimLVkwOwkn23iKKdKusNpZQMT:MdSyvYf5KkMFUtp2Z/PimR5Jf5KkTJ
MD5:	AAC45D00251F37170BD81E6FB0CD51BF
SHA1:	84296EDED92CEC4E9C09C5F475026B9F8DE51B63
SHA-256:	02C6D0A6AF21B2F6548A178B6A1C6AF8676C0C3FBE077FC197311F3B17A81B1F
SHA-512:	00B1AE8EBC9E5A0D4159E00DDE98B5146BDAC94D3232E34794D80CEF237B1F47D9B3B790BC27641A778E135F6EA3747402829039F16E1176D99DDAC2ACAAAE 8
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Preview:	2021/07/22-17:20:58.544 1ac8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/07/22-17:20:58.550 1ac8 Recovering log #3.2021/07/22-17:20:58.551 1ac8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\4cc3ab68-1515-4b7f-a2ca-0e9c6357d1ef.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.210740809384111
Encrypted:	false
SSDEEP:	12:RIvYf5KkkGHArBFUtpG1/PI5Jf5KkkGHAryJ:YYf5KkkGgPg0AJf5KkkGga
MD5:	AD59949519ED7B975AC1CF9F018329F9
SHA1:	E967203FAF13A30FA83A9F1CE0F0CEAC5F65B5A0
SHA-256:	F9A432AD3F89BF8E52C175AF1850D26E5CD2FD91E1E8C0D27DC9B064B251640D
SHA-512:	0BAAECA22F8FAB25C95A44597439A8430A878E81C91425EC757E815A3B5A91CBC2C5FCD6DB82E58CC9CB0815E846404EFA2A181829B30DE45C986F1EE25E04F
Malicious:	false
Preview:	2021/07/22-17:20:50.652 1a98 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/07/22-17:20:50.653 1a98 Recovering log #3.2021/07/22-17:20:50.653 1a98 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.200568606009649
Encrypted:	false
SSDEEP:	12:gcvYf5KkkGHArqiuFUtpU9/PJP5Jf5KkkGHArq2J:gmYf5KkkGgCgyRJf5KkkGg7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
MD5:	0C78A6C3F91862D03C1A3739C10FDDAC
SHA1:	D2281D047AF32EBE808F5E679C0F2E33A1755412
SHA-256:	83824D674A0B774BE43C53D3F48A2820B7C48E0524142C01E9A3E71036C88251
SHA-512:	2C083EB2C80C140D0C8F8B783ADCC6C73B789CCA112CD9753C9ACA86D7ED83D9A2E5D987CEBD632C81CC75FC58F2CA23DA41F7BF39FD5A686044F5BD5A1E329
Malicious:	false
Preview:	2021/07/22-17:20:50.709 1b24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/07/22-17:20:50.710 1b24 Recovering log #3.2021/07/22-17:20:50.711 1b24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.164765735789584
Encrypted:	false
SSDEEP:	12:8ovYf5KkkGHArAFUtp+/Py5Jf5KkkGHArfJ:hYf5KkkGgkg3Jf5KkkGgV
MD5:	455F3123A7BF3FD8860F75BC07E941B1
SHA1:	71411DA3674FBFD8D2F0FEE717ACA3BC39F0FFF6
SHA-256:	F80B503FCD2EF2543440685F536EC7FABCDC91BC090740D3D02A9F1BE3EE08D6
SHA-512:	C527AE9E1109845030B8352BCB80387278DF037005306D7231DCA30F39C2268CEADE884A9168155B93A26757CCF19320EFE81AD513547DE52EBC383414DBFB9F
Malicious:	false
Preview:	2021/07/22-17:21:06.017 1b08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/07/22-17:21:06.019 1b08 Recovering log #3.2021/07/22-17:21:06.020 1b08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Entropy (8bit):	5.153385866309624
Encrypted:	false
SSDEEP:	6:mDAIq2Pwkn23iKKdKpIFUtpEqJZmwPESyvzkwOwkn23iKKdKa/WLJ:0xvYf5KkmFUtpEqJ/PEbvz5Jf5KkaUJ
MD5:	28B4BB49AB6F0A6AE3800AE3F14ED260
SHA1:	721D69EB011664E999478F1183AC5A06F18D4489
SHA-256:	3D416047F303E15B4AF4732568EED0DB51210ADB9BDCE447F24C5786AC283D96
SHA-512:	D94146C722C2D0518FBF7A2F4DF753132AEFA2E953E4C44A9BEFCCE1341D62F03A0AF1CD74914460E33A3634C93F4BF7EFE60189A1D6637A4F924B36929EECD6
Malicious:	false
Preview:	2021/07/22-17:20:41.715 1ac0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/22-17:20:41.726 1ac0 Recovering log #3.2021/07/22-17:20:41.730 1ac0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.299964710643728
Encrypted:	false
SSDEEP:	12:ilyvYf5KkkOrsFUtpY/P4R5Jf5KkkOrzJ:ilYYf5Kk+gDDJf5Kkn
MD5:	C1C5D365260A09274863238DA3B762E9
SHA1:	D2C29EBDBEF585301FDC4645739ED85D1B6CE38A
SHA-256:	1388497C702ABE2E9ED65D6742A226A33BE6D22236F6753F72C0499F8A93AD8B
SHA-512:	CBFE04BCFEF6D281B1AE6AA08C7A6AAF4736F10F3BE4152C2F2CA831E3C1C278E6E0D4CE43B48A252CBCDF979D92A977C9A3F6EC0B7416E0BBC4AC82FD42EA2
Malicious:	false
Preview:	2021/07/22-17:20:53.562 1ac8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/22-17:20:53.568 1ac8 Recovering log #3.2021/07/22-17:20:53.568 1ac8 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:eoZDet:C
MD5:	395977D733F9E2F3A1F52D11B74755E9
SHA1:	3607CB27282486FA61C95304EDE5C8C6429191A1
SHA-256:	86595DBF6B8C91FE833DBF72F5D380233542DCE738994D67447248CEF8217A47
SHA-512:	BC64D769B1A11919FBD6160EE49FC9D6B39FDAAF0AD85670F79C4AFC73441246F48F692322ADEFDAE5AEEB08ADDF9864C4A9B0A4A3812760533EB5344410D83
Malicious:	false
Preview:	....:....;.\

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\abd7c84c-14a4-49a7-b36b-3ddc54235023.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\abd7c84c-14a4-49a7-b36b-3ddc54235023.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d1ca51df-e0a0-40de-b734-b9fe37c3d30f.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):	4868
Entropy (8bit):	4.932315600751183
Encrypted:	false
SSDEEP:	48:YcPkKSChkliaqArdqTlYGlQKHoTw0Orf4MqM8C1Nfct/9BhUJo3KhmeSnpNGzFen:nHLZ4MpIKIw5k0JCKL8bbOTlVuHn
MD5:	F1AD897E33561B7436D1BC49208FBB48
SHA1:	5BACA40C06E1A27109331C6EFF028F6024D6E061
SHA-256:	EA906853A48C4AD718311359CB31CEEDAF3511F84C3EADAD8F0FC3BF3BFCF2A6
SHA-512:	B722AF2426AEB6B75FF173515930A90234CAFBA7636C7EA238B5DE67B01AAEAB091A9AE34D5635DE6B4969117AB14E0C52BB1FF23837486AD204F0D847FC049B
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271440841945842","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.550085856263343
Encrypted:	false
SSDEEP:	3:tUKINiUeAG1Zmwv32O93VV8s2O8F7hVWGv:m/iUfG1ZmwP7vVv78ltv
MD5:	FE362CE459878FA52DAC449726102C01
SHA1:	FFC8F767DFFDDFB5AF26D5ED6C0D7F6D06C58D6A
SHA-256:	FCE8DF4AE127F57902B3902B939BDE899662A1550993514CBCE564102FDC797A
SHA-512:	061E5D330F277007FC04929D4C41D0AA7615FC1E3AE3795176426CFDB4D0B0730BC05467F736F11FEBCD6F0FEFBE9AD128855A1CC7EA63FA3EDABD188FCDA 8E
Malicious:	false
Preview:	2021/07/22-17:20:47.509 1a9c Recovering log #3.2021/07/22-17:20:48.502 1a9c Delete type=0 #3.2021/07/22-17:20:48.503 1a9c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.207599164408494
Encrypted:	false
SSDEEP:	6:m7BL+q2Pwkn23iKKdKfrzAdIFUtpiNz1ZmwPi5LSLVkwOwkn23iKKdKfrzILJ:kyvYf5Kk9FUtpWZ/PYSR5Jf5Kk2J
MD5:	D213F1F3044C7E0271C26D8B6047742C
SHA1:	AB0C3E11E02545EEF68DBFEC7007BAC31FAD5D16
SHA-256:	3F5D650FCD5D10BDFB1EDFE026C02010B07CD76FB29381256B811AC1A8399B54
SHA-512:	54A560C9BFECAD30E4C67D6E433E01B8EFB7C7932DA103E13BD341FD7DE75B06871A9689D47934449CE1975819F5C102BA56E17EAF2029B638F2BDA1E12A079F
Malicious:	false
Preview:	2021/07/22-17:20:53.609 1ac8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/07/22-17:20:53.610 1ac8 Recovering log #3.2021/07/22-17:20:53.611 1ac8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.28.0\Indexing in Progress	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	empty

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\9.28.0\Indexing in Progress	
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_dir6740_1124400641\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	186784
Entropy (8bit):	4.915957886381836
Encrypted:	false
SSDEEP:	3072:bl35PHEWQyoghJbTloZq6L45c7wbMn5nezpiKmneSxCgWCCkHjuhjMQBJXS:R3NKghJbTl96BXTChW
MD5:	E4ED6CE0DB78ED18701755E5FF177B82
SHA1:	7D660E76CE91C05FC52FE1AD54C28EAD7E4A04B6
SHA-256:	BBA545E82F5720A1AD3BCB3743EB27BB1F015CB2E1222615CB880DA40CE42C20
SHA-512:	F49A4487C245DE86158EE6BD675BF70C74D8FE7164A5AA5D71469AFA94071FD4C06BB09E88E06B1CCDE9ADE6C124C957E45179C25891E12BD7C9FD419B7EBF 72
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\bd27ee45-d995-46cf-9fbf-906ed2f792be.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):	166088
Entropy (8bit):	6.049965612449309
Encrypted:	false
SSDEEP:	3072:l9WW4u2Vl2CViqRnjUkQJUwYMrwjYUEDt5HCzSFFcbXafIB0u1GOJmA3iuRx:8zH2aHRnjOJYMrw8LCzSzaqfIlUOoSic
MD5:	77B3774DBC7447A0109A62DE5A64C487
SHA1:	7EC237AEADAFCF204E189019CEFE132B03534255
SHA-256:	F3A57377878C5AF08E2B375F51DFE92B8AAE5B429194B0BA4BC142F6EB1026A7
SHA-512:	F420B93F8785760CEEFFF1E32B626455ED117E710FCAB1113EDBADE0E5C96A802C8B944FEB70FE41BD04A5B270A8A754F4BAE457828836A4648E19F611DBA34 C
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626967244619998e+12,"network":1.626967247e+12,"ticks":4769258237.0,"uncertainty":3937570.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715636091"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\d7b646e6-4434-44e3-b27a-5ea06687243e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7435340900911176
Encrypted:	false
SSDEEP:	384:h3ReWoLRc70KVDlqNNGrDvai3py8BHMpGdErf8agxRMQEzrLamHzxPMuuSNOUAuE:Jemxpy88VgeXsGYofX2SKkCOhS
MD5:	895CE2F947875991C50F576016AF0A0B
SHA1:	9B6B45A5B208671923E0BD54737D56E0BB557605
SHA-256:	460BB3869A39DA86E3F5633C94D0CAE08BD2CD0273F0B8EA2078C91717B8C623
SHA-512:	5742393DF2C20C5D258654E3009866EFEE9C5DFEA83970D6CFC12F54960C741A24EA7F2320FBB5978B484A118C67878EA44BC4E0295E660D31452CFE6F2A1125

C:\Users\user\AppData\Local\Google\Chrome\User Data\d7b646e6-4434-44e3-b27a-5ea06687243e.tmp	
Malicious:	false
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...o@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\fab0d7d5-c928-402d-abb6-49c3713a1906.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):	166182
Entropy (8bit):	6.050241783957279
Encrypted:	false
SSDEEP:	3072:19WW4u2Vl2CViqRnjUkQJUwYMrwjYUEDt5HCzSFFcbXafIB0u1GOJmA3iuRx:MzH2aHRnjOJYMrw8LCzSzaqfIlUOoSic
MD5:	458F22F975FE8D7E372FE7980CFFD182
SHA1:	0843DCBC13598BB2442D009BF81BBA9FC1A8364C
SHA-256:	97DD73A265AA789DEDED82578D0AEBF87BE07805FFC4F903C500889155C4B966
SHA-512:	A2D0BEB5AABE67436F018392949CD545A13DDC5763023C4BBECB676434E1DD288034F9A08A6416D17D66B69A7E465E235E7F470CD60C04B5522A87321B378B3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626967244619998e+12,"network":1.626967247e+12,"ticks":4769258237.0,"uncertainty":3937570.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715636091"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Temp\155401cc-1527-4167-ae2f-854ceb384b41.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."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\2b4b705b-ea9a-4cdd-ab00-489e03618442.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\6740_1921723831\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\6740_1993787692\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\7b033155-332a-4c05-b8c2-d0fc46f8a7de.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\a460fe93-30f9-4ce1-8c73-bf25845e6b1e.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

C:\Users\user\AppData\Local\Temp\a460fe93-30f9-4ce1-8c73-bf25845e6b1e.tmp	
Preview:	.

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\155401cc-1527-4167-ae2f-854ceb384b41.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!.,~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir6740_1168751802\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\cs\messages.json	
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C53E0A
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\el\messages.json	
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\es_419\messages.json	
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEAD8
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavailable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\fil\messages.json	
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA7555
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "message": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D03 6E
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\hu\messages.json	
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA2
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6740_1168751802\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.977526891400088
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:	Payment Copy for Inv ps-7 -USD 24,806.PDF.htm
File size:	616977
MD5:	49132b4f0d2418a60367a0db949a426f
SHA1:	619827a6c71125baea6b8c6b7c7cfad644ae4b60

General	
SHA256:	24405ff6000d280f546b033cdccda2f6a0afe8697ae36625dd34b193bbf58875
SHA512:	89228668d0e7bbea3d84ad0ed50f04b97a83152dd9d20f92dd37d28c74e70a3e40345a698323ad15ce72d86b0631498f053444c7713a1d2161a829a13812cfc
SSDEEP:	12288:xkbt80kGfQrJWrAE/a6hm7bmB4b+ClC61wMJmb1OG1gK77Y:TgfQFWV/a6A79b+ClTfu8E7Y
File Content Preview:	<!DOCTYPE html>..<html>..<head>.. <meta http-equiv="X-UA-Compatible" content="IE=edge"/><meta charset="utf-8"/>...<title>Sign in to continue</title>...<link rel="icon" type="image/png" href="

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 17:20:46.544226885 CEST	192.168.2.4	8.8.8.8	0x193a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:20:46.575175047 CEST	192.168.2.4	8.8.8.8	0xaca	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:20:50.704099894 CEST	192.168.2.4	8.8.8.8	0xf652	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:20:46.603758097 CEST	8.8.8.8	192.168.2.4	0x193a	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 22, 2021 17:20:46.655441999 CEST	8.8.8.8	192.168.2.4	0xaca	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:20:46.655441999 CEST	8.8.8.8	192.168.2.4	0xaca	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 22, 2021 17:20:50.762794971 CEST	8.8.8.8	192.168.2.4	0xf652	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:20:50.762794971 CEST	8.8.8.8	192.168.2.4	0xf652	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jul 22, 2021 17:23:24.925997019 CEST	8.8.8.8	192.168.2.4	0x427f	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6740 Parent PID: 4480

General

Start time:	17:20:40
Start date:	22/07/2021
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\Payment Copy for Inv ps-7 -USD 24,806.PDF.htm'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 6896 Parent PID: 6740

General

Start time:	17:20:42
Start date:	22/07/2021
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=1556,11699132993908980424,10170989427665474543,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1696 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly