ID: 458788
Cookbook: browseurl.jbs
Time: 18:43:51
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

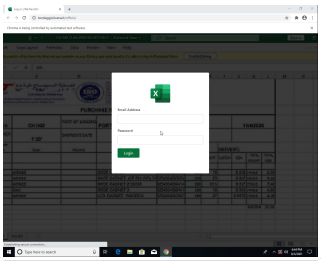
Windows Analysis Report https://tendaggisilvana.it/offic…

Overview

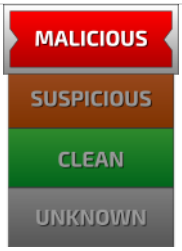
General Information

Sample URL:	http://https://tendaggisilvana.it/officix/
Analysis ID:	458788
Infos:	

Most interesting Screenshot:



Detection



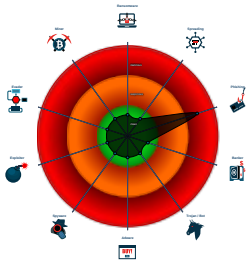
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Form action URLs do not match mai…
- HTML body contains low number of …
- No HTML title found
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5904 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://tendaggisilvana.it/officix/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5952 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,13813088594936222501,123881940111943640,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1724 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

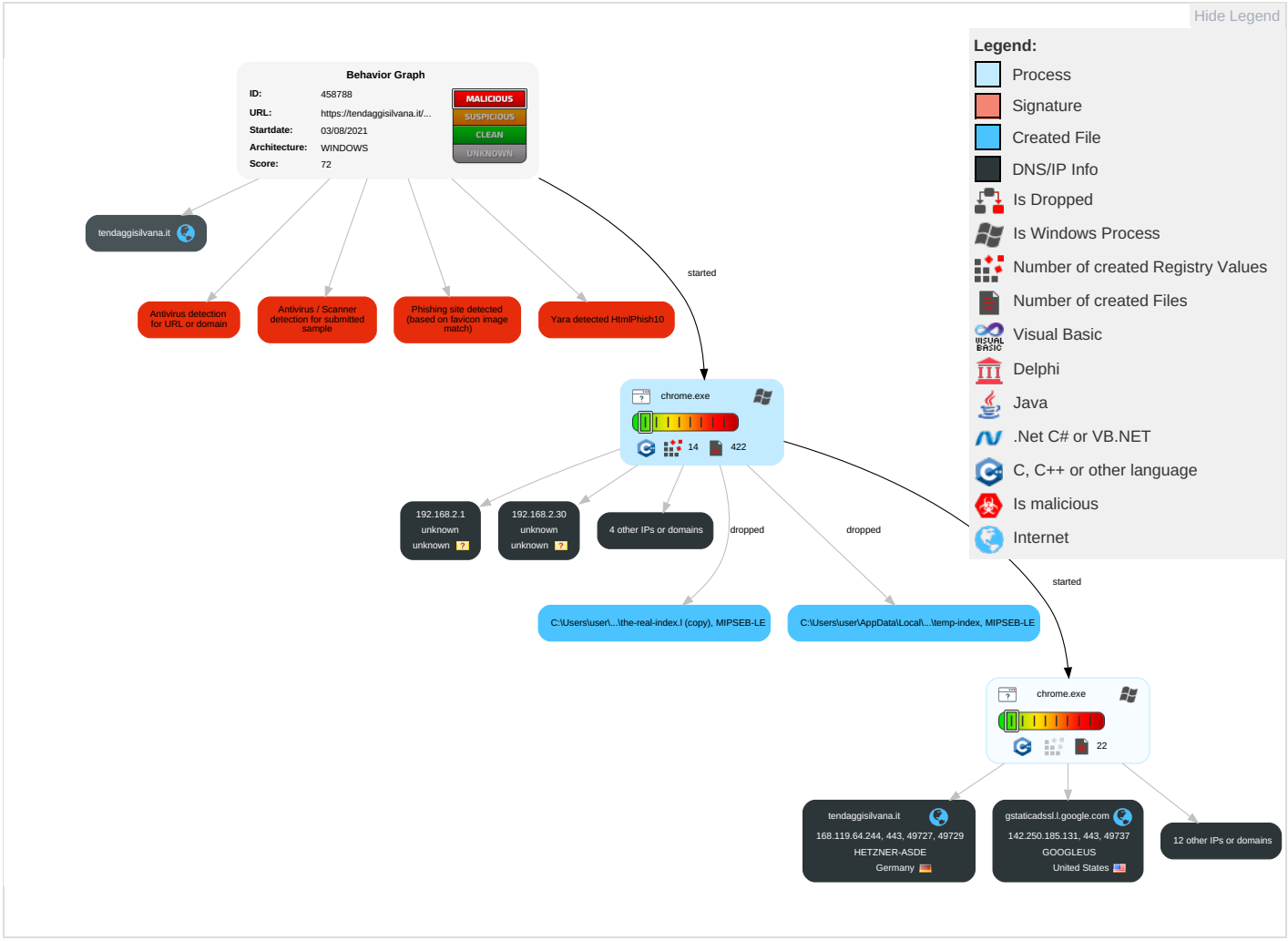
Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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

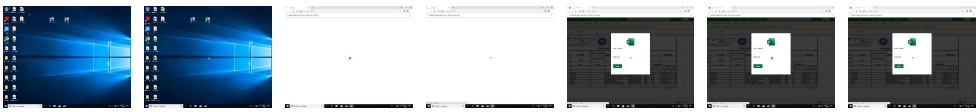
Behavior Graph

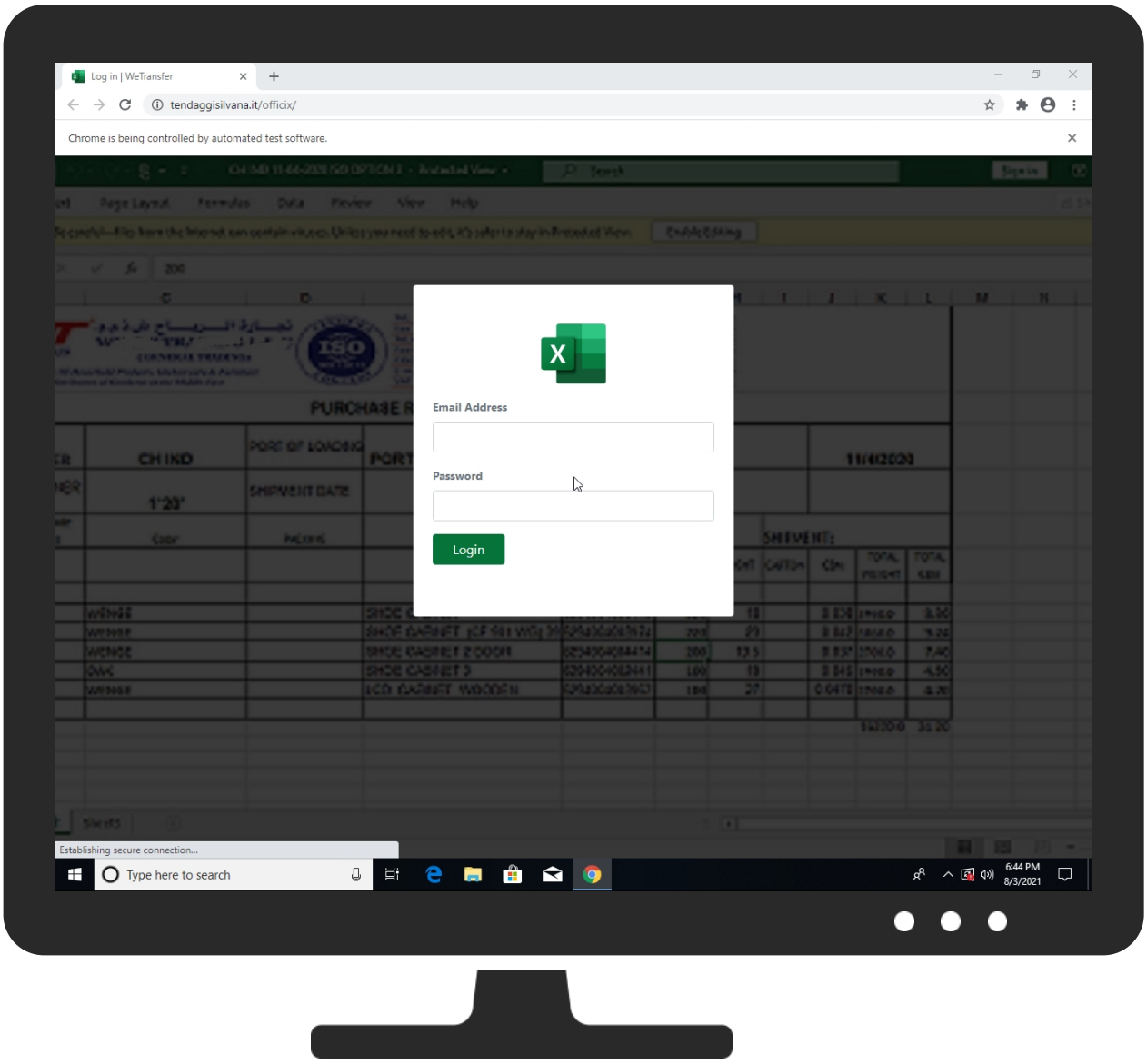


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://tendaggisilvana.it/officix/	2%	Virustotal		Browse
http://https://tendaggisilvana.it/officix/	0%	Avira URL Cloud	safe	
http://https://tendaggisilvana.it/officix/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://tendaggisilvana.it/B	0%	Avira URL Cloud	safe	
http://https://tendaggisilvana.it/	0%	Avira URL Cloud	safe	
http://https://tendaggisilvana.it/J	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://54.211.202.147/excel-b/excel/excel/mailred.php	100%	Avira URL Cloud	phishing	
http://https://tendaggisilvana.it/officix/2	0%	Avira URL Cloud	safe	
http://https://tendaggisilvana.it/officix/l	0%	Avira URL Cloud	safe	
http://https://tendaggisilvana.it	0%	Avira URL Cloud	safe	
http://https://tendaggisilvana.it/officix/Log	0%	Avira URL Cloud	safe	
http://https://tendaggisilvana.it/officix/images/logo.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.185.131	true	false		high
stackpath.bootstrapcdn.com	104.18.11.207	true	false		high
accounts.google.com	216.58.205.77	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
tendaggisilvana.it	168.119.64.244	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://tendaggisilvana.it/officix/	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
168.119.64.244	tendaggisilvana.it	Germany		24940	HETZNER-ASDE	false
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
104.18.11.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.131	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.4
192.168.2.6

IP
192.168.2.5
192.168.2.30
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458788
Start date:	03.08.2021
Start time:	18:43:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://tendaggisilvana.it/officix/
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:	3
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@31/218@11/15
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:44:50	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2F A0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{...,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1353860816263266
Encrypted:	false
SSDEEP:	6:kKudoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:i5kPlE99SNxAhUe0et
MD5:	9D8DC5873FB161E95493952016B6EA2F
SHA1:	2AEFC79B9C98B194A27EDAA4C3627FEF2DD50E59
SHA-256:	C68AE99D0B709466F6F54ECE2C63604C529C1ABD661E603E2E2125EC7332E677
SHA-512:	CAC8977FD70E5D95D13BA813328FD23695EF3E0B623B522A921C364C1A7CDDE51A85D1CBFB6471726F9BB07104756B77166FAE3F33E3FF5CF2A1625C95D18DE 3
Malicious:	false
Reputation:	low
Preview:	p..... .....n.....(..... .....T'._.....$.....\...h.t.t.p.:/./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.::0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0050ec22-f187-43a3-847c-c2f678420bfb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.748949117620136
Encrypted:	false
SSDEEP:	384:HPBeWoLN0AvqpNWrDvqi3h6Q9H4BGdUrf8ugxR0EEHrPWmDgPMu6SJOU46N31e/C:be5RKY5pgenQS48vDGqKwSaJF
MD5:	144CC51726A565ECCC2F9CC827CA944D
SHA1:	B881CE30B43D03082567716BB95BE99FB8DC8ACF
SHA-256:	422185AED1729E3617622F2CE24D62454CF21EF2388AAE5A19DDFB7B0D37EEC5
SHA-512:	E31FCC15B8480D7796F5FBCBF4C6383C3E6228E84DD8CE5B21AF881EF5110BDBC21D5E76A9EDD3346C25F2E6F9D6EC313297B05192872CADA1C20BF251C19A 91

C:\Users\user\AppData\Local\Google\Chrome\User Data\0050ec22-f187-43a3-847c-c2f678420bfb.tmp	
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\5cd31337-3cc5-401a-9ce3-b1b8f1ddb31c.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):	166026
Entropy (8bit):	6.050486615153345
Encrypted:	false
SSDEEP:	3072:QicfpuYAZ20//XkjhbEkzrw7bFcbXafIB0u1GOJmA3iuRL:QlpUubUtaqfIlUOoSiuRL
MD5:	11AB3E4F4969C592C91E73D14897E61E
SHA1:	BD08F46CD45C8AC80EB794A5215CFCD65F2251C5
SHA-256:	D73563607F2849DF94393664C33242DD7206512FA07372D78710F59C1135A1C5
SHA-512:	78F2D8DD3139D26C939388DE9B4F96A87D868A9E6B0D24985BDD6D00B91620CCF1D22158A6058400AFCC58E6411B652B3302C5D3BFC35DC0D9111E47A8C949
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":1.628009087875985e+12,"network":1.628009089e+12,"ticks":6691630284.0,"uncertainty":4981907.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBljSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715906189"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\6f2f16a7-88db-404f-80de-4cad351569ce.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.749461780999735
Encrypted:	false
SSDEEP:	384:xPBeWoLNwDAuVDlqpNWrDvqi3h6Q9H4BGdUrf8ugxR0EEHrPWmD39PMu6SJOU46L:Fae5RKYEpgenQS48vDGqKwSaJV
MD5:	5C6AB2CC45A510C70BC22505AB078D03
SHA1:	065C77E1B78A4CBE3FD4EF5371FDB237F9C39BED
SHA-256:	25509E9C869F48367902A3ED7004902D57014C8E0CF6F05AC9CC99EFCDA8F071
SHA-512:	23009595F7DCC730F7E43FF71EE73F912126BC5148F64D838ECBEFB1E7957854DD5744CB6D94EC81AB65718B171BA6A548ACC3F328B8B03AB3748289169B9C4
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\7417fa0f-3ab8-47db-9f9e-0a6ae5528647.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):	165932
Entropy (8bit):	6.050215202350764
Encrypted:	false
SSDEEP:	3072:sicfpuYAZ20//XkjhbEkzrw7bFcbXafIB0u1GOJmA3iuRL:slpUubUtaqfIlUOoSiuRL
MD5:	99E371AB6BABA41E10FAC86F5266ECED
SHA1:	75B4E307E30ADAABAF339C2225E0CAF70CF1646C
SHA-256:	E1074EAE27106800DC3022BFD52B301D6D6850F5E198EB021A15C862547E4A77
SHA-512:	08F7934886B0661FCA5D5E2EB6F1D03767C008F21DD91CE9B1E52EBE7150DD809689C58B0455CA8C502B96779446596C2C098D7D395B8FE5AA8E6F127D76427
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\7417fa0f-3ab8-47db-9f9e-0a6ae5528647.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628009087875985e+12,"network":1.628009089e+12,"ticks":6691630284.0,"uncertainty":4981907.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715906189"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\990b6f74-ede8-46ee-80cb-58f017429266.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):	174391
Entropy (8bit):	6.079668399402164
Encrypted:	false
SSDEEP:	3072:MlpicfpuYAZ20//XkjhbEkzrw7bFcbXafIB0u1GOJmA3iuRL:yplpUubUtaqfIlUOoSiuRL
MD5:	5494CA2BE27F0D174D1BF7ABE9B22ED6
SHA1:	61C235B60A64544BA4F26DBAE253F77691F29A72
SHA-256:	9A8A1B6D5FE8907EE5FD86BC64F84D0E328BB5700B716F613A013D594BFC5C81
SHA-512:	9D157ABE49185AB8A56FDF44CE84671A6A3DA188A59EA35257C28EA212AD14260D484E38FF1F637E0DFA0119E1DACE2F44F2B7DC3C87B91932CD4134EAD66FCB
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":1.628009087875985e+12,"network":1.628009089e+12,"ticks":6691630284.0,"uncertainty":4981907.0}},"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\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:	low
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\0c8c60f4-5f2c-4963-ba5b-e5edcda68b59.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):	5.53615687904282
Encrypted:	false
SSDEEP:	384:IgltjLl9PXV1kXqKf/pUZNCgVLH2HfDprUyHGbnZ/aGnA4T:TLl1V1kXqKf/pUZNCgVLH2HfdrUyGbnN
MD5:	0B5231D897DCFBD90CFAD757B8CA5797
SHA1:	E43CC7D4B9FD131687E86B4F3D69AFF86BB8FE88
SHA-256:	EAE39C24CBD777D7FACCCB8B8BE4D1B9E284C51E70B96A762DBCC50F785BD6C4
SHA-512:	A3472581D930519738C3AE85E4C77D1CDD415621100EEB1F881DA2348BBEB7CE597E443601605A2AD6B8A8C82EF4D97FAE5B10C82B6314F039C2780C9A2D9DB2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0c8c60f4-5f2c-4963-ba5b-e5edcda68b59.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272482682910260","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\114ed127-3f9f-451e-8653-73bee937e8be.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22601
Entropy (8bit):	5.536332893103934
Encrypted:	false
SSDEEP:	384:IgltjLl9PXV1kXqKf/pUZNCgVLH2HfDprUyHGgnZ/abnA4B:TLl1V1kXqKf/pUZNCgVLH2HfdrUyGgnU
MD5:	613D1F9AFD655765C512FB30AA9DA4A8
SHA1:	4E10D94D0E1C885E91FCA5F7C7495EF38676AC13
SHA-256:	64E56F093D788EC0956B28BD846F683FB1044641F1D6FB9E4A1A6DFEECA5E287
SHA-512:	0643B32DDBC8BE38C48ED3A318FBC55C62E0D7CF16E3264BEB164290BAABBF162DB41DF0BCC251106B87593F20B9B0D7E519F4047F30EC63C708045925D519 2
Malicious:	false
Reputation:	low
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":"13272482682910260","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\195d7acd-9172-4664-84cb-9ec323fec992.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):	2722
Entropy (8bit):	4.856790400177536
Encrypted:	false
SSDEEP:	48:Y2nzMKDHGXtwWsNRSepsAZ6q5C666NhpsR8qiws5kzsuDsxyKsyI3gYhbw:JnzMKDHGXOz0OZx5C666NsrihwMAxhM
MD5:	91BC25EB4AEC27623B3C566FBFAE0AD4
SHA1:	095B9F17D6C20CBD37AD5BBC51A7CBF028A76DEB
SHA-256:	3B208695BB77F14A303AD27390522145A47E219D7C5B8D36B851EBFD10E4BD87
SHA-512:	25C5B4CFB333612DDF0831ACAF80F9208BEE42170BEADF0CE1A8B337BFEEB25C4039F23730403F86485E3CD02ACC0C4DB4BFBF355966287A7BEC07C257731B B7
Malicious:	false
Reputation:	low
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://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275074689688749","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"isolation":[],"server":"https://kit.fontawesome.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"1327507468991245 2","port":443,"prot

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\454701ac-4bc5-4887-b755-89b21dc911b9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\454701ac-4bc5-4887-b755-89b21dc911b9.tmp	
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\48ada2ef-bb21-4750-9063-6dab0147735d.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):	1710
Entropy (8bit):	5.576367033344524
Encrypted:	false
SSDEEP:	48:YDcRUttVwUw6UUhveUUKUXqPeUekUeUwUHqdsYUW4PUeP:/RUtQU5UUgUUKU6PeU3UkUNYU9PUg
MD5:	7A0B4E3D34699609F9DD964F6DEEF0E4
SHA1:	6ED7ECE6FE235BF1EBC57A536EF00E9A4E42F5B7
SHA-256:	82086EF83CA7D8CD8199F991F5CD5DC58AEE3D406FF4D41CAA956CED107642EB
SHA-512:	59628ECFC560D56AE960C2C2E708B75AEC74A7C2FF0D9DA3398DD702440CA7536B8C7F248F90016EC1F5AE0F6F754E0B7D35CF25284D43B6063373FF0C75A9C
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659545090.236635,"host":"AKBA0EXj1W1QmJumkxUOTpibibkAwoUEp1CDrh5UFWY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628009090.236645},{"expiry":1643789090.475637,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628009090.475641},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659545089.922513,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628009089.92252},{"expiry":1659545089.913066,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628009089.913072},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4e840cfa-e490-43b5-9300-24a14ab17106.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):	5765
Entropy (8bit):	5.172430742090153
Encrypted:	false
SSDEEP:	96:ncLfQ9tyVUhqIKInE5k0JCKL8I9kP1NbOTlVuHn:ncLY9QCMI6h4KPkP5
MD5:	FFF7FE0C237CAA9D4CEE7FD9CCE2280E
SHA1:	2098A63B5E53553929757FFEE95D00CE8312C005
SHA-256:	D52B21836651B460DF3CFAD159FAD732078F454A29B914A7A02D4DF24564ED20
SHA-512:	096F0538E4690B9778F0EE615416D8202EFBA3E3633950E761EA04F0B3A972FF19367944B8D9729DE262F3198AB4EC00EFE26E6BADB12A02BC9866F77373FD8B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272482683233446","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\52aaa0ad-dc5c-4259-9261-04d5b91bf149.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):	5169
Entropy (8bit):	4.964635901531355
Encrypted:	false
SSDEEP:	96:ncLSt9pIKInE5k0JCKL8I9kP1NbOTlVuHn:ncLS9pI6h4KPkP5
MD5:	A3BEAD18C2E80CCE08DA12C45C20290E
SHA1:	381B2571FB47159FC19AF411BABA8A31946878F9
SHA-256:	D1DD2ED6F4D76BE39B4BDD174501BBA512186584181EF615C6F73501B26FDE8E
SHA-512:	971ABCD02A696FED1838759FE87E55F76E220DAFB61620BC438719E5D1229D852EF9813D39BAC330EDC747419C7DA3015BE05D61C83F228CBC730196BF6177C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272482683233446","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\874b9b01-d12f-46df-98fa-f10f12326915.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
Reputation:	low
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":"1324851660 7334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"adverti sed_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","s upports_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\93130777-005e-4aa2-878f-f445fbbe5e2a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577677386119199
Encrypted:	false
SSDEEP:	384:IgltuLl9PXV1kXqKf/pUZNCgVLH2HfDprUzaGnA4Y:+Ll1V1kXqKf/pUZNCgVLH2HfdrU+GA3
MD5:	AEB93A7988FF4C09C6F8A5769720961B
SHA1:	0F7FC58EEB011984C5DF3CA1615EAC5A8BC3476D
SHA-256:	178D0BADF49E8937FB166FDA5E5F010C393BB8A74AC4AFFAC46BA44542F17B9B
SHA-512:	5116B71C318A466F4A869954EB98AA360BA95A7F8C9353D0F923A17D82251E8ECB9BA7DA3980EF43D8863518813E6093A16B740427245A91DC550E5E0A01EDFC
Malicious:	false
Reputation:	low
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":"13272482682910260","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):	5.241008666485333
Encrypted:	false
SSDEEP:	6:mAHt4q2Pwkn23iKKdK9RXXTZIFUtpFF8JZmwPF3DkwOwkn23iKKdK9RXX5LJ:QvYf5Kk7XT2FUtp3O/PN5Jf5Kk7XVJ
MD5:	1A64445915C57421C82ADDABCCC7CE78
SHA1:	E0130F95C38D3AFCFC919177C1B69A5BFCD0BC63
SHA-256:	9769C39347F37CCF11ECE6132EEE108E9AD84D8F873BC82CBE9F03F6C46A37CA
SHA-512:	C4762284B042AEBEC61ADECE1E8BEA3B92A9222504A22B651687E0EAC86B127458F39B8A73BC49A8E16BA022FF93676B2F91BEA970F5136454DF7696307D0E25
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.300 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-18:44:59.301 16d0 Recovering log #3.2021/08/03-18:44:59.302 16d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.241008666485333

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
Encrypted:	false
SSDEEP:	6:mAHt4q2Pwkn23iKKdK9RXXTZIFUtpFF8JZmwPF3DkwOwkn23iKKdK9RXX5LJ:QvYf5Kk7XT2FUtp3O/PN5Jf5Kk7XVJ
MD5:	1A64445915C57421C82ADDABCCC7CE78
SHA1:	E0130F95C38D3AFCFC919177C1B69A5BFCD0BC63
SHA-256:	9769C39347F37CCF11ECE6132EEE108E9AD84D8F873BC82CBE9F03F6C46A37CA
SHA-512:	C4762284B042AEBEC61ADECE1E8BEA3B92A9222504A22B651687E0EAC86B127458F39B8A73BC49A8E16BA022FF93676B2F91BEA970F5136454DF7696307D0E25
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.300 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-18:44:59.301 16d0 Recovering log #3.2021/08/03-18:44:59.302 16d0 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):	5.257987689091376
Encrypted:	false
SSDEEP:	6:mAXZ4q2Pwkn23iKKdKyDZIFUtpFXKKpJZmwPFXXF8DkwOwkn23iKKdKyJLJ:d6vYf5Kk02FUtptrD/PtVi5Jf5KkWJ
MD5:	7124CC2E82D13F1DE677613D8500C879
SHA1:	2F19067C2E6C01776AD95EC90F35D71A3DC0D4AE
SHA-256:	D7C3FAFB360F91420DCD34565280F86B137D62EE20F4010A8649AC1DF6246742
SHA-512:	078A949F3737F3446A4804B0EF51918FC1ECCED6AAF3EAD50F09D7466318CD07CECC2C1EB5FF8C9E2D53BFE4D9DB99B1F88FC405BE037BD89043259BCB2CC53
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.263 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-18:44:59.278 16d0 Recovering log #3.2021/08/03-18:44:59.280 16d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.257987689091376
Encrypted:	false
SSDEEP:	6:mAXZ4q2Pwkn23iKKdKyDZIFUtpFXKKpJZmwPFXXF8DkwOwkn23iKKdKyJLJ:d6vYf5Kk02FUtptrD/PtVi5Jf5KkWJ
MD5:	7124CC2E82D13F1DE677613D8500C879
SHA1:	2F19067C2E6C01776AD95EC90F35D71A3DC0D4AE
SHA-256:	D7C3FAFB360F91420DCD34565280F86B137D62EE20F4010A8649AC1DF6246742
SHA-512:	078A949F3737F3446A4804B0EF51918FC1ECCED6AAF3EAD50F09D7466318CD07CECC2C1EB5FF8C9E2D53BFE4D9DB99B1F88FC405BE037BD89043259BCB2CC53
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.263 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-18:44:59.278 16d0 Recovering log #3.2021/08/03-18:44:59.280 16d0 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\Code Cache\js\5bb5e88508645c3a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.497590905694627
Encrypted:	false
SSDEEP:	6:moIYET08NaYWbVOqZw1LWxc1wGvsdlchUnK6t:3Ag8NaY8ZwIUwbdeWp
MD5:	0E648ED70DC878EF030D9CF4CCDF32DC
SHA1:	9786D24F2F07D732FBCAF8E36078BB1A7081C854
SHA-256:	9110A2D0526D98C025F714D1CB555803145A6F51BF3D29E06A7950A030C09480
SHA-512:	8A3506CF8C0272FB303617A84DCC8668C978D2B2F7176281D85B9D320FF53A2C08B34C0F2BA56BDBF435FDFED221751F1A772ADE62D5A7D1DF4431E2FB20974
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5bb5e88508645c3a_0	
Preview:	0\r..m.....j.....)...._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://tendaggisilvana.it/B...@'/...../.....!...G.{.i.....4.....8B..d)...' .A..Eo.....7TPp.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7003b29a8a2647cb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.541710206812006
Encrypted:	false
SSDEEP:	6:mIPYlNYpSVkZ1LWQEl6A4Cx7om4wbK6t:bpSVAlWkdH3N
MD5:	A4EF641F19E390DB945FB5A3913E4B82
SHA1:	F8BDE79674505361920AEE94401997C212B42EF7
SHA-256:	3BC6AF65EF3F50E5AD6C8CA6936A77A16B8F28DCED23C14CE7F7630E2C72A09F
SHA-512:	96C297FE57E136D09962F8EF3C888FA41FF781AA2CACA2482660746AACA76A43C73ADA234578FC5211A855A2AA700C31CCBF602AC116D668112880A5DF880AC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....g...._keyhttps://kit.fontawesome.com/585b051251.js .https://tendaggisilvana.it/.!..@'/.....).....kP.p../..]@.....Q^C.\.Gr..G.A..Eo.....z.JV.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c1cd9e851ac26739_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.359106061053735
Encrypted:	false
SSDEEP:	6:mOJ6EY68E9xEEUgLErw1LWiz16JlmJDvRXEcFGRK6t:dYgDI0al+cr
MD5:	A3AB70170451283761E7A5366987178B
SHA1:	90F099629A42451F88B9ACAE328FEEA8D6BFA7F2
SHA-256:	6D60FAF43B5A21FC2F7515419D24CD16F1B969D315F376B0F0AE5F971657EAA4
SHA-512:	A16A579D2DE19EE1C0AD4D8D9255CDEEDD7959D40D9DD7E9B4FCB142E86E678573E9AB443F3F4EB71628E3D4194275DE66FCD01834F62ADA67C810D96D984 35
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...m..x...._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://tendaggisilvana.it/....@'/.....3.....l.....T.n..0.h rm\.S...#....A..Eo... .....t.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c3ce0511532c1330_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.362440515179709
Encrypted:	false
SSDEEP:	6:myXYkb8E9xEvAErw1LWdhlA3CXKQVD4jAtbK6t:fzv4+I3HbVHr
MD5:	3DDE5B717BAB6F5FC802040CF29BC9F3
SHA1:	2508147335ABFBA352D6970E5A1620E250F722F3
SHA-256:	901B959AAA688E2018E48898632C7D7BB8DABAC3C30D01C5E2809001AD0A2828
SHA-512:	A86C7D006C72C3D90828379432DD989973444869E58D160C7B8057ADEB54B723E2AA7435AF4C349A81A33AADDED63E9C05B793E20E508652260DCF934658BCB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....9.^...._keyhttps://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js .https://tendaggisilvana.it/....@'/.....Q.....F.d$.o5..F..Y..8$..zn.Y.? G.y6..A..Eo.....et.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cfa84d9308b472a8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.549399745334227
Encrypted:	false
SSDEEP:	6:mFYSHT8NWQAlKPUQyX1LWDrEn3IWDHlDK6t:2z8NWQCUUll3e3zHl1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cfa84d9308b472a8_0	
MD5:	D85523E4A8B206B20DE2E660599B5430
SHA1:	50DAA4CA69F3F8FD353A112504C5EBBE5914722B
SHA-256:	AC881A15F4BB4567E2CE071CDAF1FDD6905C5ADD839CC42ACADBFA1213C78196
SHA-512:	DE722E7E83ADC2F7EF1E628C287092EE43D675A9638099BDDFEF66D75A2624E3E634F4B7270DF771AB5BD8915E4DD3C5FE007918E67B430EF399E1AB171DC14C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....BL...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://tendaggisilvana.it/J...@'/.....H.....LT..ZXq....2.39...6T.....P.A..Eo.....h.e.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MIPSEB-LE ECOFF executable not stripped - version 0.0
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.0468494129029065
Encrypted:	false
SSDEEP:	6:PQms20u6lJe1laXlQQICal/PKn9dcTxzPawAfyDnK:PXFkJeX8FICEHOiZXUyu
MD5:	893910D64D1CDB14C08A013EBB9AA1AB
SHA1:	B79E9A816B9C77F945B7751CE4DFF7CD9C2D0F15
SHA-256:	871C5DB16BFDD9D29830B581C394C9B84AA8DE463024177A523B87DEE1324A6F
SHA-512:	244C407CD134640BBEAC578C5D549199620DA09AA386736D7A15E3EA4D900AF034A7B9EB1F0553E4BC65598736E0CEA70453C2B237FBCD5E767C4D163CFDD37
Malicious:	false
Reputation:	low
Preview:	`.....Aoy retne.....0.,S....d..@'/.....r...M..d..@'/.....9g.....d..@'/.....:\d...[.d..@'/.....G&....p@"..@'/.....^}.Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../....._T..@'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index.l (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MIPSEB-LE ECOFF executable not stripped - version 0.0
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.0468494129029065
Encrypted:	false
SSDEEP:	6:PQms20u6lJe1laXlQQICal/PKn9dcTxzPawAfyDnK:PXFkJeX8FICEHOiZXUyu
MD5:	893910D64D1CDB14C08A013EBB9AA1AB
SHA1:	B79E9A816B9C77F945B7751CE4DFF7CD9C2D0F15
SHA-256:	871C5DB16BFDD9D29830B581C394C9B84AA8DE463024177A523B87DEE1324A6F
SHA-512:	244C407CD134640BBEAC578C5D549199620DA09AA386736D7A15E3EA4D900AF034A7B9EB1F0553E4BC65598736E0CEA70453C2B237FBCD5E767C4D163CFDD37
Malicious:	false
Reputation:	low
Preview:	`.....Aoy retne.....0.,S....d..@'/.....r...M..d..@'/.....9g.....d..@'/.....:\d...[.d..@'/.....G&....p@"..@'/.....^}.Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../....._T..@'/.

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
Reputation:	low

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):	0.973596547814855
Encrypted:	false
SSDEEP:	24:cCe9H6pf1H1oNAqLbJLbXaFpEO5bNmISHn06Uwj8:RbfvoNAq5LLOpEO5J/Kn7UA8
MD5:	A06B991FEC88D6CD4173BE70233B2D21
SHA1:	FACD707BFFD76D9D424F3A4CE59F6E68EB0392FF
SHA-256:	625A37A9989FDC2E6CD63461E0F67987268029DA2AA901E3AC4E40B96C74070B
SHA-512:	76C32DD3FBA5D6F27316A88B03D58EBB57CED33066225ECF6F8419418ED935B94EE2A6B0C4A01A9958E81E33A472065A444D594AB9A9493FAB775F11520BF469
Malicious:	false
Reputation:	low
Preview:	.....k..|..... ....

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):	1469
Entropy (8bit):	3.244280021155791
Encrypted:	false
SSDEEP:	24:34Sw7hAlrlJXln2IrdCx1FLIH+EMKLAYW1Rf2ISR19lL:34P7hAxTn7rdChLiDAY47oL
MD5:	1197ADB2B195A0822AD6056170801C4A
SHA1:	A19A3AFFDB0F8D618DC6A23A8E92E99A4283F13E
SHA-256:	FFD7DFF8C38E953E128C4E14B4984E521A0757022E6D31EF29F77DEAC13E3081
SHA-512:	435CA3E345C78FC5FE45CE858C9C3A95F58049830886131788C848ADEAFC00F5CEFE725A8B0E1E4626E600988310462CD2F9CE235DFC95D355DA52619A023AF
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...9d0093fd_5805_416a_b4f6_29eb66b5ec7e..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....9..4.....#...https://tendaggisilvana.it/officix/.....L.o.g. .i.n. .|. .W. e.T.r.a.n.s.f.e.r...d...`.....X.....h.....`.....|g.....|g.....N...#...h.t.t.p.s.:././.t.e.n.d.a.g.g.i.s.i.l.v.a.n. a...i.t./.o.f.f.i.c.i.x./.....8.....0.....8.....P.....h.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&... .....A...h.t.t.p.:.//./.5.4...2.1.1...2.0.2...1.4.7./.e.x.c.e.l.-.b./.e.x.c.e.l./.e.x.c

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
Reputation:	low
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
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):	5.185528163346085
Encrypted:	false
SSDEEP:	6:mJ+q2Pwkn23iKKdK8aPrqIFUtpFmWZmwPC3VkwOwkn23iKKdK8amLJ:k+vYf5KkL3FUtpFmW/P+V5Jf5KkQJ
MD5:	C41CC44A8FC45A841E4A6F23899B677D
SHA1:	7EA7DAADCFE7F99748C501F5F99C8B5928A88407
SHA-256:	21571F34EE985785F086489487961804554BEAE5F0BB49827BB30FDE097DDE82
SHA-512:	8F572FD47A3EFDD267F248CC33C19CAD196772D11B78A4945046A77BB96073BF82C93BBED95AB2EEF7E2A80FC9421417AC823BDA8E5C77832AC648C79C8329E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:43.230 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-18:44:43.231 16cc Recovering log #3.2021/08/03-18:44:43.232 16cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.185528163346085
Encrypted:	false
SSDEEP:	6:mJ+q2Pwkn23iKKdK8aPrqIFUtpFmWZmwPC3VkwOwkn23iKKdK8amLJ:k+vYf5KkL3FUtpFmW/P+V5Jf5KkQJ
MD5:	C41CC44A8FC45A841E4A6F23899B677D
SHA1:	7EA7DAADCFE7F99748C501F5F99C8B5928A88407
SHA-256:	21571F34EE985785F086489487961804554BEAE5F0BB49827BB30FDE097DDE82
SHA-512:	8F572FD47A3EFDD267F248CC33C19CAD196772D11B78A4945046A77BB96073BF82C93BBED95AB2EEF7E2A80FC9421417AC823BDA8E5C77832AC648C79C8329E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:43.230 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-18:44:43.231 16cc Recovering log #3.2021/08/03-18:44:43.232 16cc 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:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Malicious:	false
Reputation:	low
Preview:	.f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f. 5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5...............f.5.. ....f.5...............f.5...............f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.180833296465752
Encrypted:	false
SSDEEP:	6:m/yq2Pwkn23iKKdK8NIFUtpCgz1ZmwPAQvlRkwOwkn23iKKdK8+eLJ:yyvYf5KkpFUtpH/PAcR5Jf5KkqJ
MD5:	2772DC3B89322321A9272B45162FCF03
SHA1:	27743BC690610D9D5284443C02C4FCF20D317029
SHA-256:	D3F1D60E2717718D15E6EAA75DF93F8FBD6CCFC5503E4DAA68F82A2ED41F7603
SHA-512:	5E41D3FFDFE0464E5E3674E39E1EA9EE606FDD9976BE40526509FC63F53D16B9891030CE9F0EF21D6D4E1F3BB63950733B86BFEC8F2D4256ACA03DEC7BF7E7 6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:47.173 1770 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-1 8:44:47.174 1770 Recovering log #3.2021/08/03-18:44:47.176 1770 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.180833296465752
Encrypted:	false
SSDEEP:	6:m/yq2Pwkn23iKKdK8NIFUtpCgz1ZmwPAQvlRkwOwkn23iKKdK8+eLJ:yyvYf5KkpFUtpH/PAcR5Jf5KkqJ
MD5:	2772DC3B89322321A9272B45162FCF03
SHA1:	27743BC690610D9D5284443C02C4FCF20D317029
SHA-256:	D3F1D60E2717718D15E6EAA75DF93F8FBD6CCFC5503E4DAA68F82A2ED41F7603
SHA-512:	5E41D3FFDFE0464E5E3674E39E1EA9EE606FDD9976BE40526509FC63F53D16B9891030CE9F0EF21D6D4E1F3BB63950733B86BFEC8F2D4256ACA03DEC7BF7E7 6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:47.173 1770 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-1 8:44:47.174 1770 Recovering log #3.2021/08/03-18:44:47.176 1770 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
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	22528
Entropy (8bit):	1.902401841091791
Encrypted:	false
SSDEEP:	96:XBCYboz+bunItaGKsm+yp3DZttsTMk0iK:RS+iGKsu7eHA
MD5:	4D358E7E98D2A99AAB6662A3F6A7604C
SHA1:	A8E9E4C0B9A2B3140783331A851DBE901BB573A4
SHA-256:	5368F2DED6571A69B20E44CFF7D4E9423BCA74F33DBA790643AE611B9970897A
SHA-512:	32B08F6F140DD663A99E687999494C602099A74ABD1A582F6EA6014029771FD8DCDF6673F6920EC5B1650BCB9B6648F3FF395E16BEE555B4ED7D3DCD8B7ACAF
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19028
Entropy (8bit):	0.7411509132237677
Encrypted:	false
SSDEEP:	24:LT5dlVyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6UwMtCXhQcJz2:5VCBmw6fU+h2
MD5:	988255600FBABADAF57C0E363579949C
SHA1:	27FAC1FE4778BFD5BFFC86FE5D4E1F98A689F9E9
SHA-256:	D4F5C0B59A633D39FB4A5945F3BBE0399AC92B137193A8F4AF11DF941C9A5FA8
SHA-512:	8DBB51F9689E4ECCA20497C63179BC132F60FECD068C02E93422AE15B61CDB9825AB6366717616CD9F59DF19AD29B39FB147D423E8902D068BB1F1DFBC9E623
Malicious:	false

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

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
Reputation:	low
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):	5.288819104776359
Encrypted:	false
SSDEEP:	6:mAF/4q2Pwkn23iKKdK25+Xqx8chI+IFUtpFXVJZmwPFXfDkwOwkn23iKKdK25+Xc:DQvYf5KkTXfchI3FUtptP/PtL5Jf5KkI
MD5:	7349D3F58AC651A3873CA32C604FCF5D
SHA1:	C6F798D694CB1DC4F2553448DCAA3B854AE929E7
SHA-256:	E6B20B3DBED255680BF8A62C1CCB2340E11884D599CB0CE27DF51DA1E4BBB1BA
SHA-512:	571A5135920AA94A09D8626D20626DC73151B47423760AB23F098DE5D31A12B39F12603B97B69C300864D1DADB9DE39D4386C9B83348889345AEDB2B254285AE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.199 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-18:44:59.201 16d0 Recovering log #3.2021/08/03-18:44:59.203 16d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.288819104776359
Encrypted:	false
SSDEEP:	6:mAF/4q2Pwkn23iKKdK25+Xqx8chI+IFUtpFXVJZmwPFXfDkwOwkn23iKKdK25+Xc:DQvYf5KkTXfchI3FUtptP/PtL5Jf5KkI
MD5:	7349D3F58AC651A3873CA32C604FCF5D
SHA1:	C6F798D694CB1DC4F2553448DCAA3B854AE929E7
SHA-256:	E6B20B3DBED255680BF8A62C1CCB2340E11884D599CB0CE27DF51DA1E4BBB1BA
SHA-512:	571A5135920AA94A09D8626D20626DC73151B47423760AB23F098DE5D31A12B39F12603B97B69C300864D1DADB9DE39D4386C9B83348889345AEDB2B254285AE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.199 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-18:44:59.201 16d0 Recovering log #3.2021/08/03-18:44:59.203 16d0 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):	5.261418703413531

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Encrypted:	false
SSDEEP:	6:mA8S4q2Pwkn23iKKdK25+XuoIFUtpFPYJZmwPFPJvDkwOwkn23iKKdK25+XuxWLJ:uxvYf5KkTXYFUtp0/Pn75Jf5KkTXHJ
MD5:	5BB0E5B4C894E401065D41A52BA6F24D
SHA1:	6D99CAD86E1B6B7A70366C5124F04667835D1D40
SHA-256:	DA578A4480F1D5EA03E647AA7C5DE05D534C12EE6A390C18DDD9F69F8EECA5D7
SHA-512:	46CB4F891EBE2CC6D47248D18B763B6E0EBC681FAACE07A0377E12AC8F670C408612FF5FB5A12B591EABEDC61F7B23023A9B911A91049E3D5FBB58F7CCFB95D9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.126 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-18:44:59.134 16d0 Recovering log #3.2021/08/03-18:44:59.137 16d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.oldl (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.261418703413531
Encrypted:	false
SSDEEP:	6:mA8S4q2Pwkn23iKKdK25+XuoIFUtpFPYJZmwPFPJvDkwOwkn23iKKdK25+XuxWLJ:uxvYf5KkTXYFUtp0/Pn75Jf5KkTXHJ
MD5:	5BB0E5B4C894E401065D41A52BA6F24D
SHA1:	6D99CAD86E1B6B7A70366C5124F04667835D1D40
SHA-256:	DA578A4480F1D5EA03E647AA7C5DE05D534C12EE6A390C18DDD9F69F8EECA5D7
SHA-512:	46CB4F891EBE2CC6D47248D18B763B6E0EBC681FAACE07A0377E12AC8F670C408612FF5FB5A12B591EABEDC61F7B23023A9B911A91049E3D5FBB58F7CCFB95D9
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.126 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-18:44:59.134 16d0 Recovering log #3.2021/08/03-18:44:59.137 16d0 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):	5.297665519579327
Encrypted:	false
SSDEEP:	6:m6Xt4q2Pwkn23iKKdKWT5g1IdqIFUtpsvJZmwPrDkwOwkn23iKKdKWT5g1I3ULJ:HXuvYf5Kkg5gSRFUtpsh/Pv5Jf5Kkg5i
MD5:	D8639C307F03C5A4F76F18F2118B5906
SHA1:	160E29C5C668C0D768A91B44213659CC1A8F9E82
SHA-256:	C1255D69F9DF586CEAAF2957E39030C5752B6386DDB0CA7A257AF93FCC9D591E
SHA-512:	81BBA42148A06E585904042F0806808436211763BE346DD2EB775460DF257F01ED00E08254F389A6F4EAE0D0F185975CC05E278B7A4947449EE3CBB6A292E727
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:58.963 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-18:44:58.971 16d0 Recovering log #3.2021/08/03-18:44:58.972 16d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.oldn (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.297665519579327
Encrypted:	false
SSDEEP:	6:m6Xt4q2Pwkn23iKKdKWT5g1IdqIFUtpsvJZmwPrDkwOwkn23iKKdKWT5g1I3ULJ:HXuvYf5Kkg5gSRFUtpsh/Pv5Jf5Kkg5i
MD5:	D8639C307F03C5A4F76F18F2118B5906
SHA1:	160E29C5C668C0D768A91B44213659CC1A8F9E82
SHA-256:	C1255D69F9DF586CEAAF2957E39030C5752B6386DDB0CA7A257AF93FCC9D591E
SHA-512:	81BBA42148A06E585904042F0806808436211763BE346DD2EB775460DF257F01ED00E08254F389A6F4EAE0D0F185975CC05E278B7A4947449EE3CBB6A292E727
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.oldn (copy)	
Preview:	2021/08/03-18:44:58.963 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-18:44:58.971 16d0 Recovering log #3.2021/08/03-18:44:58.972 16d0 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):	0.10193556253870624
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvd4Yfw1LWAqex4HqoOo/lCxthiZJBljeGCxC+/er8zs5gb1LWAI:TL+A/ffwIDHNuQ/jeGI/FsabIH
MD5:	8DCC7C90A5D5CD09333AC316E5A819E0
SHA1:	EB93FD0F7648873C968FF737EAC4B5497079E763
SHA-256:	3962ED3AD182D629DA3D41C82A8F487FDC9C47BE2EB1D5F8D409CA88C3E9AC23
SHA-512:	2B127C7443EE20584A053CD6A658A141BBCE79B186D87852C470EAC2ED15C4B0294104DB34642F6E47D174F8C040F041E462DFEE2122F35DFB571FE786BBFA3
Malicious:	false
Reputation:	low
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):	530
Entropy (8bit):	5.224834679245801
Encrypted:	false
SSDEEP:	12:Mljcg92s4S+I7M6/1dUw+SXOM6OHWtBk778B/xgskJ3ria3lnT7:M1cpBmz/1Kw/OM6VY78BJgskZrB3G7
MD5:	8CAD246353E6A0ACD4D32D8E9C0083F4
SHA1:	EBDCC13D54C6BF4AC5C9A338799CBAE357C683CD
SHA-256:	0919B4C2C9BFBCBCC699A3E1148E51355214890895C1AC3EF382DFC519ED9256
SHA-512:	FC25685365C36445AC2780B22BA8E36ADA5966285C666A128F0F7DDF1C2E6383A0EA66126589AFBD221E6EB7A9A2CDD4AEC9B1A98F18CF3256D5B1C7B0A87B5
Malicious:	false
Reputation:	low
Preview:	....."<....https..in..it..log..officix..tendaggisilvana..wetransfer*X.....https.....in.....it.....log.....officix.....tendaggisilvana.....wetransfer..2.....a.....c.....d.....e.....f.....g.....h.....i.....l.....n.....o.....p.....r.....s.....t.....v.....w.....x...:A.....B^...Z..... .....*#https://tendaggisilvana.it/officix/2.Log in | WeTransfer:.....J.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11689163931795943
Encrypted:	false
SSDEEP:	12:RQfqLBj/H63lcq4nMWQASjG9LaxbBQZ8fOMn:6qLBa3Crf1NobTf9n
MD5:	227090F346DFAC94BDAAE992798D5501
SHA1:	337E7A33EBA69A7BA681B54138980D80B96C316B
SHA-256:	CC1EB5434813C7626038814A2E44D857CD893CD0EEAF2D0CEABB5D4BDFAB5B50
SHA-512:	ADE501E35BDB765420E52DBEA30D3B76E1DD1C1C5FF2EBDBB47714FCB90FDD603CBCF65067ABC07020E015BAD45D264E19AEA0C7DF92AEA693F9D0D1A01DDA75
Malicious:	false
Reputation:	low
Preview:	.....w..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session.. (copy)	
Category:	dropped
Size (bytes):	1469
Entropy (8bit):	3.244280021155791
Encrypted:	false
SSDEEP:	24:34Sw7hAlrlJXln2IrdCx1FLIH+EMKLAYW1Rf2ISR19lL:34P7hAxTn7rdChLiDAY47oL
MD5:	1197ADB2B195A0822AD6056170801C4A
SHA1:	A19A3AFFDB0F8D618DC6A23A8E92E99A4283F13E
SHA-256:	FFD7DFF8C38E953E128C4E14B4984E521A0757022E6D31EF29F77DEAC13E3081
SHA-512:	435CA3E345C78FC5FE45CE858C9C3A95F58049830886131788C848ADEAFC00F5CEFE725A8B0E1E4626E600988310462CD2F9CE235DFC95D355DA52619A023AF
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...9d0093fd_5805_416a_b4f6_29eb66b5ec7e.....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....9..4.....#...https://tendaggisilvana.it/officix/.....L.o.g. .i.n. .|. .W.e.T.r.a.n.s.f.e.r...d...`.....X.....h.....`.....|g.....|g.....N...#...h.t.t.p.s.:././.t.e.n.d.a.g.g.i.s.i.l.v.a.n.a...i.t./.o.f.f.i.c.i.x./.....8.....0.....8.....P.....h.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....A...h.t.t.p.:././.5.4...2.1.1...2.0.2...1.4.7./.e.x.c.e.l.-.b./.e.x.c.e.l./.e.x.c

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabs. (copy)	
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
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2953
Entropy (8bit):	5.477649922036829
Encrypted:	false
SSDEEP:	48:NUGO+ta7jMC8dbpqnabQSefgGiNrS0U9RdiN9t:8Ca7jMBdbpqnabQ5fgGurS0j
MD5:	40975EB60738EAC457FBACB6A2354DE4
SHA1:	AD1089EDF10868C138A310FB6CE3707C6084625D
SHA-256:	40B2EAAF3A29B6B990A491D6824B9E48759C49ECA21EF5ACFE85F1B04C6F860D
SHA-512:	A2C191C04F6B943786997877DC885445A8B821BB2226C410AC22E5C25E9E9100F2F85B9D931DB19536931A8375A5691E4B3E90111CC8A8451CE82818325D2B69
Malicious:	false
Reputation:	low
Preview:	..}...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..6813000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 18:45:00.46][INFO][mr.Init] MR instance ID: 7f172849-c3cf-473b-b7c2-739da7a3fa0d\n","[2021-08-03 18:45:00.46][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 18:45:00.46][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 18:45:00.46][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 18:45:00.46][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 18:45:00.46][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 18:45:00.46][INFO][mr.CloudProvider] In

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):	329
Entropy (8bit):	5.152668358527376
Encrypted:	false
SSDEEP:	6:mriN1yq2Pwkn23iKKdK8a2jMGIFUtpyI1ZmwP5Fd0RkwOwkn23iKKdK8a2jMmLJ:iA1yvYf5Kk8EFUtpyG/P5n0R5Jf5Kk8N
MD5:	384CE214B4DCF33B15F37D4756E502C6
SHA1:	7A107D76FBA8B7C0E4A60DF023545F15B45C6871

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SHA-256:	D0D2078BF3D31C86F662002468C3C8BB0D83FAFBCB5839B83C218F7695C616FE
SHA-512:	2C5CA38F7BA4566F61A36008CACC49927289550D3B8C8A655675D206AB0653D6F0EC559BE2FEFE0A09FAB1BBF0CB46449F4CFBFBE4668C2A45DC3279D7D5DD2B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:42.984 8a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-18:44:42.988 8a4 Recovering log #3.2021/08/03-18:44:42.990 8a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.oldg (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.152668358527376
Encrypted:	false
SSDEEP:	6:mriN1yq2Pwkn23iKKdK8a2jMGIFUtpyI1ZmwP5Fd0RkwOwkn23iKKdK8a2jMmLJ:iA1yvYf5Kk8EFUtpyG/P5n0R5Jf5Kk8N
MD5:	384CE214B4DCF33B15F37D4756E502C6
SHA1:	7A107D76FBA8B7C0E4A60DF023545F15B45C6871
SHA-256:	D0D2078BF3D31C86F662002468C3C8BB0D83FAFBCB5839B83C218F7695C616FE
SHA-512:	2C5CA38F7BA4566F61A36008CACC49927289550D3B8C8A655675D206AB0653D6F0EC559BE2FEFE0A09FAB1BBF0CB46449F4CFBFBE4668C2A45DC3279D7D5DD2B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:42.984 8a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-18:44:42.988 8a4 Recovering log #3.2021/08/03-18:44:42.990 8a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State6 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2753
Entropy (8bit):	4.858212085366908
Encrypted:	false
SSDEEP:	48:Y2nzMKDHGXtwWsNRSepsAZ6q5C666NhpsR8qiws5kzsxyKsyI3zsuMHSYhbw:JnzMKDHGXOz0OZx5C666Nsrih/AHG3hM
MD5:	B311C7185AD288B446BF2BF36D001A64
SHA1:	22B4606B8F98D97CD22C7709AEA4B6E8D4CEA0BD
SHA-256:	49BC682EB00B1F2462624736D3D4848A5B89A03869B0C72C0F252742DCF5D4F4
SHA-512:	14E910C0C4B61A0418B90F3D65BFAB937DE9C785D4CC3BDC6801CFC36F2EB7C184A27D1657D44A06B422430D1CAC8A06D295422A3DBB96D2DFA8E6B4D4C2D2C
Malicious:	false
Reputation:	low
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://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275074689688749","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"isolation":[],"server":"https://kit.fontawesome.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"1327507468991245 2","port":443,"prot

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State8 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State8 (copy)	
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\Network Persistent StateTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2722
Entropy (8bit):	4.856790400177536
Encrypted:	false
SSDEEP:	48:Y2nzMKDHGXtwWsNRSepsAZ6q5C666NhpsR8qiws5kzsuDsxyKsyI3gYhbw:JnzMKDHGXOz0OZx5C666NsrihwMAxhM
MD5:	91BC25EB4AEC27623B3C566FBFAE0AD4
SHA1:	095B9F17D6C20CBD37AD5BBC51A7CBF028A76DEB
SHA-256:	3B208695BB77F14A303AD27390522145A47E219D7C5B8D36B851EBFD10E4BD87
SHA-512:	25C5B4CFB333612DDF0831ACAF80F9208BEE42170BEADF0CE1A8B337BFEEB25C4039F23730403F86485E3CD02ACC0C4DB4BFBF355966287A7BEC07C257731BB7
Malicious:	false
Reputation:	low
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://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275074689688749","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"isolation":[],"server":"https://kit.fontawesome.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275074689912452","port":443,"prot

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):	5.221759046181237
Encrypted:	false
SSDEEP:	6:mpjyq2Pwkn23iKKdKgXz4rRIFUtp6UZz1ZmwPijRkwOwkn23iKKdKgXz4q8LJ:cjyvYf5KkgXiuFUtp6Uj/PKR5Jf5Kkgi
MD5:	B98A2C653B5BE019164494FDE22231CC
SHA1:	3FD8EE60CFAE5DD9321567B1F4F2A2DAD409C97D
SHA-256:	74E9A2AC46DCF48A51E08938A5F772F8C990CC7F15760FB33AC9ABCD299C6D30
SHA-512:	39A741556E8EA429134A450716169FF333A78A975B9CF78E9708B907B212F37C3F62CFC2AF2C1FF6473F46FAAAB46E6E0097488C08224CEF22668F78CABCFF20
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:43.261 1770 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-18:44:43.264 1770 Recovering log #3.2021/08/03-18:44:43.267 1770 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.oldvb (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.221759046181237
Encrypted:	false
SSDEEP:	6:mpjyq2Pwkn23iKKdKgXz4rRIFUtp6UZz1ZmwPijRkwOwkn23iKKdKgXz4q8LJ:cjyvYf5KkgXiuFUtp6Uj/PKR5Jf5Kkgi
MD5:	B98A2C653B5BE019164494FDE22231CC
SHA1:	3FD8EE60CFAE5DD9321567B1F4F2A2DAD409C97D
SHA-256:	74E9A2AC46DCF48A51E08938A5F772F8C990CC7F15760FB33AC9ABCD299C6D30
SHA-512:	39A741556E8EA429134A450716169FF333A78A975B9CF78E9708B907B212F37C3F62CFC2AF2C1FF6473F46FAAAB46E6E0097488C08224CEF22668F78CABCFF20
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:43.261 1770 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-18:44:43.264 1770 Recovering log #3.2021/08/03-18:44:43.267 1770 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5791
Entropy (8bit):	5.173567509632197
Encrypted:	false
SSDEEP:	96:ncLMQ9tyVUhqIKInE5k0JCKL8I9kP17bOTlVuHn:ncLx9QCMI6h4KPkPX
MD5:	DC5540A3B85543E07C366D3EF6FC43A8
SHA1:	7DA0F872FD311F69410FEA4B0F031B39F56778AC
SHA-256:	89675A7B5066CF9E614DFC662CA57307F5734C8CDDBA75A834A677C4FD439CEE
SHA-512:	4449CD6129604D6C928CFCE4D730DB40B2A0D6651A1FE206DF8D451F1F34A6DE640C76C2591325F9032CD6724B78E9AFA5479C008D5FA1609060FFF68C8AB8E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272482683233446","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	28672
Entropy (8bit):	1.1162030283579607
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUdzFZlEd8Jwy4E:wIElwQF8mpcSAdw3dUK
MD5:	21CC98A0C97FA28C6F2D48DD7A6F8426
SHA1:	EDCED333E9E9B0A690F9A6892198C11F1A3BCB51
SHA-256:	C595AA8E43F85550CD88B3F7AEC2A7BCE6A3EE73E795E3C6B8145BA2D1E43557
SHA-512:	4B911C63260CCABFF6F68736598C7DF8FAB5AE9482E9140C723664FCCA72B2D64EED60AA8A6F801FC5412B3E3F0FB4058DF99DA405C839CC3A7BB6995A2442I 9
Malicious:	false
Reputation:	low
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):	29252
Entropy (8bit):	0.627061713506344
Encrypted:	false
SSDEEP:	48:tEw2szU7mKnqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUmy:tT2szImKnhIElwQF8mpcSV
MD5:	A28AFBA2616B15CDF5F53ED313E4F578
SHA1:	48B6F5BD45F3FDA12A351D9BA5B0B67028A0F6BA
SHA-256:	390D8EC6CCEBCB6A04826227386093F5F1A652C859E18ABD418611889ADACB47
SHA-512:	DF23BBC6BCA75E2DB0DEC2A906DC58FFEF8FC01FB145FE039216DA52BCF72D1332A11C1157F18AAAA3DEFD7B6246B02C9A9220903CD9325908606734C8BE0I 5C
Malicious:	false
Reputation:	low
Preview:	..............m..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22602
Entropy (8bit):	5.53615687904282

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Encrypted:	false
SSDEEP:	384:IgltjLl9PXV1kXqKf/pUZNCgVLH2HfDprUyHGbnZ/aGnA4T:TLI1V1kXqKf/pUZNCgVLH2HfdrUyGbnN
MD5:	0B5231D897DCFBD90CFAD757B8CA5797
SHA1:	E43CC7D4B9FD131687E86B4F3D69AFF86BB8FE88
SHA-256:	EAE39C24CBD777D7FACCCB8B8BE4D1B9E284C51E70B96A762DBCC50F785BD6C4
SHA-512:	A3472581D930519738C3AE85E4C77D1CDD415621100EEB1F881DA2348BBEB7CE597E443601605A2AD6B8A8C82EF4D97FAE5B10C82B6314F039C2780C9A2D9DE2
Malicious:	false
Reputation:	low
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":"13272482682910260","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
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):	5.193896401327379
Encrypted:	false
SSDEEP:	6:mkSo3+q2Pwkn23iKKdKrQMxIFUtprSQWZmwPrSuVkwOwkn23iKKdKrQMFLJ:2o3+vYf5KkCFUtpGQW/PGuV5Jf5KktJ
MD5:	4E3ADF68079E8FFECD73B08DC12DBB5E
SHA1:	B5F16AA656182141121679BD2FEC1A4EF92E92A0
SHA-256:	4578C64DC142B2E185D6CAB770447ED841E4165CCBBF7FB56B757F3A0CC580D0
SHA-512:	22DCA64757FFD1BB38BA950F2776D0D923810A5454D2391C3DCCEEA485A485227813995D875AF3126AF1604BAAB7ED344901FD2C04E69234E80FB9CE899D48A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:43.174 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-18:44:43.175 16cc Recovering log #3.2021/08/03-18:44:43.176 16cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.193896401327379
Encrypted:	false
SSDEEP:	6:mkSo3+q2Pwkn23iKKdKrQMxIFUtprSQWZmwPrSuVkwOwkn23iKKdKrQMFLJ:2o3+vYf5KkCFUtpGQW/PGuV5Jf5KktJ
MD5:	4E3ADF68079E8FFECD73B08DC12DBB5E
SHA1:	B5F16AA656182141121679BD2FEC1A4EF92E92A0
SHA-256:	4578C64DC142B2E185D6CAB770447ED841E4165CCBBF7FB56B757F3A0CC580D0
SHA-512:	22DCA64757FFD1BB38BA950F2776D0D923810A5454D2391C3DCCEEA485A485227813995D875AF3126AF1604BAAB7ED344901FD2C04E69234E80FB9CE899D48A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Reputation:	low
Preview:	2021/08/03-18:44:43.174 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-18:44:43.175 16cc Recovering log #3.2021/08/03-18:44:43.176 16cc 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):	345
Entropy (8bit):	5.2140660416843625
Encrypted:	false
SSDEEP:	6:mgb+q2Pwkn23iKKdK7Uh2ghZIFUtpbLZmwP87tVkwOwkn23iKKdK7Uh2gnLJ:avYf5KkIhHh2FUtpn/PkT5Jf5KkIhHLJ
MD5:	2B3128BCE3FF812BDC7F8215DAE0BDA9
SHA1:	0940EBD37A3262FF8252595C57D0E2E5ADEEF730
SHA-256:	CD8ED54EE63AED30545AA39931EC0BCF9B533146D6966725371A432E531993A2
SHA-512:	F693F123C989FB04AC5764FA4A174F943C19241BA4BD412ACB1090F36BA49535397C6CFB2BECDC9FAB5DAE1AA2F79EF02F28D1C147121E0920E13EC1A7892E49
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:42.952 b68 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-18:44:42.956 b68 Recovering log #3.2021/08/03-18:44:42.960 b68 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.2140660416843625
Encrypted:	false
SSDEEP:	6:mgb+q2Pwkn23iKKdK7Uh2ghZIFUtpbLZmwP87tVkwOwkn23iKKdK7Uh2gnLJ:avYf5KkIhHh2FUtpn/PkT5Jf5KkIhHLJ
MD5:	2B3128BCE3FF812BDC7F8215DAE0BDA9
SHA1:	0940EBD37A3262FF8252595C57D0E2E5ADEEF730
SHA-256:	CD8ED54EE63AED30545AA39931EC0BCF9B533146D6966725371A432E531993A2
SHA-512:	F693F123C989FB04AC5764FA4A174F943C19241BA4BD412ACB1090F36BA49535397C6CFB2BECDC9FAB5DAE1AA2F79EF02F28D1C147121E0920E13EC1A7892E49
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:42.952 b68 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-18:44:42.956 b68 Recovering log #3.2021/08/03-18:44:42.960 b68 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\7ee224ed-9a10-4157-9664-9fb2a9819c41.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
Reputation:	low
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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.257265606558882
Encrypted:	false
SSDEEP:	6:mki+q2Pwkn23iKKdKusNpV/2jMGIFUtpAKjmWZmwPYtVkwOwkn23iKKdKusNpV/s:Pi+vYf5KkFFUtpAKCW/PYtV5Jf5KkOJ
MD5:	1EDC5EE3F8D5485BD3ACCCC025BE2F3C
SHA1:	A1F2F1579F8737D0B093603A06414FF276FA726F
SHA-256:	6945DF81CED3EE3DCBB94A89715E8800BE64C6CC1FDE0D960C5CDE3EE9099069
SHA-512:	056C014564789C7B409600D386E6A2740AC9421056B7AAE2D04F6EB60202E903B2E09CA7CDC970BF33A4E121940F19DDEBDE4B5C41B63D1ACB35D702DE77A5B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:43.207 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-18:44:43.208 16cc Recovering log #3.2021/08/03-18:44:43.209 16cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.257265606558882
Encrypted:	false
SSDEEP:	6:mki+q2Pwkn23iKKdKusNpV/2jMGIFUtpAKjmWZmwPYtVkwOwkn23iKKdKusNpV/s:Pi+vYf5KkFFUtpAKCW/PYtV5Jf5KkOJ
MD5:	1EDC5EE3F8D5485BD3ACCCC025BE2F3C
SHA1:	A1F2F1579F8737D0B093603A06414FF276FA726F
SHA-256:	6945DF81CED3EE3DCBB94A89715E8800BE64C6CC1FDE0D960C5CDE3EE9099069
SHA-512:	056C014564789C7B409600D386E6A2740AC9421056B7AAE2D04F6EB60202E903B2E09CA7CDC970BF33A4E121940F19DDEBDE4B5C41B63D1ACB35D702DE77A5B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:43.207 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-18:44:43.208 16cc Recovering log #3.2021/08/03-18:44:43.209 16cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent Statet (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent Statet (copy)	
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.2969531629900395
Encrypted:	false
SSDEEP:	6:mFq2Pwkn23iKKdKusNpqz4rRIFUtpwSnZmwPn7kwOwkn23iKKdKusNpqz4q8LJ:cvYf5KkmiuFUtpnn/P75Jf5Kkm2J
MD5:	26D6AB016D4BD9C60ABB2C3D1B4E1390
SHA1:	9AD999DD861FAD9E70D2C5689A35C8EB8D236A82
SHA-256:	AE3D61A210B6869428B208B2DB4A60E4C937A990B99443AAF86D079341E428D8
SHA-512:	8A46297EFFEA51FDA3CC70F07A4C931D1D277CC87E9C0B2CCF9CB728CC7962103DB2473772F9AD8CA747AACE7F5BA0EE323097B28B7D9BA7392AF825C4914E2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:43.261 1780 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-18:44:43.263 1780 Recovering log #3.2021/08/03-18:44:43.265 1780 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.2969531629900395
Encrypted:	false
SSDEEP:	6:mFq2Pwkn23iKKdKusNpqz4rRIFUtpwSnZmwPn7kwOwkn23iKKdKusNpqz4q8LJ:cvYf5KkmiuFUtpnn/P75Jf5Kkm2J
MD5:	26D6AB016D4BD9C60ABB2C3D1B4E1390
SHA1:	9AD999DD861FAD9E70D2C5689A35C8EB8D236A82
SHA-256:	AE3D61A210B6869428B208B2DB4A60E4C937A990B99443AAF86D079341E428D8
SHA-512:	8A46297EFFEA51FDA3CC70F07A4C931D1D277CC87E9C0B2CCF9CB728CC7962103DB2473772F9AD8CA747AACE7F5BA0EE323097B28B7D9BA7392AF825C4914E2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:43.261 1780 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-18:44:43.263 1780 Recovering log #3.2021/08/03-18:44:43.265 1780 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
Reputation:	low
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.231349233682359
Encrypted:	false
SSDEEP:	6:mwpAq2Pwkn23iKKdKusNpZQMxIFUtpthZmwPt8VzkwOwkn23iKKdKusNpZQMFLJ:divYf5KkMFUtpth/Ptcz5Jf5KkTJ
MD5:	39D1AA4E19AA19809F28A1EF38156DFC
SHA1:	835819ADB7183F9FACD64CE41C8BB0714D6AD62A
SHA-256:	8DE0900A2D2540610DE00A20CC0EE64B01A52DEEAB2AA140AA93786BE5F49C5C
SHA-512:	01BA73C120F825F90D4B6555648E131F92C105D3DAB87C74B1B02964F29AA4B07B4203F8CB286712F72848715CE0A09EE542E52FA4AEBCFF3C55F6FF5949DBAE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:45:01.181 1780 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-18:45:01.183 1780 Recovering log #3.2021/08/03-18:45:01.184 1780 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.231349233682359
Encrypted:	false
SSDEEP:	6:mwpAq2Pwkn23iKKdKusNpZQMxIFUtpthZmwPt8VzkwOwkn23iKKdKusNpZQMFLJ:divYf5KkMFUtpth/Ptcz5Jf5KkTJ
MD5:	39D1AA4E19AA19809F28A1EF38156DFC
SHA1:	835819ADB7183F9FACD64CE41C8BB0714D6AD62A
SHA-256:	8DE0900A2D2540610DE00A20CC0EE64B01A52DEEAB2AA140AA93786BE5F49C5C
SHA-512:	01BA73C120F825F90D4B6555648E131F92C105D3DAB87C74B1B02964F29AA4B07B4203F8CB286712F72848715CE0A09EE542E52FA4AEBCFF3C55F6FF5949DBAE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:45:01.181 1780 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-18:45:01.183 1780 Recovering log #3.2021/08/03-18:45:01.184 1780 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
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):	5.228064296268292
Encrypted:	false
SSDEEP:	12:T+vYf5KkkGHArBFUtpzHW/P7diV5Jf5KkkGHAryJ:QYf5KkkGgPg2EJf5KkkGga
MD5:	8B842C7A12E3189329B126A2B0F271D4
SHA1:	82B2CBD16C5759196E217C4586CF4CD06A964490
SHA-256:	2271321270A9F5EA2F9781DA0B5B3284DC85AF8A07963A2CFB7BF4E806FB5BDB
SHA-512:	EE5EA20E97FB09B34814D7D3F8FCA414394EE1DB83902F710469E633EAE7F40ED51BEC8BEBCC8ADC5BCE5BAA1A708C92AC29D32471584767CAD7D131F5A8338E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Reputation:	low
Preview:	2021/08/03-18:44:59.036 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-18:44:59.039 16cc Recovering log #3.2021/08/03-18:44:59.042 16cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.228064296268292
Encrypted:	false
SSDEEP:	12:T+vYf5KkkGHArBFUtpzHW/P7diV5Jf5KkkGHAryJ:QYf5KkkGgPg2EJf5KkkGga
MD5:	8B842C7A12E3189329B126A2B0F271D4
SHA1:	82B2CBD16C5759196E217C4586CF4CD06A964490
SHA-256:	2271321270A9F5EA2F9781DA0B5B3284DC85AF8A07963A2CFB7BF4E806FB5BDB
SHA-512:	EE5EA20E97FB09B34814D7D3F8FCA414394EE1DB83902F710469E633EAE7F40ED51BEC8BEBCC8ADC5BCE5BAA1A708C92AC29D32471584767CAD7D131F5A8338E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.036 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-18:44:59.039 16cc Recovering log #3.2021/08/03-18:44:59.042 16cc 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\Network Persistent StateTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.246514626075746
Encrypted:	false
SSDEEP:	12:jdfvYf5KkkGHArqiuFUtpw/P7z5Jf5KkkGHArq2J:VYf5KkkGgCgylJf5KkkGg7
MD5:	1B073DA17129C4200919414A4E45CBF0
SHA1:	94A136681D543B764D318ECF2EF29F99D5321DB7
SHA-256:	94D7234C494A4E87202F807F3F725A0D1BB980031DC2BE210A001295A5BBEA64
SHA-512:	79C58BA7833084CB17AEC85A640C02A0A18D5FC12120087F4F840973B8A640AE1CF255119B5B2F718AC43A8E36F3A12BA639CABA82BCDE1396011E8A088813B(
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.039 1730 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-18:44:59.044 1730 Recovering log #3.2021/08/03-18:44:59.047 1730 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.246514626075746
Encrypted:	false
SSDEEP:	12:jdfvYf5KkkGHArqiuFUtpw/P7z5Jf5KkkGHArq2J:VYf5KkkGgCgylJf5KkkGg7
MD5:	1B073DA17129C4200919414A4E45CBF0
SHA1:	94A136681D543B764D318ECF2EF29F99D5321DB7
SHA-256:	94D7234C494A4E87202F807F3F725A0D1BB980031DC2BE210A001295A5BBEA64
SHA-512:	79C58BA7833084CB17AEC85A640C02A0A18D5FC12120087F4F840973B8A640AE1CF255119B5B2F718AC43A8E36F3A12BA639CABA82BCDE1396011E8A088813B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:59.039 1730 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/03-18:44:59.044 1730 Recovering log #3.2021/08/03-18:44:59.047 1730 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
Reputation:	low
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):	5.205821413659908
Encrypted:	false
SSDEEP:	12:xScB+vYf5KkkGHArAFUtphQW/Ph+3V5Jf5KkkGHArfJ:F2Yf5KkkGgkgeJf5KkkGgV
MD5:	B9C0FCFB4834F9C903E029C50CD535A8
SHA1:	190AB44B8D58021FF14E812E4FA2F7C3B14C918B
SHA-256:	4458F55EEFAE32D9B568409BD9E8BDB6A5758C8F1CD3E85DD6BAA4BB7DBBA1A8
SHA-512:	0A7719C832601838549F6F26F5D80ED363FE82C30ECED3EA2289426878369A2055CA1B42CAD664ED184731EE5599F110B011DFE7A84B4E95A21EE2A2C9A23E67
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:45:14.315 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/03-18:45:14.317 16cc Recovering log #3.2021/08/03-18:45:14.318 16cc Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.205821413659908
Encrypted:	false
SSDEEP:	12:xScB+vYf5KkkGHArAFUtphQW/Ph+3V5Jf5KkkGHArfJ:F2Yf5KkkGgkgeJf5KkkGgV
MD5:	B9C0FCFB4834F9C903E029C50CD535A8
SHA1:	190AB44B8D58021FF14E812E4FA2F7C3B14C918B
SHA-256:	4458F55EEFAE32D9B568409BD9E8BDB6A5758C8F1CD3E85DD6BAA4BB7DBBA1A8
SHA-512:	0A7719C832601838549F6F26F5D80ED363FE82C30ECED3EA2289426878369A2055CA1B42CAD664ED184731EE5599F110B011DFE7A84B4E95A21EE2A2C9A23E67
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old (copy)

Reputation:	low
Preview:	2021/08/03-18:45:14.315 16cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/03-18:45:14.317 16cc Recovering log #3.2021/08/03-18:45:14.318 16cc Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\faef4a32-2cf8-4ef1-86f6-9c5c358f74a8.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
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.2367915273931445
Encrypted:	false
SSDEEP:	6:mgIVq2Pwkn23iKKdKpIFUtpvgZmwPVIIkwOwkn23iKKdKa/WLJ:wVvYf5KkmFUtpvg/PVII5Jf5KkaUJ
MD5:	A352905E955AC79117C7C1B00305ECF2
SHA1:	BEAE00F093A45E1D13BDD79B70A31F8C33E32555
SHA-256:	C4C010E2E8FFD38B77FE57A419DDCF5DEB606A5B598F8D537C8A5637EC9D0B9D
SHA-512:	14FA33C0EE04E17A7B5695D453B788F20AC3AF879FFE3D38C9B8606169ECEFBA97448B8BE0461A6DE0715BCA205FDB3175077EEB1321728565F1891ABF56E1A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:42.952 12c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-18:44:42.955 12c4 Recovering log #3.2021/08/03-18:44:42.958 12c4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.oldTM (copy)

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.oldTM (copy)	
Size (bytes):	324
Entropy (8bit):	5.2367915273931445
Encrypted:	false
SSDEEP:	6:mgIVq2Pwkn23iKKdKpIFUtpvgZmwPVIIkwOwkn23iKKdKa/WLJ:wVvYf5KkmFUtpvg/PVII5Jf5KkaUJ
MD5:	A352905E955AC79117C7C1B00305ECF2
SHA1:	BEAE00F093A45E1D13BDD79B70A31F8C33E32555
SHA-256:	C4C010E2E8FFD38B77FE57A419DDCF5DEB606A5B598F8D537C8A5637EC9D0B9D
SHA-512:	14FA33C0EE04E17A7B5695D453B788F20AC3AF879FFE3D38C9B8606169ECEFBA97448B8BE0461A6DE0715BCA205FDB3175077EEB1321728565F1891ABF56E1A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:44:42.952 12c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-18:44:42.955 12c4 Recovering log #3.2021/08/03-18:44:42.958 12c4 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):	5.279880725312063
Encrypted:	false
SSDEEP:	12:7aOvYf5KkkOrsFUtpch/Pt75Jf5KkkOrzJ:7aMYf5Kk+gktJf5Kkn
MD5:	9E96396A1B5B07EB1A782241901352D3
SHA1:	7349F7297F2C6601A191DC02463647A05ED766B6
SHA-256:	E3F2FDC7CD8BF57F3851217AA830B9E6C775E542BB8DDA52514BFC3ED7E3FC59
SHA-512:	EF2DB07D5B6CB2015DFBCC50D2D4F9CFEA0082689FD5D57E6F4342861F9749523F38DDA30B1AE365505303F76D69986E96BA86D42677DE6B358FACB003AB03
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:45:00.440 1780 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-18:45:00.442 1780 Recovering log #3.2021/08/03-18:45:00.443 1780 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.279880725312063
Encrypted:	false
SSDEEP:	12:7aOvYf5KkkOrsFUtpch/Pt75Jf5KkkOrzJ:7aMYf5Kk+gktJf5Kkn
MD5:	9E96396A1B5B07EB1A782241901352D3
SHA1:	7349F7297F2C6601A191DC02463647A05ED766B6
SHA-256:	E3F2FDC7CD8BF57F3851217AA830B9E6C775E542BB8DDA52514BFC3ED7E3FC59
SHA-512:	EF2DB07D5B6CB2015DFBCC50D2D4F9CFEA0082689FD5D57E6F4342861F9749523F38DDA30B1AE365505303F76D69986E96BA86D42677DE6B358FACB003AB03
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:45:00.440 1780 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-18:45:00.442 1780 Recovering log #3.2021/08/03-18:45:00.443 1780 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\TransportSecurityd (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1710
Entropy (8bit):	5.576367033344524
Encrypted:	false
SSDEEP:	48:YDcRUttVwUw6UUhveUUKUXqPeUekUeUwUHqdsYUW4PUeP:/RUtQU5UUgUUKU6PeU3UkUNYU9PUg
MD5:	7A0B4E3D34699609F9DD964F6DEEF0E4
SHA1:	6ED7ECE6FE235BF1EBC57A536EF00E9A4E42F5B7
SHA-256:	82086EF83CA7D8CD8199F991F5CD5DC58AEE3D406FF4D41CAA956CED107642EB
SHA-512:	59628ECFC560D56AE960C2C2E708B75AEC74A7C2FF0D9DA3398DD702440CA7536B8C7F248F90016EC1F5AE0F6F754E0B7D35CF25284D43B6063373FF0C75A9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurityd (copy)	
Preview:	{"expect_ct":[],"sts":[{"expiry":1659545090.236635,"host":"AKBA0EXj1W1QmJumkxUOTpibibkAwoUEp1CDrh5UFWY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628009090.236645},{"expiry":1643789090.475637,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628009090.475641},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659545089.922513,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628009089.92252},{"expiry":1659545089.913066,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628009089.913072},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_ob

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:	3:9HDj:9n
MD5:	E0883382075E9A8D0C4B320D90CB6520
SHA1:	8D5924B139AEE93F2B968A39DAE9903E25FAFFC0
SHA-256:	010FCBECE7305817E65BC9E09CC485A206D81E231DA494FBC4638E23FE487D7F
SHA-512:	CCD9438A485183922585BE29B5462D6E576598D98C087C0F765683B380EC6183859DB35DFE14ACAE0A537D5811217390A0F10A4290CB275B82EED4A8860ABA84
Malicious:	false
Reputation:	low
Preview:	....Yv...V..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a3dc6d3f-ce8e-48ac-aa4c-aadaa00f6721.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):	5791
Entropy (8bit):	5.173567509632197
Encrypted:	false
SSDEEP:	96:ncLMQ9tyVUhqIKInE5k0JCKL8I9kP17bOTlVuHn:ncLx9QCMI6h4KPkPX
MD5:	DC5540A3B85543E07C366D3EF6FC43A8
SHA1:	7DA0F872FD311F69410FEA4B0F031B39F56778AC
SHA-256:	89675A7B5066CF9E614DFC662CA57307F5734C8CDDBA75A834A677C4FD439CEE
SHA-512:	4449CD6129604D6C928CFCE4D730DB40B2A0D6651A1FE206DF8D451F1F34A6DE640C76C2591325F9032CD6724B78E9AFA5479C008D5FA1609060FFF68C8AB8E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272482683233446","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

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

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:44:49.431237936 CEST	192.168.2.4	8.8.8.8	0x36f6	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:49.432523966 CEST	192.168.2.4	8.8.8.8	0xfda7	Standard query (0)	tendaggisilvana.it	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:49.433871984 CEST	192.168.2.4	8.8.8.8	0x2193	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:49.965184927 CEST	192.168.2.4	8.8.8.8	0x4fb6	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:49.965845108 CEST	192.168.2.4	8.8.8.8	0xfc3c	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:50.153493881 CEST	192.168.2.4	8.8.8.8	0x632f	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:50.168430090 CEST	192.168.2.4	8.8.8.8	0xd0fe	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:50.182887077 CEST	192.168.2.4	8.8.8.8	0xdd06	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:50.190407038 CEST	192.168.2.4	8.8.8.8	0xf419	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:51.894921064 CEST	192.168.2.4	8.8.8.8	0x8c2a	Standard query (0)	tendaggisilvana.it	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:57.725692987 CEST	192.168.2.4	8.8.8.8	0x2806	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
Aug 3, 2021 18:44:49.463992119 CEST	8.8.8.8	192.168.2.4	0x36f6	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:49.466304064 CEST	8.8.8.8	192.168.2.4	0x2193	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:44:49.466304064 CEST	8.8.8.8	192.168.2.4	0x2193	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:49.467794895 CEST	8.8.8.8	192.168.2.4	0xfda7	No error (0)	tendaggisilvana.it		168.119.64.244	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:49.997518063 CEST	8.8.8.8	192.168.2.4	0x4fb6	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:44:50.002780914 CEST	8.8.8.8	192.168.2.4	0xfc3c	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:50.002780914 CEST	8.8.8.8	192.168.2.4	0xfc3c	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:44:50.168921947 CEST	8.8.8.8	192.168.2.4	0x4368	No error (0)	gstaticadssl.l.google.com		142.250.185.131	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:50.181746960 CEST	8.8.8.8	192.168.2.4	0x632f	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:44:50.202136040 CEST	8.8.8.8	192.168.2.4	0xd0fe	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:50.202136040 CEST	8.8.8.8	192.168.2.4	0xd0fe	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:50.218249083 CEST	8.8.8.8	192.168.2.4	0xdd06	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:44:50.226067066 CEST	8.8.8.8	192.168.2.4	0xf419	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:50.226067066 CEST	8.8.8.8	192.168.2.4	0xf419	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:51.930103064 CEST	8.8.8.8	192.168.2.4	0x8c2a	No error (0)	tendaggisilvana.it		168.119.64.244	A (IP address)	IN (0x0001)
Aug 3, 2021 18:44:57.767416000 CEST	8.8.8.8	192.168.2.4	0x2806	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:44:57.767416000 CEST	8.8.8.8	192.168.2.4	0x2806	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)

HTTPS Packets

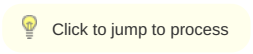
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 18:44:49.538449049 CEST	168.119.64.244	443	192.168.2.4	49729	CN=tendaggisilvana.it CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jul 07 01:28:05 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Oct 05 01:28:04 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Aug 3, 2021 18:44:49.538463116 CEST	168.119.64.244	443	192.168.2.4	49727	CN=tendaggisilvana.it CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jul 07 01:28:05 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Oct 05 01:28:04 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Aug 3, 2021 18:44:51.983439922 CEST	168.119.64.244	443	192.168.2.4	49753	CN=tendaggisilvana.it CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jul 07 01:28:05 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Oct 05 01:28:04 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5904 Parent PID: 4940

General

Start time:	18:44:41
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://tendaggisilvana.it/officix/'
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:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 5952 Parent PID: 5904

General

Start time:	18:44:43
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,13813088594936222501,123881940111943640,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1724 /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:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly