ID: 458805
Cookbook: browseurl.jbs
Time: 19:03:02
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

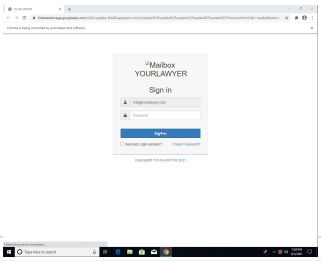
Windows Analysis Report https://firebasestorage.googl…

Overview

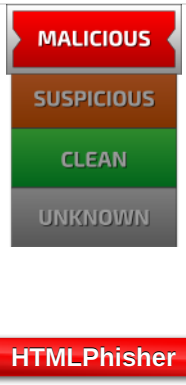
General Information

Sample URL:	https://firebasestorage.googleapis.com/v0/b/update-8c6d0.appspot.com/o/upda...ml?alt=media&token=478143df-eeb1-4635-a6e5-c6d8cdc5e89d#info@yourlawyer.com
Analysis ID:	458805
Infos:	

Most interesting Screenshot:



Detection



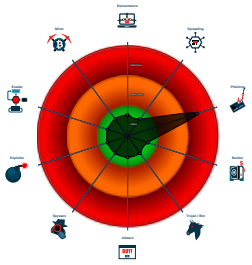
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Phishing URL detected (based on va…
- Yara detected HtmlPhish10
- Form action URLs do not match mai…
- HTML body contains low number of …
- Invalid 'forgot password' link found
- No HTML title found
- Suspicious form URL found
- URL contains potential PII (phishing…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4824 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://firebasestorage.googleapis.com/v0/b/update-8c6d0.appspot.com/o/update%2Fupdate%2Fupdate%2Fupdate%2Fupdate%2FUniversal.html?alt=media&token=478143df-eeb1-4635-a6e5-c6d8cdc5e89d#info@yourlawyer.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5888 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1568,5417355904452027015,11801000389847120122,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1800 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Copyright Joe Security LLC 2021

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

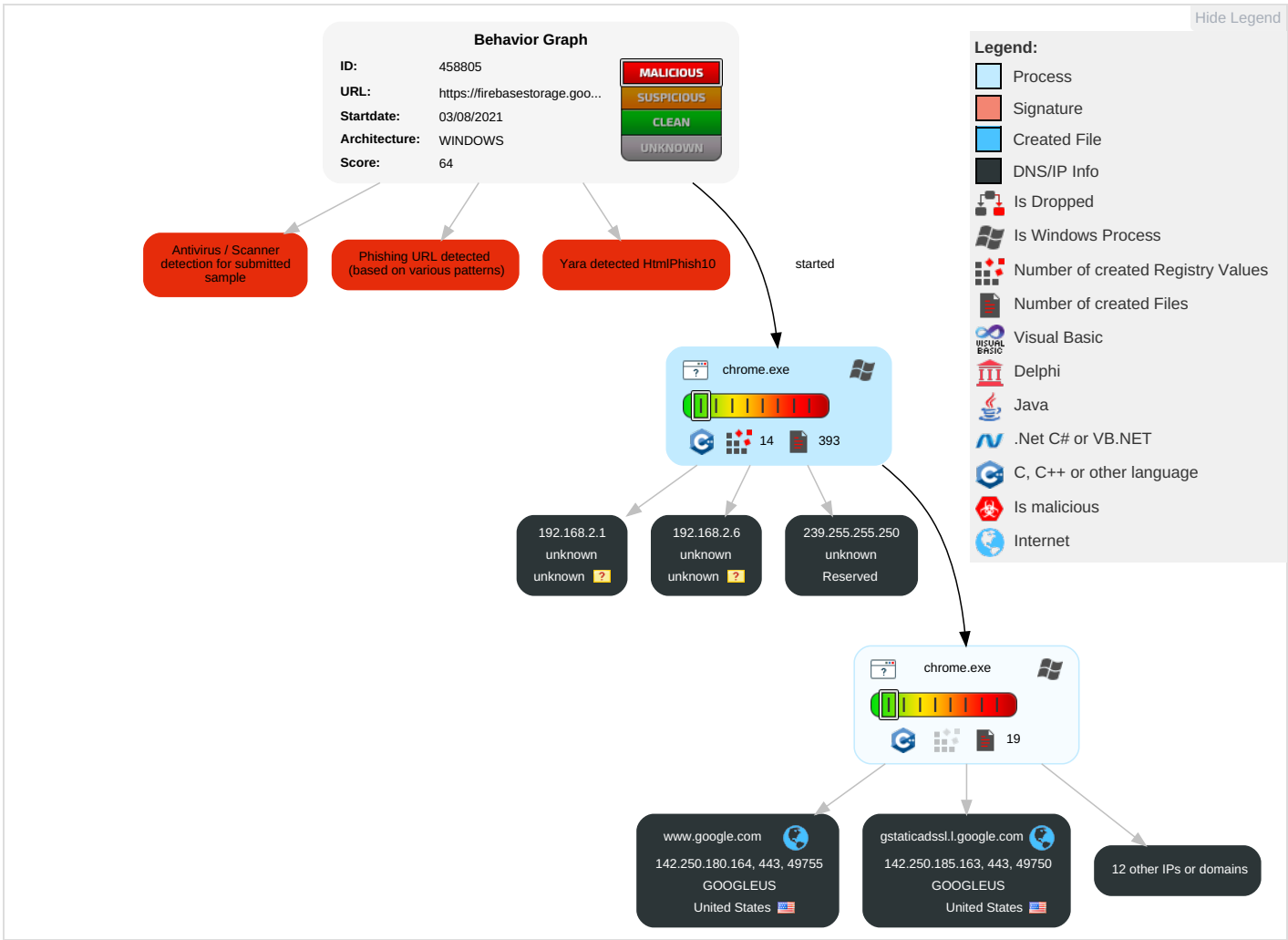
Phishing URL detected (based on various patterns)

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

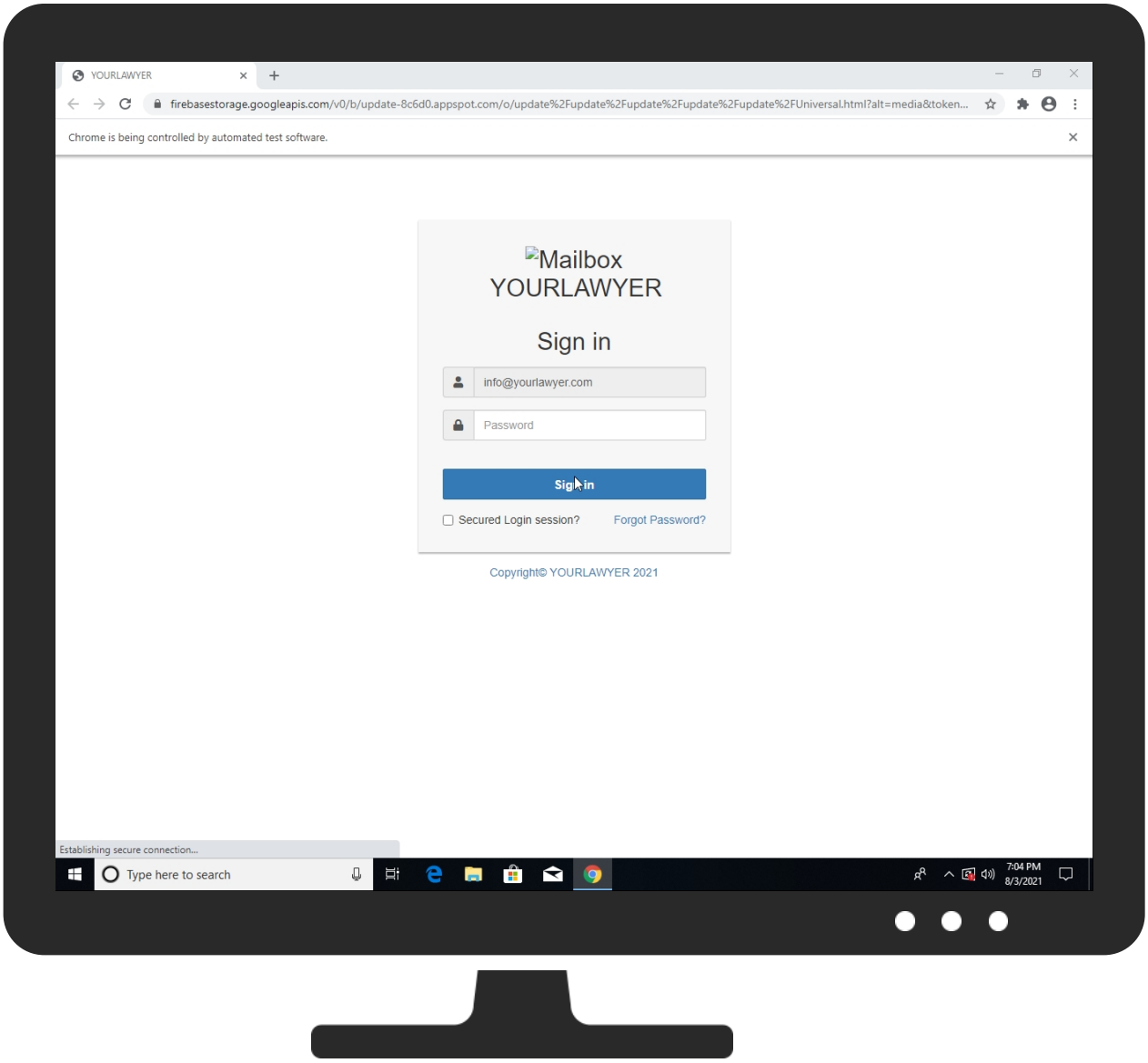


Copyright Joe Security LLC 2021

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://firebasestorage.googleapis.com/v0/b/update-8c6d0.appspot.com/o/update%2Fupdate%2Fupdate%2Fupdate%2Fupdate%2FUniversal.html?alt=media&token=478143df-eeb1-4635-a6e5-c6d8cdc5e89d#info@yourlawyer.com	0%	Avira URL Cloud	safe	
http://https://firebasestorage.googleapis.com/v0/b/update-8c6d0.appspot.com/o/update%2Fupdate%2Fupdate%2Fupdate%2Fupdate%2FUniversal.html?alt=media&token=478143df-eeb1-4635-a6e5-c6d8cdc5e89d#info@yourlawyer.com	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
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external(U	0%	Avira URL Cloud	safe	
http://https://alomrania.com.sa/html-icons/includes/server/index.php	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
gstaticadssl.l.google.com	142.250.185.163	true	false		high
accounts.google.com	216.58.205.77	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
www.google.com	142.250.180.164	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.163	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
142.250.180.164	www.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.6
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458805
Start date:	03.08.2021
Start time:	19:03:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://firebasestorage.googleapis.com/v0/b/update-8c6d0.appspot.com/o/update%2Fupdate%2Fupdate%2Fupdate%2Fupdate%2FUniversal.html?alt=media&token=478143df-eeb1-4635-a6e5-c6d8cdc5e89d#info@yourlawyer.com
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:	2
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:	• EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@28/206@11/11
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:04:06	API Interceptor	3x 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):	244080
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	6144:0rec7VDBGbrec7VDBGbrec7VDBGbrec7VDBGm:0reGZ8breGZ8breGZ8breGZ8m
MD5:	297B8B6156FC978E98086708BE851002
SHA1:	B0D749B7C1CECCF6F588F194607A76F81F73C5D2
SHA-256:	C0D6629F1B36C27A5B0F9E23FB3739219FBC20E1BC2974D84B1C6F929358EA8B
SHA-512:	251146031870BC5086D07D5AF6FAD5E901FFAE35F9A86708EE21CB1193F31673D83B57343BD5AD676D7E31B0C15E35715F19BF83F4C508F276766F267ABD5716
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):	1304
Entropy (8bit):	3.1474615609656387
Encrypted:	false
SSDEEP:	24:T75kPcUQUfed75kPcUQUfeg5kPcUQUfek5kPcUQUfet:A1QG1Qv1Qb1Qt
MD5:	8AF8D9DEEAA52D9E62517B45DB7E2E0E
SHA1:	9C30A3D501E69B246CA2DDFB8F6F2F970EA6FB11
SHA-256:	5F8A1FB83804A13542FC598535C4C93E36A771495430EED3B4F7D8CCE5824964
SHA-512:	250CF3654F789B9CB7CE22DBB0F3633862429D827E5C9924300FBFA0D55FB44A592D2AF81AABDADBE54434E4DCDED34FFB19BA3ACDD8F59E9E94460C6C669 84
Malicious:	false
Reputation:	low
Preview:	p..... .....tk.....(..... .....T'._.....$.....\...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...p..... .....tk.....(..... .....T'._.....$.....\...h.t.t.p. :./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0.". ..p..... .....Z\.....(..... .....T'._.....$.....\...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3. /.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...p..... .....S.k...

C:\Users\user\AppData\Local\Google\Chrome\User Data\42d04509-8346-48c1-9262-eab574aeec3a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	modified
Size (bytes):	94708
Entropy (8bit):	3.7502012165145016
Encrypted:	false
SSDEEP:	384:NnWdlbAaTYNVDVMXCXRAN/JrXqv/Nv3uB/KHLGGXS1rQTp1xuvnXbWrEFmlyl1Qx:tKWBlqz6SgerJfj4nrWbKdDZJj
MD5:	7E24762D877A0A1B217345D68B6267D8
SHA1:	6D0A86D9F89CC7EE4B7E90194A68263E4579310C
SHA-256:	E0528956E206CEC9202FB9F62DE70D6D613D1133B7AB8D6F69EADA52EF8238EE
SHA-512:	9C3874641F84257CA250AC07BDD6BE320A96283D0C34FEBD2A1344EE55961E44448F6CA2CC3DF92CA9CCF024FB513F952053B30872837C354994440459F49BA/
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\42d04509-8346-48c1-9262-eab574aeec3a.tmp	
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\4cc42bcc-408d-4dd7-86fd-f373f066be64.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):	174470
Entropy (8bit):	6.079633622074918
Encrypted:	false
SSDEEP:	3072:CtvGaYTJQE+mugy9+QV1T7IRwdfLSNPUFcbXafIB0u1GOJmA3iuRZ:4exaV+QfT7GSmhSaqfIlUOoSiuRZ
MD5:	64940496D59E7ED01134C42F3195F262
SHA1:	4018B20C4CCFBE5C6CC9E16054B392B8077A6639
SHA-256:	D066173D40598DA067F55338ABB05314AFAF99912DC8BEB01339AA32FC8028FE
SHA-512:	EA364DCE53B2EC65618FAA99197B8EDF83D125401C763F5EF49D64989A9BCA5420427C8296C3050227FC9E3A749CB422B997E195F274346CF429722853F3F136
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":1.628010238388292e+12,"network":1.62801024e+12,"ticks":6076497993.0,"uncertainty":4545460.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\766e4bd5-55f0-45a3-84f7-84495f21f352.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):	174470
Entropy (8bit):	6.079633575088769
Encrypted:	false
SSDEEP:	3072:E6tvGaYTJQE+mugy9+QV1T7IRwdfLSNPUFcbXafIB0u1GOJmA3iuRZ:EQexaV+QfT7GSmhSaqfIlUOoSiuRZ
MD5:	A5BA448EB02467B1041F9A92FC203D28
SHA1:	F6B7BF9843629078321C7ED782DEC7CEC035A6B4
SHA-256:	FBEB1439BF8AD5F8E412C2F02C82D74E69B446D833BA7EAAB045E34102E0C6B1
SHA-512:	73FF7C091137C63BE3EDCFDC939DCED7E8CD7EE7DE2B8B9AA8FF1D62F6D20EE008CE4C47355B19A78D063D0E52B85A7A444D045CA065D573252AF2B39A2070A
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":1.628010238388292e+12,"network":1.62801024e+12,"ticks":6076497993.0,"uncertainty":4545460.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715175426"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\77695ae7-ae0d-410b-930c-4f928a3c4456.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.749551965972552
Encrypted:	false
SSDEEP:	384:DnWdlbAavNVlCXRAN/JrXqv/Nv3uB/KHLGGXS1rQTp1xuvnXbWrEFmlyl1QvRxp1:qWBlqz6SgerJfj4nrWbKdDZJd
MD5:	4A27E33BEE11C178D3332548350FD775
SHA1:	91C41C0683B85ECD264ACB767F5BAFCD7CD7903D
SHA-256:	F911DE7EC335FBCE44605169125DBB4F7D9F5AF253041052933D21ECE5E053F1
SHA-512:	2448AA9C89DD86A3AB0B6990235196785AFDAACC6CCCAB824D4C7351802C802F4D3641C41428A5D56AFEDA5CA47F428981575539C5CFEA292959F9552644DB9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\77695ae7-ae0d-410b-930c-4f928a3c4456.tmp	
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\9660abc8-1c48-478c-a538-ea5394550864.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):	174470
Entropy (8bit):	6.079633231681122
Encrypted:	false
SSDEEP:	3072:C7TGaYTJQE+mugy9+QV1T7IRwdfLSNPUFcbXafIB0u1GOJmA3iuRZ:WixaV+QfT7GSmhSaqfIlUOoSiuRZ
MD5:	6822A1CDC62C795FE517705CC5D98565
SHA1:	DADAF20565C46712EE80D9B594AACF635C3DB86B
SHA-256:	A8DDF56D5FB7DF6C752392A5316F0C53525FDFE18C0292242561805C8DEB6FA2
SHA-512:	5355A579607642E27049A2F4ABAA4EC741C3B2EB195EBEF13FF2193ABDAC64A59B10E7D5DF46D4224DE164A669629688D09BE83AE1C9D622F5FF6F2482E8807
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":1.628010238388292e+12,"network":1.62801024e+12,"ticks":6076497993.0,"uncertainty":4545460.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\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\03bbff91-d6b0-41b6-927e-8a6eb73f310f.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):	2438
Entropy (8bit):	4.84523531218547
Encrypted:	false
SSDEEP:	48:Y2nzM3qyvKDHGXtwWsxIDsxLFRSepsxF6q56N6Dsxm8qChpsxNoMHRzgYhbw:JnzMa+KDHGXOvIoLF0/Fx56N6omrCAN2
MD5:	2395B4C262A05680C88EDA884ADF073B
SHA1:	5142EEB08B679503AA93F4022F2B96C08A084548
SHA-256:	C5F9DC9B985D5DDFFE2164C232B7974AFA11349F976F9101E0C2CC24EFB303BD
SHA-512:	24117E77812D2BFE895FD8676DEE63B4471AEBC5AADC13CA0AE3407635A26EFCD21A74449AA8F966165921AA98ADD857687F81CE09AEBEC94720D08CC099F9D
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://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275075840019652","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\03bbff91-d6b0-41b6-927e-8a6eb73f310f.tmp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\059caf30-1c8a-41b8-943d-80e59880761f.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):	5.174612987345948
Encrypted:	false
SSDEEP:	96:nFLAh9Vx61ReZIKIe5k0JCKL8UVkJ1TbOTlVuHn:nFLs9b61sZIAh4KTkJb
MD5:	92557D9F1357A989DDD7C2ECCB4A4B4C
SHA1:	0BAE61198FF4EE2584092C41458E1CE6074BC1E6
SHA-256:	D7C00DD3E8359DDED9FC9A8D3A6A988F284494A9D42B37DE50965316D0E47EE5
SHA-512:	16B81DB36961824A3FBE6119AB72FDBECC75E0F1AB1E26606832E5C327267956D8AA9082198D2BCAE77DA2C9FFEA52E7C8809D2AA20C7D46FCD1778672F1E0C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272483831542198","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\0d5e4bee-1e83-4f5c-afcf-2dd6fbd92f44.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4891
Entropy (8bit):	4.933417526894524
Encrypted:	false
SSDEEP:	48:YclkKSChkliLqAOqqTlYGlQKHoTw03Erf4MqM8C1Nfct/9BhUJo3KhmeSnpNGzFc:nFLkt9pIKIe5k0JCKL8bbOTlVuHn
MD5:	5C81AF9FBC005E3475037CCFB30D70F3
SHA1:	09D2C9FC5A2381FAED584E133BC9841749DBFEFE
SHA-256:	937EF01C287E6FC4C5ED4438955C839574D0C5D8D88C7EAE88D564BFFCCC2DDF
SHA-512:	214C74E6BCAD16DDA13F8CBAE7D087EC7A74BD493B9ADD70D32590FD819B34209CA50023C12E24C7835C4C2E2401DE41BC8C0FCE74C74A39C5D509E03C026B9
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272483831542198","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\57c5c32b-3d8f-4071-a14c-2d261f6551dc.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

Copyright Joe Security LLC 2021

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\57c5c32b-3d8f-4071-a14c-2d261f6551dc.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5ee9df7c-8fec-4d15-bcfc-e40b026e6971.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):	5.5800886019550076
Encrypted:	false
SSDEEP:	48:YEcRUgvVwU/6UUhSeU/KUvYqPeUekUe0wU0tsYUHUeP:sRUZUCUU1U/KUvHPeU3UCU0+YUHUg
MD5:	AC584E4227B1942102F0A7722C1FF03E
SHA1:	DBA2E873E636E584D2799683F98BC38A705048E2
SHA-256:	7B5262D2018557610E8C5D49C1F79795D8B24808F6681EA5F33A08E443325624
SHA-512:	B46F185EF5E759D78B86240173F25AA0B4E48DCB7F882E8AB0EC587797EBB616F66B33C6584A411676617295C413216F58013D8E0DD7BF800D83F1ECD052F517
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659546245.921696,"host":"AKBA0EXj1W1QmJumkxUOTpibkAwoUEp1CDrh5UFWY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628010245.921703},{"expiry":1643790245.166417,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628010245.166421},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659546244.046669,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628010244.046677},{"expiry":1659546245.137379,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628010245.137385},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\69a052e1-0868-46fd-9880-15c801a03520.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

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):	5.208435731660004
Encrypted:	false
SSDEEP:	6:mNOSEVSVq2Pwkn23iKKdK9RXXTZIFUtp+OQLgZmwP+OZwIkwOwkn23iKKdK9RXXH:m8SVvYf5Kk7XT2FUtpcLg/PSI5Jf5KkT
MD5:	0E39C3C4FEEB13D411833FC888BB8FC2
SHA1:	42BFC3759090E9B301C0DB287A16DC0EAA271DCE
SHA-256:	DFB3E3E42E27F94C1A69DA42E797F4BD026D0FF18DA78069C328BC9D883EABAF
SHA-512:	197164503EF5B7160B5E05D219DFA990ACAC7D07E6FE189DDF417F79587A2F4E4EF2B527CA305A5D86C1647C800F360C10880BAE4304B5ECB2E7D4E20D85BB96
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.725 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-19:04:12.729 16a0 Recovering log #3.2021/08/03-19:04:12.730 16a0 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):	5.208435731660004
Encrypted:	false
SSDEEP:	6:mNOSEVSVq2Pwkn23iKKdK9RXXTZIFUtp+OQLgZmwP+OZwIkwOwkn23iKKdK9RXXH:m8SVvYf5Kk7XT2FUtpcLg/PSI5Jf5KkT
MD5:	0E39C3C4FEEB13D411833FC888BB8FC2
SHA1:	42BFC3759090E9B301C0DB287A16DC0EAA271DCE
SHA-256:	DFB3E3E42E27F94C1A69DA42E797F4BD026D0FF18DA78069C328BC9D883EABAF
SHA-512:	197164503EF5B7160B5E05D219DFA990ACAC7D07E6FE189DDF417F79587A2F4E4EF2B527CA305A5D86C1647C800F360C10880BAE4304B5ECB2E7D4E20D85BB9 6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.725 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-19:04:12.729 16a0 Recovering log #3.2021/08/03-19:04:12.730 16a0 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):	5.178370759634201
Encrypted:	false
SSDEEP:	6:mNOCfYVq2Pwkn23iKKdKyDZIFUtp+OcUoSgZmwP+OaLIkwOwkn23iKKdKyJLJ:XVvYf5Kk02FUtpAwg/PuLI5Jf5KkWJ
MD5:	FF6A759126A9ED12177DB5FE93AE6828
SHA1:	F7B722838553B0B11F02AE491B5D71A8958D0BD7
SHA-256:	82EE48521151A849223957C48863C625CA409767E5666C04A20B94CB702E387A
SHA-512:	378E591BC1452F059F5ACBA39C95D7DF8DF6B049ECBB53F462C13FBE0597F4D546105A6C4A9BC7769865A756281323D47459113117E706F03B8B29E86487F404
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.681 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-19:04:12.683 16a0 Recovering log #3.2021/08/03-19:04:12.684 16a0 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):	5.178370759634201
Encrypted:	false
SSDEEP:	6:mNOCfYVq2Pwkn23iKKdKyDZIFUtp+OcUoSgZmwP+OaLIkwOwkn23iKKdKyJLJ:XVvYf5Kk02FUtpAwg/PuLI5Jf5KkWJ
MD5:	FF6A759126A9ED12177DB5FE93AE6828
SHA1:	F7B722838553B0B11F02AE491B5D71A8958D0BD7
SHA-256:	82EE48521151A849223957C48863C625CA409767E5666C04A20B94CB702E387A
SHA-512:	378E591BC1452F059F5ACBA39C95D7DF8DF6B049ECBB53F462C13FBE0597F4D546105A6C4A9BC7769865A756281323D47459113117E706F03B8B29E86487F404
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.681 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-19:04:12.683 16a0 Recovering log #3.2021/08/03-19:04:12.684 16a0 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\3e29eaa8f606a452_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.408922609568607
Encrypted:	false
SSDEEP:	6:mko/lXY68E9xEEUgLErtElLZHI6L/EDzaEYOnK6t:O/DYg5JZP/kzaEF
MD5:	0FDD48E9E0E1D0164909D496C18E243B
SHA1:	B14CB7F992C03432BDDA3BF9E82A7DDF4E4BD5F3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3e29eaa8f606a452_0	
SHA-256:	BDA45D4B27A3C1F32D4CF7292A085D9C5AC79C0BEE488395B31855A8638A7BDD
SHA-512:	476104AAC1CC94FD959EC1B90F91A898D19C9ED2A62B56B2554B334815DBC2A52D75CD81559C68D67AFC47B4DFE58723083E31B21F3F986B60FF66B69C00204
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p...\5.h...._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://firebasestorage.googleapis.com/....@'/.....=u.U.uL..l...8.t..&..-E.z.c....A..Eo.....$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5351a31f681c3a5b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97736
Entropy (8bit):	5.7865628441899295
Encrypted:	false
SSDEEP:	1536:LGADvOlYR/iMYC7In8zBKeVhdJK97Bw5aO4/zdicZsvxcLkTyeX7XcegjvvJu9Gn:LC+R/Pkn+zjY9W5aOCnZ+xcoTyscDrVn
MD5:	9D53602E08E7505D1FAC9076DF8CB78F
SHA1:	99A0D93B7B1900E12DE06EF2E67DF88FDB73F2EF
SHA-256:	B144F2D44F29B783557EF5C36D4C63AD7733ABC4FC184010575FA0080B3B845F
SHA-512:	6296A78B814F09FEFF087B06559655D0EA50C98E204EE2368672FE0B02A02A2F9A45A5AB9A05AFF94E521F654640E76FC038302820577BFD8E8B489517272A0E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....d.....504D43A85C776CA1E05FBECAC6635558F9FDEEA333915148CC339AB5E0609037.....'.JN....O!...p|..`tD.....!.....L.....(.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@.P.*....module....Q.@r+.....exports...Qcz.....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.jsa.....D`....D`....D`.....`z...&...&..!.&....&.(S....!..`.C.....q.L`.....Rc@.....M.....QbJ.....d.....QbB.mX....e.....Qbv.....f.....Qb..TA....h.....S...Qb.....j.....Qbj.w.....k.....Qb."^....l.....Qb.....n.....Qb2.....o.....Qb.j'.....p.....Qb..8;....q.....QbZN.....r.....Qb.\.{....s.....R....Qbv.....v.....Qb.Z.z....w.....QbJ(\.....x.....Qb2R...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\56aefa09742044bf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	373
Entropy (8bit):	6.020526332314361
Encrypted:	false
SSDEEP:	6:m0l/VYSHT8NWQAlKPUQykElLZHdnv67D6nnDx6Wt41lZK6tbKf4zSj3jg55fQCOV:Dz8NWQCUUPJZ91nDnGBPS3ajODnx
MD5:	F24DCD547F75C78338C4E0A4171058A9
SHA1:	291488214FEE8B24EF286A900840A8BAB23580D4
SHA-256:	D6EF7576ED991EB4F210691447A1890C83D7A1B42C487D5E0EE6AA7510373E06
SHA-512:	B33A31B34C5E60B2EDA724EF4DCD68CA911B5B6D1634448FC5119807938098F43944ED9FE25E60018FC3434ACBFAD36BEC31695F92075BC91D0489E5E723816
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m...0.;.....,_keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://firebasestorage.googleapis.com/....@'/.....!.....P..[..IQ_...U+'..L..TH..A..Eo.....Q.....A..Eo.....@'/. }..504D43A85C776CA1E05FBECAC6635558F9FDEEA333915148CC339AB5E0609037!.....P..[..IQ_...U+'..L..TH..A..Eo.....NL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e47a33ac8e679b3a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.329548451752245
Encrypted:	false
SSDEEP:	6:mDgEVYkb8E9xEvAErtElLZHVw67vqpe4iPiaoAHKXhK6t:Uggv4oJZRsiOSq7
MD5:	87F05909C76E2DCD2DEF7DCC9F56D4EA
SHA1:	3455F08F86C3247FC84FB15F1721590858A83761
SHA-256:	FA500269204AEF5D2B8873C16AF1492CA6673849947FA223FA8E5DE3D7D56881
SHA-512:	EB90B0FB3C4B7429252220CFD8411C09B720A575FBC3B028DD5C8CDCA891BA9AF84B9558ED15594C08FE415AE1202B77F7585FAE2BE3B6445DA1C784B23683 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...'.....,_keyhttps://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js .https://firebasestorage.googleapis.com/g/..@'/.....E..5A..._$@..]m./.xgG.k.....].A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f8d798d069065fcb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	5.457817995409714
Encrypted:	false
SSDEEP:	6:mN/PYET08NaYWbVOqZtElLZH8lh6eO6pSxdK6t:Mbg8NaY8Z2JZQO6C3
MD5:	E7B70CA78EBC922E7B3A94D153AD40AC
SHA1:	2F2A14D245AEBE267B7CD29589EC6A9302C81515
SHA-256:	319CE765E7C93230288993DE864D610800E957175C8947FA8EE2B720BDCB3615
SHA-512:	CED6E85B660D398C8EBEB78807D085D694CF56823ED9749EFCBE877AC90FB88B847F759F1BB859765580B9A745197F33C6372242A376E1B49EF44A7DD6AC357
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://firebasestorage.googleapis.com/0...@'/.....b.5.e..Z....v....u-..I.o4.8m....A..Eo.....1j.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fd3140fcc260accb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.503501095885987
Encrypted:	false
SSDEEP:	6:mc/VYlNYpSVkmElLZHWATNo+KT2jons5RK6t:zvpSVGJZ22QiHr
MD5:	C03871497BC9B6EF036A3B3EB941A5B1
SHA1:	5A559A9D52F24AB9835048BA0BEC7AFCE68F35F6
SHA-256:	CF75B76C88DB205C21B827A524552F6D24802D30D7A1CF915C587D27012B3726
SHA-512:	CFDD210CEEEE0D4A796E22228B79E27A6EBE758CA3F24E41142DEC9702A38D069EC495951D7D34B2C5C7D5037801075AF3D25B9E406B4B6C5C005FDE036A035
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....2....._keyhttps://kit.fontawesome.com/585b051251.js .https://firebasestorage.googleapis.com/....@'/.....9(L.])J+.T.gj..y|.)...=$'.j.....A..Eo.....s.....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:	zlib compressed data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	5.091542892949816
Encrypted:	false
SSDEEP:	6:ToAzA3JueQ2+uzhg2dbB/AxlWDcTxzPawAfyDns:kqEJgTuXAxlZXUyI
MD5:	A4A1EE8DE6D3AD819E217F316505D923
SHA1:	09E313693758B0D0E440A7C879D8A673CD2D6F88
SHA-256:	DF1660E8A030A0F16734B909F49EFB9E5DEAAEB8D96AB4502B8DB013887BD300
SHA-512:	424BE462F19F9FB9A2AAC01F8F65D71B014DCB12F978A88F03A298AC51B892B977D9A386DD6C2441DC43814AEE2E14708B0F0E45C705E82AE4B40EF0C7EB8C1F
Malicious:	false
Reputation:	low
Preview:	x.....nKoy retne.....:g..3z...@'/.....[:.h..QS....@'/.....R.....)>....@'/....._.i.....@'/.....`..@1.....@'/.....D t...V@K..@'/.....^}.Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../.....U...@'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	zlib compressed data
Category:	dropped
Size (bytes):	384
Entropy (8bit):	5.091542892949816
Encrypted:	false
SSDEEP:	6:ToAzA3JueQ2+uzhg2dbB/AxlWDcTxzPawAfyDns:kqEJgTuXAxlZXUyI
MD5:	A4A1EE8DE6D3AD819E217F316505D923
SHA1:	09E313693758B0D0E440A7C879D8A673CD2D6F88
SHA-256:	DF1660E8A030A0F16734B909F49EFB9E5DEAAEB8D96AB4502B8DB013887BD300

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index (copy)	
SHA-512:	424BE462F19F9FB9A2AAC01F8F65D71B014DCB12F978A88F03A298AC51B892B977D9A386DD6C2441DC43814AEE2E14708B0F0E45C705E82AE4B40EF0C7EB8C F
Malicious:	false
Reputation:	low
Preview:	x.....nKoy retne.....:g..3z...@'/.....[:.h..QS....@'/.....R.....)>....@'/....._i.....@'/.....`..@1.....@'/.....D t...V@K..@'/.....^}.Np....4&../.....-..0. .x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../.....U...@'/.

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:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC761 F
Malicious:	false
Reputation:	low
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):	0.9728627603450565
Encrypted:	false
SSDEEP:	24:se9H6pf1H1oNHRqLbJLbXaFpEO5bNmISHn06UwQ8:sbfvoNxq5LLOpEO5J/Kn7UL8
MD5:	0EFA1BF25A5BF2DE9DA0F1CD8ABA5FE1
SHA1:	61B42A601BA1407B6B312D893B6DC86A8E7FB518
SHA-256:	8339BAD933AB7311BDAD1FF880FC6B69913790CB9DEB8B77C9734C540D0BE39F
SHA-512:	0E668FB7D835D7615808B436A738D990CB6161BD9CBF7F474AB80CD732AA8465A8635AAF22F624C7E0D217B4BEC894B2E8AAE12AA8461D7A639E79370928BBF 8
Malicious:	false
Reputation:	low
Preview:	.....K.1..... ....

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):	3610
Entropy (8bit):	3.9433515372820094
Encrypted:	false
SSDEEP:	48:34VxTb5Efl8PEYH/ZYQt+q5EfIX5EfIfALPEYH/ZYQt+XDx78VTz15Efl/:34z5oQQ75oQ5oHwQ7V15oK
MD5:	67C5F74CAB6F20645E353CAC153F055D
SHA1:	3DFE92523D66C0787874E63BB3524C7462D5C4DC
SHA-256:	060540E18116EB10781E09CBD4EC2944BAC2AC057D69BA6C10FECFDBEB3A8EC6
SHA-512:	1CDF8A6E1D0E3E335B5F8F808C81504808D03AD7A736DB4E7E122CDF55B54C0E0402D5D9147E1B09F10F3C67C2C4FDD4FA213D15642C691B236C8D7951371F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Preview:	SNSS.....!.....1.,.....$...f58db7f7_5433_4fa4_b3f2_f8c34e50f93b.....i.....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....https://firebasestorage.googleapis.com/v0/b/update-8c6d0.appspot.com/o/update%2Fupdate%2Fupdate%2Fupdate%2Fupdate%2FUniversal.html?alt=media&token=478143df-eeb1-4635-a6e5-c6d8cdc5e89d#info@yourlawyer.com.....h.....`.....^4C....._4C.....@.....X.....h.t.t.p.s.:././.f.i.r.e.b.a.s.e.s.t.o.r.a.g.e...g.o.o.g.l.e.a.p.i.s...c.o.m./.v.0./.b./.u.p.d.a.t.e.-.8.c.6.d.0...a.p.p.s.p.o.t...c.o.m./.o./.u.p.d.a.t.e.%.2.F.u.p.d.a.t.e.%.2.F.u.p.d.a.t.e.%.2.F.u.p.d.a.t.e.%.2.F.u.p.d.a.t.e.%.2.F.U.n.i.v.e.r.s

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
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):	5.206633101990995
Encrypted:	false
SSDEEP:	6:mQHcWq2Pwkn23iKKdK8aPrqIFUtpJH7XZmwPJHQ9zkwOwkn23iKKdK8amLJ:9cWvYf5KkL3FUtpNr/PNQd5Jf5KkQJ
MD5:	27C68815289F2B67D878F7BC42405BED
SHA1:	5F5ACD5C0D27CD848569DD5E009B1DEA18394FBC
SHA-256:	656F5373B654E53818258EF638E9478A3BCCCD95CC2C61A8687C09D448B11FEE
SHA-512:	EC6C238DD96CE4F93DB2FB7532424011C78D231FD31964AD4E1B8248205B1E3982DB1692676D4E636A616070C5C7DE46C48A97F495BB02A68B293228D407723E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.571 1740 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-19:03:51.574 1740 Recovering log #3.2021/08/03-19:03:51.575 1740 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):	5.206633101990995

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old. (copy)

Encrypted:	false
SSDEEP:	6:mQHcWq2Pwkn23iKKdK8aPrqIFUtpJH7XZmwPJHQ9zkwOwkn23iKKdK8amLJ:9cWvYf5KkL3FUtpNr/PNQd5Jf5KkQJ
MD5:	27C68815289F2B67D878F7BC42405BED
SHA1:	5F5ACD5C0D27CD848569DD5E009B1DEA18394FBC
SHA-256:	656F5373B654E53818258EF638E9478A3BCCCD95CC2C61A8687C09D448B11FEE
SHA-512:	EC6C238DD96CE4F93DB2FB7532424011C78D231FD31964AD4E1B8248205B1E3982DB1692676D4E636A616070C5C7DE46C48A97F495BB02A68B293228D407723E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.571 1740 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-1 9:03:51.574 1740 Recovering log #3.2021/08/03-19:03:51.575 1740 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
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):	5.171300509383033
Encrypted:	false
SSDEEP:	6:mA2lyq2Pwkn23iKKdK8NIFUtp52z1ZmwP3uS4RkwOwkn23iKKdK8+eLJ:rfvYf5KkpFUtpu1/P3u75Jf5KkqJ
MD5:	F3A4CD1FAB67DACBB5B463B8FB0D45A3
SHA1:	91D323A02AD1C41825EB5B264C75BB1887A88357
SHA-256:	E4C6A44054EE306F96314D18A1DDEF449222DFDA90BC99C097B7F6D779DB66B7
SHA-512:	E7CFC377CE5CC5A136903D9D03B04F46330650EF000A38BDEA8B3A2A7C2B6BCEEBF8892D995FA1AE53507BED8C142C60450C0069396F988B085CC17D1384C9 2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:58.104 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-1 9:03:58.106 1710 Recovering log #3.2021/08/03-19:03:58.108 1710 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):	5.171300509383033
Encrypted:	false
SSDEEP:	6:mA2lyq2Pwkn23iKKdK8NIFUtp52z1ZmwP3uS4RkwOwkn23iKKdK8+eLJ:rfvYf5KkpFUtpu1/P3u75Jf5KkqJ
MD5:	F3A4CD1FAB67DACBB5B463B8FB0D45A3
SHA1:	91D323A02AD1C41825EB5B264C75BB1887A88357
SHA-256:	E4C6A44054EE306F96314D18A1DDEF449222DFDA90BC99C097B7F6D779DB66B7
SHA-512:	E7CFC377CE5CC5A136903D9D03B04F46330650EF000A38BDEA8B3A2A7C2B6BCEEBF8892D995FA1AE53507BED8C142C60450C0069396F988B085CC17D1384C9 2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old. (copy)	
Preview:	2021/08/03-19:03:58.104 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-19:03:58.106 1710 Recovering log #3.2021/08/03-19:03:58.108 1710 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
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:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	5.236233514100395
Encrypted:	false
SSDEEP:	6:mNOBSVq2Pwkn23iKKdK25+Xqx8chI+IFUtp+ObgZmwP+OqIkwOwkn23iKKdK25+M:9SVvYf5KkTXfchI3FUtpPg/PuI5Jf5KN
MD5:	EB4C9649EBA1AF49D95D4021DE6FB6AA
SHA1:	8EB5FF4098637395D4B0666B442FA2FCA9847DC3
SHA-256:	FE0AFDBF5D58AEE34DAD293402A8653AB43DE518479F646B604E7B650D97F4D4
SHA-512:	A53C2DE4D7F223DC626502B82EE59832B1D201F24B3A56CDFA63FE6543B4E07634A36077F19A5D8BCEBFF5A7F190DEB3F00D67E2AA06ECD6DA67CDD8CD3B25C
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.633 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-19:04:12.634 16a0 Recovering log #3.2021/08/03-19:04:12.635 16a0 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):	5.236233514100395
Encrypted:	false
SSDEEP:	6:mNOBSVq2Pwkn23iKKdK25+Xqx8chI+IFUtp+ObgZmwP+OqIkwOwkn23iKKdK25+M:9SVvYf5KkTXfchI3FUtpPg/PuI5Jf5KN
MD5:	EB4C9649EBA1AF49D95D4021DE6FB6AA
SHA1:	8EB5FF4098637395D4B0666B442FA2FCA9847DC3
SHA-256:	FE0AFDBF5D58AEE34DAD293402A8653AB43DE518479F646B604E7B650D97F4D4
SHA-512:	A53C2DE4D7F223DC626502B82EE59832B1D201F24B3A56CDFA63FE6543B4E07634A36077F19A5D8BCEBFF5A7F190DEB3F00D67E2AA06ECD6DA67CDD8CD3B25C
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.633 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-19:04:12.634 16a0 Recovering log #3.2021/08/03-19:04:12.635 16a0 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):	5.172508192341767
Encrypted:	false
SSDEEP:	6:mNO8PVq2Pwkn23iKKdK25+XuoIFUtp+OSULgZmwP+O4LIkwOwkn23iKKdK25+Xu6:2VvYf5KkTXYFUtpmULg/P4I5Jf5KkTXp
MD5:	517E17005B41FF80479D1BA838D0A0B5
SHA1:	632CCF1E5379B563213800F3A6C1AE55C5C767F2
SHA-256:	C8975124517B2630F8EA82B65167BD91C35ADE207E8DE2BDE3289C40A4F294BD
SHA-512:	3CFDA8878DDA6A05962BCEA1A4D7BB2E289754C22C4388C206FFB7363936BA1B906D830A8B7B0C859B3E9D4D455280F4099327B1C5F96193BFF2469EF7A1B9E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.622 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-19:04:12.623 16a0 Recovering log #3.2021/08/03-19:04:12.624 16a0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.172508192341767

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Encrypted:	false
SSDEEP:	6:mNO8PVq2Pwkn23iKKdK25+XuoIFUtp+OSULgZmwP+O4LIkwOwkn23iKKdK25+Xu6:2VvYf5KkTXYFUtpmULg/P4I5Jf5KkTXp
MD5:	517E17005B41FF80479D1BA838D0A0B5
SHA1:	632CCF1E5379B563213800F3A6C1AE55C5C767F2
SHA-256:	C8975124517B2630F8EA82B65167BD91C35ADE207E8DE2BDE3289C40A4F294BD
SHA-512:	3CFDA8878DDA6A05962BCEA1A4D7BB2E289754C22C4388C206FFB7363936BA1B906D830A8B7B0C859B3E9D4D455280F4099327B1C5F96193BFF2469EF7A1B9E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.622 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-19:04:12.623 16a0 Recovering log #3.2021/08/03-19:04:12.624 16a0 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):	5.186282481553324
Encrypted:	false
SSDEEP:	6:mNOjVq2Pwkn23iKKdKWT5g1IdqIFUtp+O4YgZmwP+O99SIkwOwkn23iKKdKWT5gZ:PVvYf5Kkg5gSRFUtpXg/PDSI5Jf5Kkgk
MD5:	7801CCC4078055AA96007E5F4E65E1BC
SHA1:	3904D0136966AD09BC71630DA6212AFC311F0E25
SHA-256:	8793DA8031C69414F686AFB4D75CD7F45476EBA8D8D5445A69359C46E5924957
SHA-512:	123EC4CF4C0C55CA6864F60B60213E107FB23811CD85E0D4E1AAB6F10C5A8D2E782AA9DDF986F65B850E48D1DF14A6578A91504B5C9F89478390267D03CA0E4
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.601 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-19:04:12.609 16a0 Recovering log #3.2021/08/03-19:04:12.613 16a0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.186282481553324
Encrypted:	false
SSDEEP:	6:mNOjVq2Pwkn23iKKdKWT5g1IdqIFUtp+O4YgZmwP+O99SIkwOwkn23iKKdKWT5gZ:PVvYf5Kkg5gSRFUtpXg/PDSI5Jf5Kkgk
MD5:	7801CCC4078055AA96007E5F4E65E1BC
SHA1:	3904D0136966AD09BC71630DA6212AFC311F0E25
SHA-256:	8793DA8031C69414F686AFB4D75CD7F45476EBA8D8D5445A69359C46E5924957
SHA-512:	123EC4CF4C0C55CA6864F60B60213E107FB23811CD85E0D4E1AAB6F10C5A8D2E782AA9DDF986F65B850E48D1DF14A6578A91504B5C9F89478390267D03CA0E4
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.601 16a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-19:04:12.609 16a0 Recovering log #3.2021/08/03-19:04:12.613 16a0 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):	0.22733134104444291
Encrypted:	false
SSDEEP:	24:TLxPfQVVVV6LEfIM8VsuCTsRzDQVVVV6LEfIMe:Tp5EfIZCgD5EfIp
MD5:	BC4FB149EA71381CC125C1A15CF66D2F
SHA1:	4EEE0E4E4EFFA5B83B28DDAD6D4564BED489DBE9
SHA-256:	4CA570785F029A781857264EAA0AF4C9B9FEF56E8C1A27E9C4CC875390B29003
SHA-512:	3072B716B8A0F6425478687EFB08D53752A76DDDD098B1C5C04E20007C318DFEC32D27CB33C0B9C2C87D21C05F845735DBC00A78569BAC22EEE0B926EC1191 8
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1326
Entropy (8bit):	5.646974021063623
Encrypted:	false
SSDEEP:	24:9ARBuVuDusSVAbLPNHyGIptDoY78BJgskfa9yBDOxo7nQBrxzkr25wdu8jQVVVVD:+OIDGfGIzuU8JFEY8j5EfIg
MD5:	E27110977CF3BAF1BCF69466D5E00DE2
SHA1:	88C7396BD55362853FA329C9979F05938E8C47C4
SHA-256:	196379B1F43DDABAF9894E49FC616FE513CCA1FADD537DE56A962E6DFA300B47
SHA-512:	385BDCEC5A02AEB2D23F641DA1A681AD0F4D8FF5C45B52054456F465A5B6F3909D921AB01E412935CA82F6E608F613E1A3808FE744F6E99932B99F7708CF2517
Malicious:	false
Reputation:	low
Preview:	.....".....4635..478143df..8c6d0..a6e5..alt..appspot..b..c6d8cdc5e89d..com..eeb1..firebasestorage..googleapis..html..https..info..media..o..token..universal..update..v0..yourlawyer*.....4635.....478143df.....8c6d0.....a6e5.....alt.....appspot.....b.....c6d8cdc5e89d.....com.....eeb1.....firebasestorage.....googleapis.....html.....https.....info.....media.....o.....token.....universal.....update.....v0.....yourlawyer..2.....0.....1.....3.....4.....5.....6.....7.....8.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....w.....y...:..... .....

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):	33356
Entropy (8bit):	0.04761656801783402
Encrypted:	false
SSDEEP:	6:+oq7oPotl/Oo34ouood4o9o/vg9bNFlWCj/ll9/l3n:KVlPEYqLBj/nz3n
MD5:	806318485EBB278B35D33582605FE861
SHA1:	CF49195D3252C6B155B4086FBE6F8292E885B759
SHA-256:	33E4026A3CCDBED62ABBDE5EBBD6B6F1BCE565DE8CC10DA66DED334C991CC92E
SHA-512:	F8F4A4E51BF847360B450DEE548934D3E3D4A0B31D50B158AB46D0F78F999F229A71CFCCB21D42482BFB6562CF5B81B9FAA09B89A319ADBF306544CB7E9DCF57
Malicious:	false
Reputation:	low
Preview:	.....- ....

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
Category:	dropped
Size (bytes):	3610
Entropy (8bit):	3.9433515372820094
Encrypted:	false
SSDEEP:	48:34VxTb5EfI8PEYH/ZYQt+q5EfIX5EfIfALPEYH/ZYQt+XDx78VTz15EfI/:34z5oQQ75oQ5oHwQ7V15oK
MD5:	67C5F74CAB6F20645E353CAC153F055D
SHA1:	3DFE92523D66C0787874E63BB3524C7462D5C4DC
SHA-256:	060540E18116EB10781E09CBD4EC2944BAC2AC057D69BA6C10FECFDBEB3A8EC6
SHA-512:	1CDF8A6E1D0E3E335B5F8F808C81504808D03AD7A736DB4E7E122CDF55B54C0E0402D5D9147E1B09F10F3C67C2C4FDD4FA213D15642C691B236C8D7951371F0
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...f58db7f7_5433_4fa4_b3f2_f8c34e50f93b.....i..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....https://firebasestorage.googleapis.com/v0/b/update-8c6d0.appspot.com/o/update%2Fupdate%2Fupdate%2Fupdate%2Fupdate%2FUniversal.html?alt=media&token=478143df-eeb1-4635-a6e5-c6d8cdc5e89d#info@yourlawyer.com.....h.....`.....^4C....._4C.....@.....X.....h.t.t.p.s.:././.f.i.r.e.b.a.s.e.s.t.o.r.a.g.e...g.o.o.g.l.e.a.p.i.s...c.o.m./.v.0./.b./.u.p.d.a.t.e.-.8.c.6.d.0...a.p.p.s.p.o.t...c.o.m./.o./.u.p.d.a.t.e.%.2.F.u.p.d.a.t.e.%.2.F.u.p.d.a.t.e.%.2.F.u.p.d.a.t.e.%.2.F.u.p.d.a.t.e.%.2.F.U.n.i.v.e.r.s

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last TabsId (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):	2955
Entropy (8bit):	5.468749920945704
Encrypted:	false
SSDEEP:	48:N34Gm/a7iMx8dbcr7MbQSefgGbNrS0U9RdiN9h:Sa7iMydbcr7MbQ5fgGprS0/
MD5:	7C3B7C6FFB929E206924CF8934AADAFC
SHA1:	A2ED59146BAFE9A14AFF048BD925ECA0B276AC41
SHA-256:	2A42F49687426637D4A75B2DDBC8F90A8401C8CB11F66040BAAB572C364537F8
SHA-512:	A6FBAC36D6310A6DF55A2875837AC8FD73533E3C9B42A784C854FCFD3DD1511265FB59EFC47781D695714F81B1D578DAD6A19CDF65C093BD94756EA533F8B0B
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..773937000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 19:04:14.27][INFO][mr.Init] MR instance ID: ffdcd83c-c5d9-41d4-9d23-ea11f436e89c\n","[2021-08-03 19:04:14.28][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 19:04:14.28][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 19:04:14.28][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 19:04:14.28][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 19:04:14.28][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 19:04:14.28][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.198456151026425
Encrypted:	false
SSDEEP:	6:mQ2gpM+q2Pwkn23iKKdK8a2jMGIFUtpJImZmwPJ+MVkwOwkn23iKKdK8a2jMmLJ:9M+vYf5Kk8EFUtp5/PEMV5Jf5Kk8bJ
MD5:	797AE1321E6E51078655FED20C149FD1
SHA1:	581D0097BD3F8F171AD2F23B157622D49689D2C3
SHA-256:	346B7726FB80512657263CBC2C0F3C2EAB09D3AB3CD053222AB6F3F5AB0FC0A4
SHA-512:	1E88625571A2CF387165F19EEC9D55C7463CCEB66AD50B2EA116BAD3AFC3AFCD0C5219E82F5731079F0B03AF69CC6959DB812C6BA7A0A4EAF2EDAA0FAA462B2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.288 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-19:03:51.289 176c Recovering log #3.2021/08/03-19:03:51.300 176c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.198456151026425
Encrypted:	false
SSDEEP:	6:mQ2gpM+q2Pwkn23iKKdK8a2jMGIFUtpJImZmwPJ+MVkwOwkn23iKKdK8a2jMmLJ:9M+vYf5Kk8EFUtp5/PEMV5Jf5Kk8bJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
MD5:	797AE1321E6E51078655FED20C149FD1
SHA1:	581D0097BD3F8F171AD2F23B157622D49689D2C3
SHA-256:	346B7726FB80512657263CBC2C0F3C2EAB09D3AB3CD053222AB6F3F5AB0FC0A4
SHA-512:	1E88625571A2CF387165F19EEC9D55C7463CCEB66AD50B2EA116BAD3AFC3AFCD0C5219E82F5731079F0B03AF69CC6959DB812C6BA7A0A4EAF2EDAA0FAA462B2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.288 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-19:03:51.289 176c Recovering log #3.2021/08/03-19:03:51.300 176c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	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":"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 State3d (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):	2438
Entropy (8bit):	4.84523531218547
Encrypted:	false
SSDEEP:	48:Y2nzM3qyvKDHGXtwWsxIDsxLFRSepsxF6q56N6Dsxm8qChpsxNoMHRzgYhbw:JnzMa+KDHGXOvIoLF0/Fx56N6omrCAN2
MD5:	2395B4C262A05680C88EDA884ADF073B
SHA1:	5142EEB08B679503AA93F4022F2B96C08A084548
SHA-256:	C5F9DC9B985D5DDFFE2164C232B7974AFA11349F976F9101E0C2CC24EFB303BD
SHA-512:	24117E77812D2BFE895FD8676DEE63B4471AEBC5AADC13CA0AE3407635A26EFCD21A74449AA8F966165921AA98ADD857687F81CE09AEBEC94720D08CC099F9D
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://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275075840019652","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.google.com","supports_spdy":true},{"alternative_

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):	5.2244017684217186
Encrypted:	false
SSDEEP:	6:mQuljL+q2Pwkn23iKKdKgXz4rRIFUtpJZKWZmwPJUi+LVkwOwkn23iKKdKgXz4qG:gljL+vYf5KkgXiuFUtp6W/PYLV5Jf5K2
MD5:	9B980131FDB3885485F2CB4C11B3FB0B
SHA1:	5997EA4BE9A6176502B755B3738299A405488CD0
SHA-256:	BCC201227CB0C8DAD70BB9646265B8CC91B58A5271D02F6C1BF78A111E640822
SHA-512:	D8120766DC29B995B482BC4B15905EF084BCCB947A0539DD7A7A07D43C8774CC4A203179C7CF1BF9BC2C8D9FA27B6C94DB1F3C777058605E5EE233F3618498(

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.612 173c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-19:03:51.613 173c Recovering log #3.2021/08/03-19:03:51.614 173c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2244017684217186
Encrypted:	false
SSDEEP:	6:mQuljL+q2Pwkn23iKKdKgXz4rRIFUtpJZKWZmwPJUi+LVkwOwkn23iKKdKgXz4qG:gljL+vYf5KkgXiuFUtp6W/PYLV5Jf5K2
MD5:	9B980131FDB3885485F2CB4C11B3FB0B
SHA1:	5997EA4BE9A6176502B755B3738299A405488CD0
SHA-256:	BCC201227CB0C8DAD70BB9646265B8CC91B58A5271D02F6C1BF78A111E640822
SHA-512:	D8120766DC29B995B482BC4B15905EF084BCCB947A0539DD7A7A07D43C8774CC4A203179C7CF1BF9BC2C8D9FA27B6C94DB1F3C777058605E5EE233F3618498(
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.612 173c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-19:03:51.613 173c Recovering log #3.2021/08/03-19:03:51.614 173c 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):	5.174612987345948
Encrypted:	false
SSDEEP:	96:nFLAh9Vx61ReZIKIe5k0JCKL8UVkJ1TbOTlVuHn:nFLs9b61sZIAh4KTkJb
MD5:	92557D9F1357A989DDD7C2ECCB4A4B4C
SHA1:	0BAE61198FF4EE2584092C41458E1CE6074BC1E6
SHA-256:	D7C00DD3E8359DDED9FC9A8D3A6A988F284494A9D42B37DE50965316D0E47EE5
SHA-512:	16B81DB36961824A3FBE6119AB72FDBECC75E0F1AB1E26606832E5C327267956D8AA9082198D2BCAE77DA2C9FFEA52E7C8809D2AA20C7D46FCD1778672F1E0C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272483831542198","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):	57344
Entropy (8bit):	1.1361002001413723
Encrypted:	false
SSDEEP:	192:wIElwQF8mpcSteMfCSIElwQF8mpcS+LElXhlKPfH1:4eMfCjLElXhlKPfH1
MD5:	F511B3CB2FAA8CD93051BD1DC89A4E46
SHA1:	D7BF10111551D4ABC9DFAEB097C6601DD5B75AFF
SHA-256:	86B797795B54AB07401EE97BAE6034DD49D23D844FF409F5CD76FC3803960E1D
SHA-512:	0485960F07617D498F61F184EB6CBB697AC4FF62405B84C53BA1C82F3AB76594D1A3A0EB56AEEAEFC6A1868BB3FDC521F9BB9ADE1FE0433C91E3D90CE77B2F47
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):	58504
Entropy (8bit):	0.8333768118270967
Encrypted:	false
SSDEEP:	192:KhIElwQF8mpcS26CiwfLMxIElwQF8mpcSk:Ke6C7fLMM
MD5:	D08184A45DE6C2862D006F686AFCEB08
SHA1:	C8BAFEAC4F41CE95C1CD71236D65A21C6CFFA24E
SHA-256:	5EF76285A627DC41CAEE6E2782DF7D770F258B2F6C246938D691C030AA35E777
SHA-512:	ED38B84210A123F4A26C9A1DDD414C436C760043101B8805C5CFE35D56A25DD264C3D3D5520E04A9AA43219268D43FC8A5B4A85D041326F78FF759725AF1E3C
Malicious:	false
Reputation:	low
Preview:	.....5..... ....

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):	5.536329378401846
Encrypted:	false
SSDEEP:	384:wNAtyLlwhX51kXqKf/pUZNCgVLH2HfDSrU/HGznZk/+4Y:0Llg51kXqKf/pUZNCgVLH2HfGrUvGzn5
MD5:	CEEF693D46A1DE861E6D1888BB905FA4
SHA1:	E35772F6BF071EA3FD54C98C8D9F671438912E69
SHA-256:	6A241E044CA7F484D2BC863360609387E510E9BB5E4571776B6E394CE1550268
SHA-512:	FC3D71B6E0560D80B9DA7F31197A93DD894582C3181C6ABA0EF7D9DBC39F2A2A33FFD7AE796C2DFC1CA074C61991A7F093BFA8FB28B304BA045B4EDBB9FF3C4
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":"13272483831186439","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl: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):	5.1786986695883845
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
SSDEEP:	6:mQD/+q2Pwkn23iKKdKrQMxIFUtpJDGFZZmwPJDhnVkwOwkn23iKKdKrQMFLJ:5/+vYf5KkCFUtpJm/PJtV5Jf5KktJ
MD5:	4A8341289C7F74D97BA52C6D8F8471C3
SHA1:	C7E30B83E6279FAF507DE9FF003919B09317765E
SHA-256:	536AC43AE315E305692DF94160D5C339BFF8F5623456B4FEC7E76A7DD4700B74
SHA-512:	13D114AF234D98BF200D8FDE0B495E23F06BF08A49C2534CDAD599F5433FF9E9FB07C19160CB64D440F0641C59A0AFBE14FB88096E8A67CBE8B34ED7F863386
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.537 169c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-19:03:51.538 169c Recovering log #3.2021/08/03-19:03:51.539 169c 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):	5.1786986695883845
Encrypted:	false
SSDEEP:	6:mQD/+q2Pwkn23iKKdKrQMxIFUtpJDGFZZmwPJDhnVkwOwkn23iKKdKrQMFLJ:5/+vYf5KkCFUtpJm/PJtV5Jf5KktJ
MD5:	4A8341289C7F74D97BA52C6D8F8471C3
SHA1:	C7E30B83E6279FAF507DE9FF003919B09317765E
SHA-256:	536AC43AE315E305692DF94160D5C339BFF8F5623456B4FEC7E76A7DD4700B74
SHA-512:	13D114AF234D98BF200D8FDE0B495E23F06BF08A49C2534CDAD599F5433FF9E9FB07C19160CB64D440F0641C59A0AFBE14FB88096E8A67CBE8B34ED7F863386
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.537 169c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-19:03:51.538 169c Recovering log #3.2021/08/03-19:03:51.539 169c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.151978233599769
Encrypted:	false
SSDEEP:	6:mQkQyq2Pwkn23iKKdK7Uh2ghZIFUtpJuSG1ZmwPJnQRkwOwkn23iKKdK7Uh2gnLJ:WQyvYf5KklhHh2FUtpsSg/PVQR5Jf5KF
MD5:	65B076A9EA8D81B372879F274921436E
SHA1:	E5338827049B0304FFC7C2D0593FD1D8C929BA3B
SHA-256:	DF7EA03525EFE912CE98A3DA714759CDCAA8304D132D6C7A2BF3565633E39F7B
SHA-512:	3E799C248932DEFEF10D0B4F060889C5CDB0A3833BEC80787976E192B2AC825D944191C99D90D13561E6F76DE846BD4EB397325D88C73B6BF82AE0DBA610F66
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.215 1690 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-19:03:51.229 1690 Recovering log #3.2021/08/03-19:03:51.238 1690 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):	348
Entropy (8bit):	5.151978233599769
Encrypted:	false
SSDEEP:	6:mQkQyq2Pwkn23iKKdK7Uh2ghZIFUtpJuSG1ZmwPJnQRkwOwkn23iKKdK7Uh2gnLJ:WQyvYf5KklhHh2FUtpsSg/PVQR5Jf5KF
MD5:	65B076A9EA8D81B372879F274921436E
SHA1:	E5338827049B0304FFC7C2D0593FD1D8C929BA3B
SHA-256:	DF7EA03525EFE912CE98A3DA714759CDCAA8304D132D6C7A2BF3565633E39F7B
SHA-512:	3E799C248932DEFEF10D0B4F060889C5CDB0A3833BEC80787976E192B2AC825D944191C99D90D13561E6F76DE846BD4EB397325D88C73B6BF82AE0DBA610F66
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.215 1690 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-19:03:51.229 1690 Recovering log #3.2021/08/03-19:03:51.238 1690 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\7ea83294-a583-4899-a7a8-3722784ace79.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
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):	5.28732617151414
Encrypted:	false
SSDEEP:	6:mQJAM+q2Pwkn23iKKdKusNpV/2jMGIFUtpJJSZmwPJJTMVkwOwkn23iKKdKusNp+:kM+vYf5KkFFUtpW/PvMV5Jf5KkOJ
MD5:	F2652E4F7509C1EB79F7416CADED38D3
SHA1:	2C005CB577C54CF6159F05929AD4191C86F00400
SHA-256:	03403571889D0D302B43858A63582DC3DADD78F253217D3E0A00C33361FE4E9E
SHA-512:	3C969B29858FB7F3D749DC5E64ED6CD7DA370E9CB3250115137C1385EA851EEFA9BF9035407966BEA2879E15314CAC2444805F55F1D8D31E750F808509473FC1
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.591 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-19:03:51.594 176c Recovering log #3.2021/08/03-19:03:51.596 176c 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):	5.28732617151414
Encrypted:	false
SSDEEP:	6:mQJAM+q2Pwkn23iKKdKusNpV/2jMGIFUtpJJSZmwPJJTMVkwOwkn23iKKdKusNp+:kM+vYf5KkFFUtpW/PvMV5Jf5KkOJ
MD5:	F2652E4F7509C1EB79F7416CADED38D3
SHA1:	2C005CB577C54CF6159F05929AD4191C86F00400
SHA-256:	03403571889D0D302B43858A63582DC3DADD78F253217D3E0A00C33361FE4E9E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old. (copy)	
SHA-512:	3C969B29858FB7F3D749DC5E64ED6CD7DA370E9CB3250115137C1385EA851EEFA9BF9035407966BEA2879E15314CAC2444805F55F1D8D31E750F808509473FC1
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.591 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-19:03:51.594 176c Recovering log #3.2021/08/03-19:03:51.596 176c Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\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):	5.27893996140671
Encrypted:	false
SSDEEP:	6:mQdl+q2Pwkn23iKKdKusNpqz4rRIFUtpJVZmwPJIKDtVkwOwkn23iKKdKusNpqzW:TwvYf5KkmiuFUtpX/P//5Jf5Kkm2J
MD5:	66D7C93CC86FDC4B6B4B81B579EF725E
SHA1:	F4C3E4CC6F2CAFEBA786AF5A37ACBFA8E30E625D
SHA-256:	36F241423B5B57067F88D01FB27D766778FF586C8573002352AFB29B99D93B5E
SHA-512:	6BB08D6163D44778ED6FB231A6A94F7223A8D4FB77C4595FC68056A2C30688479F837EAC4259BC417A6B728D3C2C5BF747197800BF351C9B33A6E7A87E4ACC5
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.607 16f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-19:03:51.609 16f8 Recovering log #3.2021/08/03-19:03:51.610 16f8 Reusing old log C:\Users\user\AppData\Lo cal\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):	5.27893996140671
Encrypted:	false
SSDEEP:	6:mQdl+q2Pwkn23iKKdKusNpqz4rRIFUtpJVZmwPJIKDtVkwOwkn23iKKdKusNpqzW:TwvYf5KkmiuFUtpX/P//5Jf5Kkm2J
MD5:	66D7C93CC86FDC4B6B4B81B579EF725E
SHA1:	F4C3E4CC6F2CAFEBA786AF5A37ACBFA8E30E625D
SHA-256:	36F241423B5B57067F88D01FB27D766778FF586C8573002352AFB29B99D93B5E
SHA-512:	6BB08D6163D44778ED6FB231A6A94F7223A8D4FB77C4595FC68056A2C30688479F837EAC4259BC417A6B728D3C2C5BF747197800BF351C9B33A6E7A87E4ACC5
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.607 16f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/08/03-19:03:51.609 16f8 Recovering log #3.2021/08/03-19:03:51.610 16f8 Reusing old log C:\Users\user\AppData\Lo cal\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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
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
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.233813872678594
Encrypted:	false
SSDEEP:	6:mNOqL4yq2Pwkn23iKKdKusNpZQMxIFUtp+On1ZmwP+Ob6RkwOwkn23iKKdKusNpB:+L9vYf5KkMFUtpr1/PHe5Jf5KkTJ
MD5:	537DD01929B0A13837347B65EDBF9D2B
SHA1:	A7E7D6EB662A3608594FF81E751B0723F7794C94
SHA-256:	9A3B208B9D0EB7D37B866F3C19640AC7D9C35333CD6CBFB5113848E7135702D3
SHA-512:	963BE315827A69350B6B3B4DB89F53B6097BFB93237049B20A03DC08D0D1555EB9FCA4098A210D33789A6A6C090DB27268F29E29E5B6D1725142C554E6F1C345
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.263 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-19:04:12.270 1710 Recovering log #3.2021/08/03-19:04:12.271 1710 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):	5.233813872678594
Encrypted:	false
SSDEEP:	6:mNOqL4yq2Pwkn23iKKdKusNpZQMxIFUtp+On1ZmwP+Ob6RkwOwkn23iKKdKusNpB:+L9vYf5KkMFUtpr1/PHe5Jf5KkTJ
MD5:	537DD01929B0A13837347B65EDBF9D2B
SHA1:	A7E7D6EB662A3608594FF81E751B0723F7794C94
SHA-256:	9A3B208B9D0EB7D37B866F3C19640AC7D9C35333CD6CBFB5113848E7135702D3
SHA-512:	963BE315827A69350B6B3B4DB89F53B6097BFB93237049B20A03DC08D0D1555EB9FCA4098A210D33789A6A6C090DB27268F29E29E5B6D1725142C554E6F1C345
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.263 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-19:04:12.270 1710 Recovering log #3.2021/08/03-19:04:12.271 1710 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
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):	5.1990073639012815
Encrypted:	false
SSDEEP:	12:4mIvYf5KkkGHArBFUtpIv1/PIB5Jf5KkkGHAryJ:4m6Yf5KkkGgPgyqTJf5KkkGga
MD5:	1E3AB4E88D2E0FF84C94DF0C0D0F5EB0
SHA1:	782E574F21929685596C447A8274C3BD1F5139D5
SHA-256:	247634BA09BE8AD390EB629FF90D122D1CD9A989A634D9239E7FAE3CAB0291F0
SHA-512:	258C2D7051BE99E14F50A7066435D409B32FE270D567237C7A3648A23C9480A66850645EC23648B57DC9727B6BDEA1EE75DB0E96E6B1D1AC7D13E56BC7B7680
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:13.389 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-19:04:13.393 1710 Recovering log #3.2021/08/03-19:04:13.395 1710 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\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):	5.1990073639012815
Encrypted:	false
SSDEEP:	12:4mIvYf5KkkGHArBFUtpIv1/PIB5Jf5KkkGHAryJ:4m6Yf5KkkGgPgyqTJf5KkkGga
MD5:	1E3AB4E88D2E0FF84C94DF0C0D0F5EB0
SHA1:	782E574F21929685596C447A8274C3BD1F5139D5
SHA-256:	247634BA09BE8AD390EB629FF90D122D1CD9A989A634D9239E7FAE3CAB0291F0
SHA-512:	258C2D7051BE99E14F50A7066435D409B32FE270D567237C7A3648A23C9480A66850645EC23648B57DC9727B6BDEA1EE75DB0E96E6B1D1AC7D13E56BC7B7680
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:13.389 1710 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-19:04:13.393 1710 Recovering log #3.2021/08/03-19:04:13.395 1710 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.227816229816073
Encrypted:	false
SSDEEP:	12:4evYf5KkkGHArqiuFUtpI4/PI65Jf5KkkGHArq2J:48Yf5KkkGgCgy1kJf5KkkGg7
MD5:	9640FF4F0F0C44818240AFCC02D585AE
SHA1:	EB81EE30FC684DBF0A16FC9EBD5B1E2294DBF2B7
SHA-256:	1ADCC9AE9E7EADE379AE9740E90A70783589B6FDAC56624D085DD54F8E393300
SHA-512:	5D6D76FA8EF667CDF270A4A085C72A1CCEB6C1DB30AD9636DA09FA8431C0302CF74760E95A397A5E90AFA7421A2CD4C43A3A6DF89E6D4B654BEB3B5DE0C8177
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:13.393 1688 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/03-19:04:13.396 1688 Recovering log #3.2021/08/03-19:04:13.398 1688 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.227816229816073
Encrypted:	false
SSDEEP:	12:4evYf5KkkGHArqiuFUtpI4/PI65Jf5KkkGHArq2J:48Yf5KkkGgCgy1kJf5KkkGg7
MD5:	9640FF4F0F0C44818240AFCC02D585AE
SHA1:	EB81EE30FC684DBF0A16FC9EBD5B1E2294DBF2B7
SHA-256:	1ADCC9AE9E7EADE379AE9740E90A70783589B6FDAC56624D085DD54F8E393300
SHA-512:	5D6D76FA8EF667CDF270A4A085C72A1CCEB6C1DB30AD9636DA09FA8431C0302CF74760E95A397A5E90AFA7421A2CD4C43A3A6DF89E6D4B654BEB3B5DE0C8177
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:13.393 1688 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-19:04:13.396 1688 Recovering log #3.2021/08/03-19:04:13.398 1688 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):	5.237985989096677
Encrypted:	false
SSDEEP:	12:VL+vYf5KkkGHArAFUtpEW/PfLV5Jf5KkkGHArfJ:VYYf5KkkGgkgZDJf5KkkGgV
MD5:	C01BF54EAC57319FECF1DD9702672D3E
SHA1:	68FBCE17CAFB1607B708C1E3CFCCD0257E404581
SHA-256:	E11C102AA7E370C5FD640AD37023AEA1E97624A569572D74E67BA52F97C986D1
SHA-512:	32E3C4BB18381DE8C156B38A045A2C7FF58E8B52340908249BFF7C2056F8B231B50C40E555EF2F535C88AA60102BC105B38FA03E93F957DCDADE23345A768B8
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:28.656 173c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-19:04:28.658 173c Recovering log #3.2021/08/03-19:04:28.658 173c 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.old27 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.237985989096677
Encrypted:	false
SSDEEP:	12:VL+vYf5KkkGHArAFUtpEW/PfLV5Jf5KkkGHArfJ:VYYf5KkkGgkgZDJf5KkkGgV
MD5:	C01BF54EAC57319FECF1DD9702672D3E
SHA1:	68FBCE17CAFB1607B708C1E3CFCCD0257E404581
SHA-256:	E11C102AA7E370C5FD640AD37023AEA1E97624A569572D74E67BA52F97C986D1
SHA-512:	32E3C4BB18381DE8C156B38A045A2C7FF58E8B52340908249BFF7C2056F8B231B50C40E555EF2F535C88AA60102BC105B38FA03E93F957DCDADE23345A768B8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old27 (copy)	
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:28.656 173c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/08/03-19:04:28.658 173c Recovering log #3.2021/08/03-19:04:28.658 173c Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
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):	5.257556234041532
Encrypted:	false
SSDEEP:	6:mQCE9+q2Pwkn23iKKdKpIFUtpJnwJZmwPJok9VkwOwkn23iKKdKa/WLJ:li+vYf5KkmFUtp5y/PaCV5Jf5KkaUJ
MD5:	4628AE1182C5BADD3BE1970C439F333F
SHA1:	ED98C5104340AE9910B66A18EE83A8618DE56038
SHA-256:	F1DD6A82676C915C315F888E89CFF1C0906E7BE0AF40242111D02BD2282FEBBE
SHA-512:	379E59B376E18C833C23E543B0C4E9625E453BE2135C31D6F86C1CA0545DD200D87AC5EFC51210D28ECAB95CE5193EE6D6980A842167C036308764D230058B3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.239 16bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-19:03:51.281 16bc Recovering log #3.2021/08/03-19:03:51.284 16bc 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.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.257556234041532
Encrypted:	false
SSDEEP:	6:mQCE9+q2Pwkn23iKKdKpIFUtpJnwJZmwPJok9VkwOwkn23iKKdKa/WLJ:li+vYf5KkmFUtp5y/PaCV5Jf5KkaUJ
MD5:	4628AE1182C5BADD3BE1970C439F333F
SHA1:	ED98C5104340AE9910B66A18EE83A8618DE56038
SHA-256:	F1DD6A82676C915C315F888E89CFF1C0906E7BE0AF40242111D02BD2282FEBBE
SHA-512:	379E59B376E18C833C23E543B0C4E9625E453BE2135C31D6F86C1CA0545DD200D87AC5EFC51210D28ECAB95CE5193EE6D6980A842167C036308764D230058B3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:03:51.239 16bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-19:03:51.281 16bc Recovering log #3.2021/08/03-19:03:51.284 16bc 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Size (bytes):	402
Entropy (8bit):	5.316646909909075
Encrypted:	false
SSDEEP:	12:V7LW+L+vYf5KkkOrsFUtpFgW/PFDLV5Jf5KkkOrzJ:ti+YYf5Kk+gFDJf5Kkn
MD5:	9C0A2B8B063A45D022749403E63E0B59
SHA1:	09961735439773DCD8CE06791F52D12C23ACBAB1
SHA-256:	0DD4B76D89EEE6F2193713646D969C1A3AFFD16FED4FAD23E992B73C699CF0F1
SHA-512:	1A0DD7CD45BB2515D989733EDC903B279C0CB6FD672D4F64A7206CF58A17E0E882DE7C22394F0B5986CB8A38DBE387EFB10F5F54F950F61E55CB3D2C00ED396
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:14.273 173c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-19:04:14.275 173c Recovering log #3.2021/08/03-19:04:14.275 173c 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):	5.316646909909075
Encrypted:	false
SSDEEP:	12:V7LW+L+vYf5KkkOrsFUtpFgW/PFDLV5Jf5KkkOrzJ:ti+YYf5Kk+gFDJf5Kkn
MD5:	9C0A2B8B063A45D022749403E63E0B59
SHA1:	09961735439773DCD8CE06791F52D12C23ACBAB1
SHA-256:	0DD4B76D89EEE6F2193713646D969C1A3AFFD16FED4FAD23E992B73C699CF0F1
SHA-512:	1A0DD7CD45BB2515D989733EDC903B279C0CB6FD672D4F64A7206CF58A17E0E882DE7C22394F0B5986CB8A38DBE387EFB10F5F54F950F61E55CB3D2C00ED396
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:14.273 173c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-19:04:14.275 173c Recovering log #3.2021/08/03-19:04:14.275 173c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1710
Entropy (8bit):	5.5800886019550076
Encrypted:	false
SSDEEP:	48:YEcRUgvVwU/6UUhSeU/KUvYqPeUekUe0wU0tsYUHUeP:sRUZUCUU1U/KUvHPeU3UCU0+YUHUg
MD5:	AC584E4227B1942102F0A7722C1FF03E
SHA1:	DBA2E873E636E584D2799683F98BC38A705048E2
SHA-256:	7B5262D2018557610E8C5D49C1F79795D8B24808F6681EA5F33A08E443325624
SHA-512:	B46F185EF5E759D78B86240173F25AA0B4E48DCB7F882E8AB0EC587797EBB616F66B33C6584A411676617295C413216F58013D8E0DD7BF800D83F1ECD052F517
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659546245.921696,"host":"AKBA0EXj1W1QmJumkxUOTpibibkAwoUEp1CDrh5UFWY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628010245.921703},{"expiry":1643790245.166417,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628010245.166421},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1659546244.046669,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628010244.046677},{"expiry":1659546245.137379,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628010245.137385},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_o

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:E8CCGn:QCG
MD5:	A8AAA7A455690F7B3D4FDE4371EFFDB0
SHA1:	CB59D0EBA956F83607632F5829379E8CEFD863C0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
SHA-256:	7D6170F246A020D8531C42591E9491BF1543D98E54D0040D1CE1BB4C4E32B60D
SHA-512:	13B34B2F692A781F8234164BC17974B8BB4C93938CEFEC448215122192554EAD2C66D97A2B356AEF6DA612D902F00E4523065556A0B6786EDF9E172CA48BC25A
Malicious:	false
Reputation:	low
Preview:	....`Y.y)f.R

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a1f2131f-08be-4cbb-adee-fac0cb016721.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):	5.536329378401846
Encrypted:	false
SSDEEP:	384:wNAtyLlwhX51kXqKf/pUZNCgVLH2HfDSrU/HGznZk/+4Y:0Llg51kXqKf/pUZNCgVLH2HfGrUvGzn5
MD5:	CEEF693D46A1DE861E6D1888BB905FA4
SHA1:	E35772F6BF071EA3FD54C98C8D9F671438912E69
SHA-256:	6A241E044CA7F484D2BC863360609387E510E9BB5E4571776B6E394CE1550268
SHA-512:	FC3D71B6E0560D80B9DA7F31197A93DD894582C3181C6ABA0EF7D9DBC39F2A2A33FFD7AE796C2DFC1CA074C61991A7F093BFA8FB28B304BA045B4EDBB9FF3C4
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":"13272483831186439","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\ad05f71e-0b88-462c-817c-553ecb68b580.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):	5.536191679373252
Encrypted:	false
SSDEEP:	384:wNAtyLlwhX51kXqKf/pUZNCgVLH2HfDSrU/HG8nZky+4l7:0Llg51kXqKf/pUZNCgVLH2HfGrUvG8nb
MD5:	23183603A14F6C8F8B15B6F8D71E1664
SHA1:	DC68F3BF094FDABB475E9AD673591E253EABB10C
SHA-256:	4D7B68F0D3F5B3376AE1D1878474B51318387B70CDF6AE4AACD4EB53141A6C6D
SHA-512:	8FC187244129BF0625454AB36ADF3C670C877B8E1173C219CD7F5F66D0A03DCCE24356BBE3F1F0AF1F8FE4EAB8048F1122F8432832E1F0C5135430341DDDA77
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":"13272483831186439","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\d5d7d93b-431c-4c68-8847-8b5f02cf47ab.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):	5.577429337891301
Encrypted:	false
SSDEEP:	384:wNAtTLlwhX51kXqKf/pUZNCgVLH2HfDSrUHs+4a:1Llg51kXqKf/pUZNCgVLH2HfGrUM+d
MD5:	CF10B59FA463E00D811BA14C8EF9F324
SHA1:	CE024024372630029A49339BEDF13B786554B2A6
SHA-256:	01EB523D4DE549880627F780EAE678BB50B04D1843882EFCADDD76A710865219
SHA-512:	718FB6D6823FB559252C52FC7D3C42FA8B3FC87B0386C9E56C58C313FEDFBDC29B8813095DC22F053D08740FBE567CD6EB9BE553956EC777C48B50ECA46277C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d5d7d93b-431c-4c68-8847-8b5f02cf47ab.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":"13272483831186439","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\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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENTl (copy)	
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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.536779994117245
Encrypted:	false
SSDEEP:	3:tUK6zOpFwgZmwv3lzOjfW01V8sIzOjfW01WGv:mNO8gZmwP+OjjVv+Ojjtv
MD5:	C403B6347DF33541DBBD83FFE70D6690
SHA1:	51B906E8784E4098AD29621CAB0D1D4D18C81AF9
SHA-256:	9E6E3EE2ED81065BF552F64E647FD6A6E30A7DAE3AC8B79699A83BE8B7337307
SHA-512:	35DACA4A7193C26396CC5BA9CEBF1252E0C4802C903A0619D1D1FBB1E578C9A1610256AB7B044EF9FE14F7C2165EF53C4B46A9D47E6CBAD500F25503E8ECAA0B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.369 16a0 Recovering log #3.2021/08/03-19:04:12.435 16a0 Delete type=0 #3.2021/08/03-19:04:12.435 16a0 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.olde (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.olde (copy)	
Entropy (8bit):	4.536779994117245
Encrypted:	false
SSDEEP:	3:tUK6zOpFwgZmwv3lzOjfW01V8slzOjfW01WGv:mNO8gZmwP+OjjVv+Ojjtv
MD5:	C403B6347DF33541DBBD83FFE70D6690
SHA1:	51B906E8784E4098AD29621CAB0D1D4D18C81AF9
SHA-256:	9E6E3EE2ED81065BF552F64E647FD6A6E30A7DAE3AC8B79699A83BE8B7337307
SHA-512:	35DACA4A7193C26396CC5BA9CEBF1252E0C4802C903A0619D1D1FBB1E578C9A1610256AB7B044EF9FE14F7C2165EF53C4B46A9D47E6CBAD500F25503E8ECAA0B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.369 16a0 Recovering log #3.2021/08/03-19:04:12.435 16a0 Delete type=0 #3.2021/08/03-19:04:12.435 16a0 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.257566273114117
Encrypted:	false
SSDEEP:	6:mNObHM+q2Pwkn23iKKdKfrzAdIFUtp+OddKXZmwP+O2MVkwOwkn23iKKdKfrzILJ:PM+vYf5Kk9FUtp5d6/PyMV5Jf5Kk2J
MD5:	24D6EF5BA2B2759924746512F8FDE1B2
SHA1:	C5C7A20D1D089A23F81D39CD20E3A9CFCD256E59
SHA-256:	0D62F56496EC185CECC6D0F63612E8F6B8AF9941314B7F2139B764968A2C0336
SHA-512:	30B7A1C189C528F8A0C862071393F307CD53E4172F72E30B810C6C3B117F2693DAF5CE457B6BCFE88CFE4D25E3B7DF62E3C9A6F13DCEC4A4299145D1D21DBE0
Malicious:	false
Reputation:	low
Preview:	2021/08/03-19:04:12.833 176c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-19:04:12.835 176c Recovering log #3.2021/08/03-19:04:12.836 176c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

Static File Info

No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-19:04:00.123092	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55854	8.8.8.8	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 19:04:00.086601019 CEST	192.168.2.4	8.8.8.8	0x37	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:00.092129946 CEST	192.168.2.4	8.8.8.8	0x2ac7	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:04.152080059 CEST	192.168.2.4	8.8.8.8	0x82b5	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:04.156846046 CEST	192.168.2.4	8.8.8.8	0x52f8	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:04.231170893 CEST	192.168.2.4	8.8.8.8	0x82d4	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:04.234105110 CEST	192.168.2.4	8.8.8.8	0x5672	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:04.248420954 CEST	192.168.2.4	8.8.8.8	0xe0b1	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:06.898662090 CEST	192.168.2.4	8.8.8.8	0x54d0	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:07.184581995 CEST	192.168.2.4	8.8.8.8	0xae5e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:12.461560965 CEST	192.168.2.4	8.8.8.8	0xdc5b	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:12.997858047 CEST	192.168.2.4	8.8.8.8	0x9873	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 19:04:00.121880054 CEST	8.8.8.8	192.168.2.4	0x37	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:04:00.121880054 CEST	8.8.8.8	192.168.2.4	0x37	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:00.124794960 CEST	8.8.8.8	192.168.2.4	0x2ac7	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:04.179770947 CEST	8.8.8.8	192.168.2.4	0x82b5	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:04:04.198012114 CEST	8.8.8.8	192.168.2.4	0x52f8	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:04:04.262742996 CEST	8.8.8.8	192.168.2.4	0x5672	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:04.262742996 CEST	8.8.8.8	192.168.2.4	0x5672	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:04.268079996 CEST	8.8.8.8	192.168.2.4	0x82d4	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:04.268079996 CEST	8.8.8.8	192.168.2.4	0x82d4	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 19:04:04.286978960 CEST	8.8.8.8	192.168.2.4	0xe0b1	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:04.286978960 CEST	8.8.8.8	192.168.2.4	0xe0b1	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:05.574449062 CEST	8.8.8.8	192.168.2.4	0x8127	No error (0)	gstaticadssl.l.google.com		142.250.185.163	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:06.935663939 CEST	8.8.8.8	192.168.2.4	0x54d0	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:04:07.212068081 CEST	8.8.8.8	192.168.2.4	0xae5e	No error (0)	www.google.com		142.250.180.164	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:12.499469995 CEST	8.8.8.8	192.168.2.4	0xdc5b	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:04:12.499469995 CEST	8.8.8.8	192.168.2.4	0xdc5b	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:13.041440964 CEST	8.8.8.8	192.168.2.4	0x9873	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:04:13.041440964 CEST	8.8.8.8	192.168.2.4	0x9873	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4824 Parent PID: 4940

General

Start time:	19:03:49
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://firebasestorage.googleapis.com/v0/b/update-8c6d0.appspot.com/o/update%2Fupdate%2Fupdate%2Fupdate%2Fupdate%2FUniversal.html?alt=media&token=478143df-eeb1-4635-a6e5-c6d8cdc5e89d#info@yourlawyer.com'
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: 5888 Parent PID: 4824

General

Start time:	19:03:54
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=1568,5417355904452027015,11801000389847120122,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1800 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Disassembly

Copyright Joe Security LLC

Copyright Joe Security LLC 2021