ID: 458786
Cookbook: browseurl.jbs
Time: 18:41:33
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

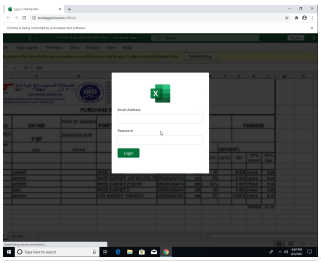
Windows Analysis Report https://tendaggisilvana.it/offic…

Overview

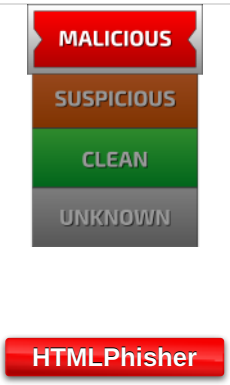
General Information

Sample URL:	http://https://tendaggisilvana.it/officix/
Analysis ID:	458786
Infos:	

Most interesting Screenshot:



Detection

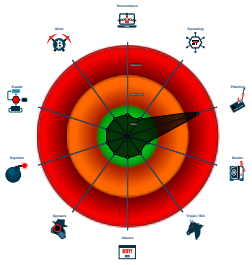


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5800 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://tendaggisilvana.it/officix/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5984 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1632,162788243972043073,8402254026257192306,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1744 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

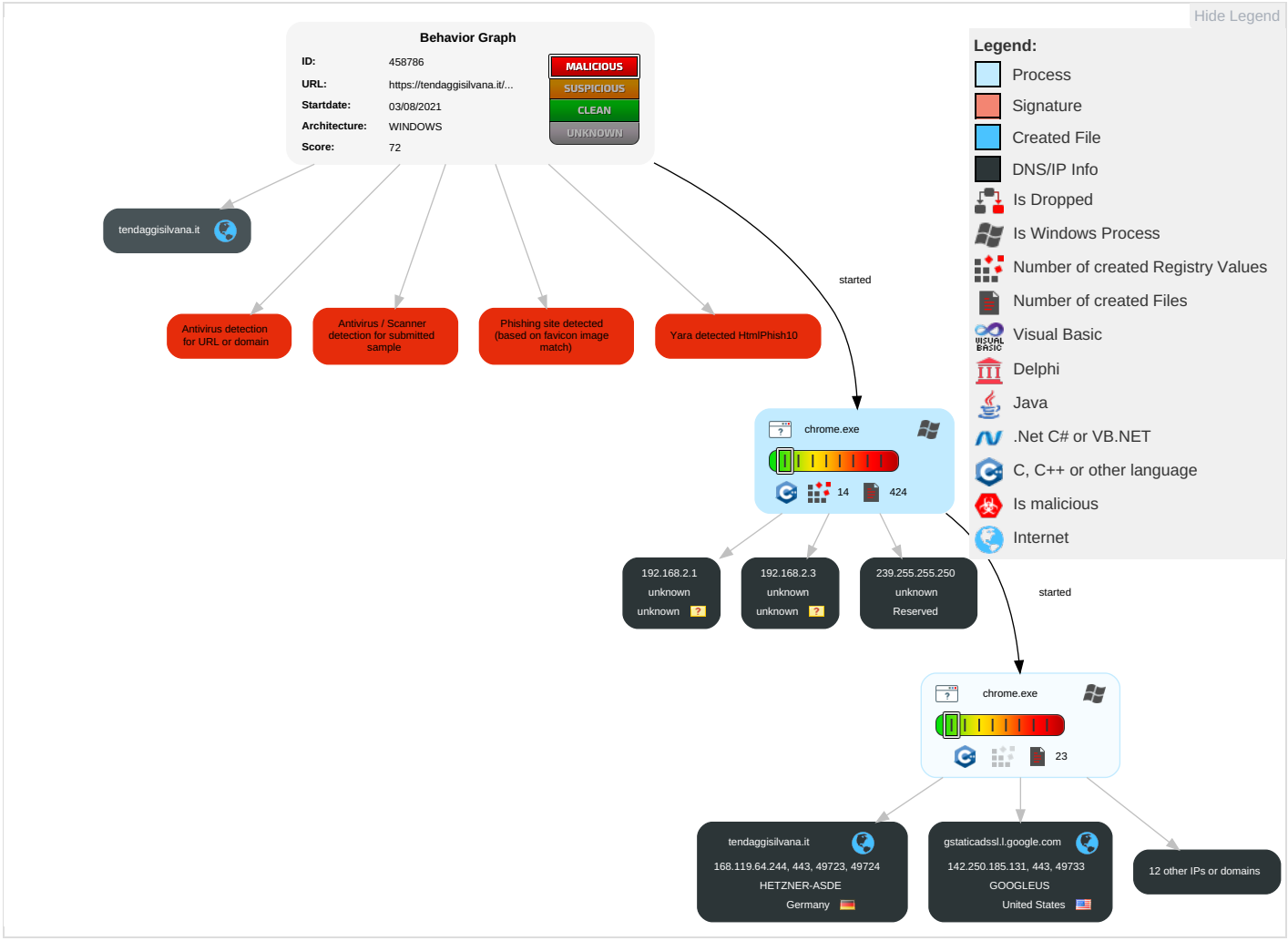
Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Mitre Att&ck Matrix

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

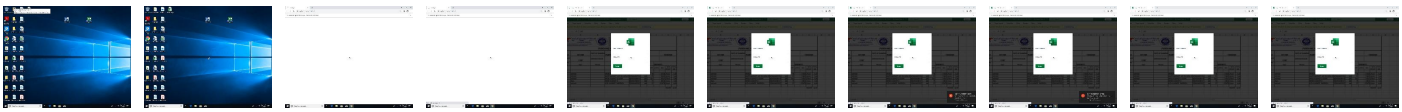
Behavior Graph

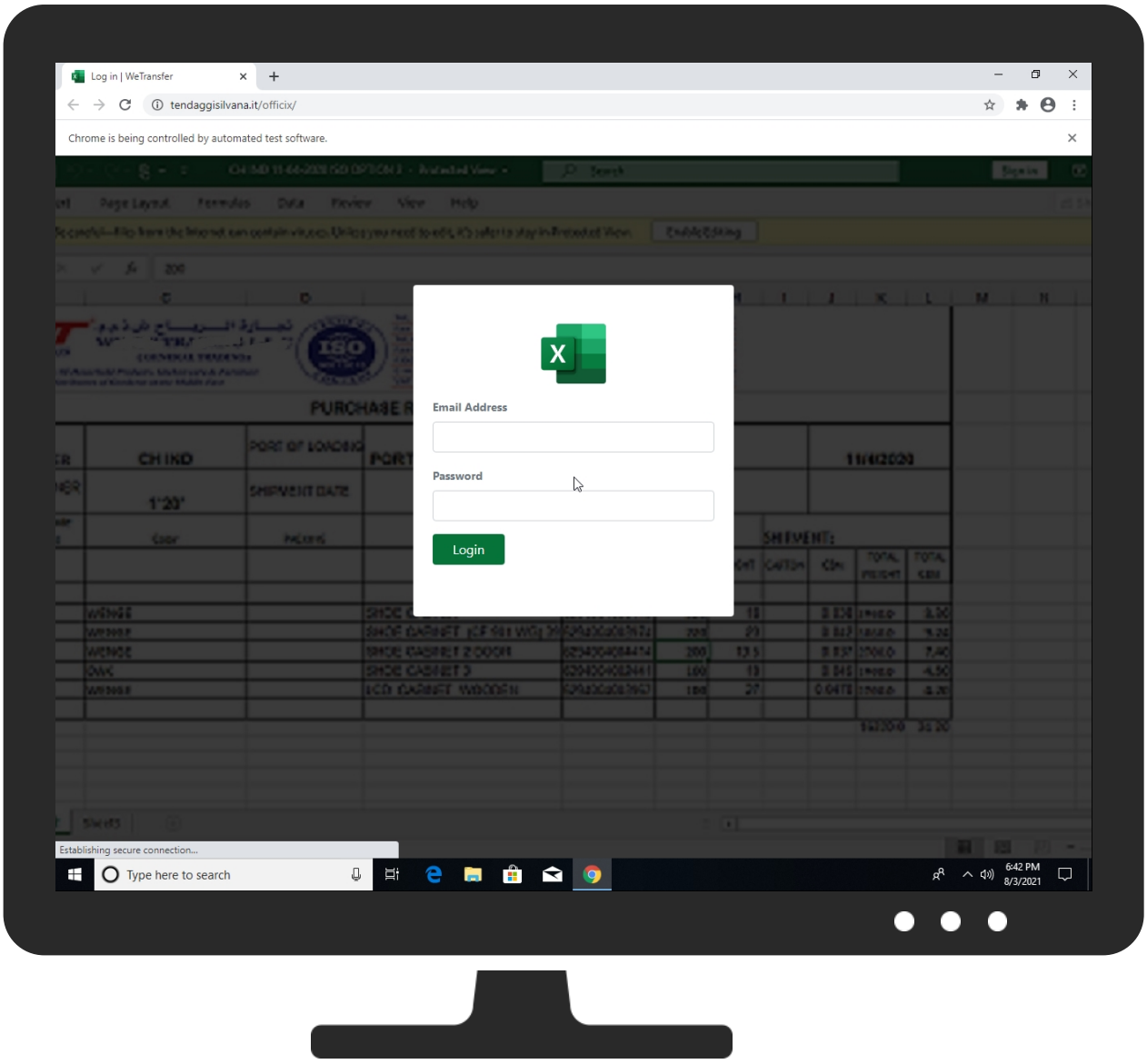


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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

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	

Source	Detection	Scanner	Label	Link
http://https://tendaggisilvana.it/	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://54.211.202.147/excel-b/excel/excel/mailred.php	100%	Avira URL Cloud	phishing	
http://https://tendaggisilvana.it/officix/2	0%	Avira URL Cloud	safe	
http://https://tendaggisilvana.it	0%	Avira URL Cloud	safe	
http://https://tendaggisilvana.it/g	0%	Avira URL Cloud	safe	
http://https://tendaggisilvana.it/officix/Log	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://tendaggisilvana.it/officix/images/logo.png	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.185.131	true	false		high
stackpath.bootstrapcdn.com	104.18.11.207	true	false		high
accounts.google.com	216.58.205.77	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
tendaggisilvana.it	168.119.64.244	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.208.161	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

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

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458786
Start date:	03.08.2021
Start time:	18:41:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://tendaggisilvana.it/officix/
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@32/223@11/12
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:42:36	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$...._Y..Y`&..s.1.....s.{..,.":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.111501739428656
Encrypted:	false
SSDEEP:	6:kKixl8doW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:A+5kPlE99SNxAhUe0et
MD5:	82A51954B62F5E51582923358534490E
SHA1:	CA53074101D3D025C34D358845FF8EB339B29494
SHA-256:	793AC846B680E9F0DA091DC6F7FCC3E9B9278312552226BF3527677813D41334
SHA-512:	072638BA31148B79D2427AB3C3C5832A356A3EAAC47970297B06493221A28CF31AA65E681831E00E1E5FFD50A46A949B1387514C6E0E99F77B117BB44D192EF0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	p..... .....l.....(..... ....T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\3aa58be2-2ecb-4993-9ab3-30edba5288d4.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):	377420
Entropy (8bit):	6.049277100439161
Encrypted:	false
SSDEEP:	6144:llpUubUVG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinv:zpUubUVGNPUZ+w7wJHyEtAW+
MD5:	8F00AEDB209DFB44F6B35B33E82FA902
SHA1:	E838035B9170FD435FA3394E60B41CC939229C5F
SHA-256:	B29164B51B5184C0321D782FC7F4D50A22558D73EF109C52C00B73E23D0B8FB5
SHA-512:	FA8A4FC1817DC481FDA94EFC4A655D7CB713C1489EDD5A38479C143211D600C5E9B1971890B93AACBF58037C027A254AE6B3D1C7FA6F84D8366A45942C0727C A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628041353697964e+12,"network":1.628008955e+12,"ticks":5262840506.0,"uncertainty":5040604.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0JJd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\4a649860-1e37-49b1-b266-cf583d98f954.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.748218627776533
Encrypted:	false
SSDEEP:	384:d3e1dD4CbgjLVkq54NZryvdn3GJHiHzeGq9rIbx9xW3vTurs9mcIe43JJh2OjDJC:da2Blab4awerhXboH7GjKFbBpg
MD5:	9AA065FFFC53BBD8AAFDFD9487D80023
SHA1:	D4E3F5BA31D50856EAA7AC4996D5AF09170E1314
SHA-256:	ADF67A1019050FAEADE00BE3C5DC3A44C46FD1C7854121C4D7A1FC543185E645
SHA-512:	95F426E554A8BFA0F4ADABBF3A1A7D7ECD7E21960261B6551D6EDF54BCC4CB51B8E355FFE28D78567CA8895515C17F9DC713AB88802CEF920E8C718E779E18 5
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\5e19e68d-ded2-4729-bdf9-0dbfdcaa9aaa.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):	368961
Entropy (8bit):	6.028190535639912
Encrypted:	false
SSDEEP:	6144:klpUubUVG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinv:qpUubUVGNPUZ+w7wJHyEtAW+
MD5:	782762469A57CB8FB92DB5ABDD13400F
SHA1:	1D2637716220FD70259EFDAD09ACBC1B1ACBA9A6
SHA-256:	E02088F6C1ABA13AD8BE10E846B6F3236442C9BE1D19A67C6CFA4671C3E1D607
SHA-512:	ED6C928307799E091C56B09412EF42BA510B1E25BE9A2DE19E2C1EA3795979DDBC070AEA5B845C28D743E59E715A33AE089CDB6846DA671AA747FD03DC9118 0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\5e19e68d-ded2-4729-bdf9-0dbfdcaa9aaa.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628041353697964e+12,"network":1.628008955e+12,"ticks":5262840506.0,"uncertainty":5040604.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488669178"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\722de754-c991-41f3-9aea-a58889d3d082.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.747808746884563
Encrypted:	false
SSDEEP:	384:D3e1dD4CHjM54NZryvdn3GJHiHzeGq9rIbx9xW3vTurs9mc/43JJh2OjDJNI1xIp:i2BlabCawerhXboH7GjKFbBpB
MD5:	C9A2830C0847675B67A30DC1804FD474
SHA1:	9129D2EE60F51ED95D0D0ABE1272F5BA0FB31DBC
SHA-256:	2A1845E6F35D3A2366ED7AFAFBB71D3CC009F4140849D7E5D546F202CF158892
SHA-512:	9CBBA0B9339E81ABF4225B416E7DCEB18FE9A4B85BCA387AB6C30D4858113E02E312878F1CAAA0F0B486A6BFE91D4BBA29E8FC8DA857DB7A6C850B0C7229027B
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\73ee8ad8-27a1-41ef-9053-eb8c1ef8c5b9.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):	377420
Entropy (8bit):	6.0492773412606455
Encrypted:	false
SSDEEP:	6144:vlpUubUVG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinv:dpUubUVGNPUZ+w7wJHyEtAW+
MD5:	841A8E0581ACAEAABEE5B84725FEAC93
SHA1:	BF196483A9AD8B7EF9B462511B5A2CDADC844C3B
SHA-256:	E272B74F6842DAC0A50E568B8D08291F328B22E3B5C7CAA455B71A51C3D735AB
SHA-512:	33FD9D4C2D6941FEF8D382A12F0703C2C1FF5613B17A9953A8AAE78FCF4EA0355EC1208137DA970CFB2FDF1EAB4D1287544C384A8A1C2B71E36EC6382C2484F6
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628041353697964e+12,"network":1.628008955e+12,"ticks":5262840506.0,"uncertainty":5040604.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\94df18bb-9af4-409c-bfdc-8be5bbbe698c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.748270505369668
Encrypted:	false
SSDEEP:	384:t3e1dD4CbgjLVkq54NZryvdn3GJHiHzeGq9rIbx9xW3vTurs9mc/43JJh2OjDJNl:Na2BlabCawerhXboH7GjKFbBpF
MD5:	669FC6E2F812A8D41FA39F4E3C57EFFF
SHA1:	692C930BD58F1B17BE3705C58A73F7497108E96C
SHA-256:	5CFECBA4BC9BC4F9D81BB368350304C7AD516CF542AFCCE060E9CA78E7DBC011
SHA-512:	D4002E68149823D2BCA7FFC1A815948A24D07982EAC444A1D60C1CE4BB62AAE8A430648B077E3CD27F0293923350E4A297E66CB90934A247A3A8016B34D6E531
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\94df18bb-9af4-409c-bfdc-8be5bbbe698c.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\9a50a46f-5a29-45df-8020-87dc5478f6c0.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):	377420
Entropy (8bit):	6.04927730526711
Encrypted:	false
SSDEEP:	6144:ylpUubUVG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinv:gpUubUVGNPUZ+w7wJHyEtAW+
MD5:	F2017480FCE3C23B4C6F9BA57B0E4BD2
SHA1:	067A7240CA2B7A4927815AFE588D16E3B6134D5B
SHA-256:	6BC67FB22ABE7AB9A216F9FE1B035E118318CADAC80E385744967626F0A91070
SHA-512:	41A168D93AC06012CB56F0E7C1C0FE9D335133F68BAE63CB50880B6A8E04BD55F743AF928954DC23ED6DF4FC4ACF2F7048EBC9A6150E6D29FECD7F32651CD4F
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628041353697964e+12,"network":1.628008955e+12,"ticks":5262840506.0,"uncertainty":5040604.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488669178"},"plugins":{"metadata":{"adobe-flash-player":{"dis

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\04fdd6e9-8973-49ff-a896-5daff47a3ff0.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):	5143
Entropy (8bit):	4.978438494842401
Encrypted:	false
SSDEEP:	96:n7XbGXqm9paAKIWxk0JCKL8IOki1f1TbOTQVuwn:n7XbJm9p9c4KwkiBB
MD5:	49FFA8D80F56F0652750F5BC324AD6C7
SHA1:	32FF309082A345BB89A11C819AB79657A4306F2A
SHA-256:	82DDEF90A1459FC93746F6C3D9D746137DEF83445664AEE598066109AEB321A8
SHA-512:	44F67088BE3FE5DD2D175FA7E08EC361C57181A92618B8A006ED2EA6A057B8DE6AE13CA80B41CF41FA7B7E1F523CD980047C3FFC6E8F4E01686AEFC545F4B8D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\04fdd6e9-8973-49ff-a896-5daff47a3ff0.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272514948953045","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\10b9c84d-2825-4c53-b404-2edaaa435120.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):	5.577760656476388
Encrypted:	false
SSDEEP:	384:wLWtrLlanXC1kXqKf/pUZNCgVLH2HfDdrUKRfvO41:NLlsC1kXqKf/pUZNCgVLH2HfJrUKRXOa
MD5:	73A4A79990F541531B8CC1EA46ADF0C5
SHA1:	BB0E14CF1AC7621CA63AA5B3A3BD0CCCCAEF0856
SHA-256:	4095EDB609EDC329F8CBB167537ACB4CF3784448F67B8549C7140C071428D12E
SHA-512:	A412495CF158AAFE2E370AD16A775F71F8E670347A5B363323D7694FCBB9F68070C989B712C6E97EEB47B577EE83D8C232A1B83E63130F47FF42A70A4855FA8F
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":"13272514948694790","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\37ffeead-724a-4b78-a7c5-618267c9cbd3.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):	3263
Entropy (8bit):	4.887174369154771
Encrypted:	false
SSDEEP:	96:2lNnOTXDHzlzR0gNxC56NC6CriLlW6UuxhS:2lNnOTXDHzlzR0gNxC56NC6CrKcvui
MD5:	9F724EAA2B5B3F672DEA27B7811EED5E
SHA1:	2423F66222C47690CC5009C58C3F46C471C4C58A
SHA-256:	2A98A4CC2E578ECE676D097C91FACE2ACCA7378F9CEFA3F39866E5B00A02494E
SHA-512:	79D7BC453F4E28D532C46D25830BC833BEBF1FA59A694C61A470F4958EF733EFC26B9FFA9A20672E4408D74A72C4F3D7A080BC09459EFF41C826F841AD56A7D
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275106955635504","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275106955671490","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3948afb1-3bfa-43d0-8c5f-073146cb0677.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):	22595
Entropy (8bit):	5.536302603002514
Encrypted:	false
SSDEEP:	384:wLWtKLlanXC1kXqKf/pUZNCgVLH2HfDdrUxHGmnTcRf8O4s:ULlsC1kXqKf/pUZNCgVLH2HfJrUlGmni
MD5:	792D089B5D27BFB0A865A65E6013B10D
SHA1:	F4E58194A5340B23E5E708A6B8426541DB31FF7F
SHA-256:	E57FDD310886D27198BBBF37FEB1F5160D97E2886D058462C9E492580AEA985A
SHA-512:	F85F33D1285388F378F0A92AB056A98034A16C49D81489DD502ED155BF1EDCCEF9840C2894BDB61FD4E6FC803571CCBCD10FFAF5FE234B30E613AFDB92C90FC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3948afb1-3bfa-43d0-8c5f-073146cb0677.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":"13272514948694790","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\3ddb2680-3b07-46e4-8895-0e3ec4b143ad.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):	1544
Entropy (8bit):	5.575619506760185
Encrypted:	false
SSDEEP:	48:YGcRUaVwUD6UUhcoeUe5ZKU6qaUeBwUc4sYUghUew:qRU9UWUUa9UezKU1aUPUcpYUGUD
MD5:	FE77ADA1677BFBA152C1036237605B1A
SHA1:	0DAF48A5F0EDA337A2719A2C6650E0DC05E6D266
SHA-256:	CC06F60D47E8E6289960E274F8F5E24A522B8E4E720D836C293172E53B11C787
SHA-512:	C4683783FCB1FE4EEA81234CEC67F12EB35CAFC03F8C1A42C493EF501EECB8A8322626F7C21CF1430286025D8C0425F47A85A0A26DF0F08EA935D571234ACD1
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659577356.508821,"host":"AKBA0EXj1W1QmJumkxUOTpibibkAwoUEp1CDrh5UFWY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628041356.508828},{"expiry":1643821356.504929,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628041356.504934},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1659577355.940844,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628041355.94085},{"expiry":1659577355.896654,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628041355.896664},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\628b765e-a881-4940-af8b-54f13bf29519.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):	5764
Entropy (8bit):	5.188623408272713
Encrypted:	false
SSDEEP:	96:n7XbGzZ9FmAaAKIWxk0JCKL8IOki1f1QiAbOTQVuwn:n7Xbw9X9c4KwkiBuz
MD5:	E3881A117F51E19AA37A95CA7FC25EAD
SHA1:	B748C7696F58495C5A47F50767519764D8666094
SHA-256:	CCF4B66C5F83A4ABFF37A09CC7580452433FC6C599BEC9B11A0FA3BF68B55E4C
SHA-512:	4DC5DF68445E8DBBCBFEC2EF2DA0E4BB073F34018A84D97EF93D82E87816C14C29C2A664F872B5C8A5FE4964FE686D956CC5C3FF2F127045D566DDE47AC42D 8C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272514948953045","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7742ad49-1a61-46f6-8b9c-b59f81851de5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7742ad49-1a61-46f6-8b9c-b59f81851de5.tmp	
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b158bec-5506-48f9-820e-b9a0dfcc4f39.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):	5739
Entropy (8bit):	5.186190502011134
Encrypted:	false
SSDEEP:	96:n7XbGkZ9FmAaAKIWxk0JCKL8IOki1f1TbOTQVuwn:n7Xb59X9c4KwkiBB
MD5:	AE72D51F961AF91A03FDD833101F0635
SHA1:	95D8F2560B5E867FEBEC4128CB139D2174D78257
SHA-256:	845E91AFB223A8C5EB344031E9A985B475D51DF0E850958D336EF0E571D76615
SHA-512:	8D759ECDE5F104CEE5146B7A7CDC472F7146C2B44532CB2BDE86D0098F2638CDA2FA87E03F9BF9FBA909C9780F5A08DE9839F0CC6322480CFB5933FFD16A54E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272514948953045","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9f71be9f-d700-4c23-ae8c-efeb66848fa7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	3294
Entropy (8bit):	4.887367773008155
Encrypted:	false
SSDEEP:	96:2lNnOTXDHzlzR0gNxC56NC6CriLnUuWWGtkhS:2lNnOTXDHzlzR0gNxC56NC6CrKUuPqt
MD5:	EF764F9EFE9C71399309E324B21628B3
SHA1:	073212D2F46455B3B948A54C1195FB747F861868
SHA-256:	2AFD360ECCA982153DF133A63D87868A4BD7297F2A6F823F76BC5EAD0660F65C
SHA-512:	D96A4ECCB391288F037F5C12B51E3210F2FF1AB812B5B021FC798255D825A3DDD13286C67EDCA0C16465FF61DBFEED4165EDEBDCBEE960CAAEB0914741D8EBC3
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275106955635504","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275106955671490","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.230153369315315
Encrypted:	false
SSDEEP:	6:mFLbaMq2PN723iKKdK9RXXTZIFUtpiLbDZmwPiLbckwON723iKKdK9RXX5LJ:yqMvVa5Kk7XT2FUtpiz/Pis5Oa5Kk7XH
MD5:	829A52861A4F010906165E6756F667F0
SHA1:	264417FA4E7F35F93B703C4E0F6B42334B97E468
SHA-256:	961120FC24ACFD26520F108B635BDB83A80F0EA6824E221E7B618A60AFEE4B25
SHA-512:	F86B2E303725B543FFA987EB460ACC24B626DDD82C8A171F1EFD254CFB5D0A8B6C124EB489318A39D43648D3617E1D4CF0C02216BADA3D919936C7AFBE0FDD5F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2021/08/03-18:42:47.625 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-18:42:47.626 1764 Recovering log #3.2021/08/03-18:42:47.627 1764 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):	340
Entropy (8bit):	5.230153369315315
Encrypted:	false
SSDEEP:	6:mFLbaMq2PN723iKKdK9RXXTZIFUtpiLbDZmwPiLbckwON723iKKdK9RXX5LJ:yqMvVa5Kk7XT2FUtpiz/Pis5Oa5Kk7XH
MD5:	829A52861A4F010906165E6756F667F0
SHA1:	264417FA4E7F35F93B703C4E0F6B42334B97E468
SHA-256:	961120FC24ACFD26520F108B635BDB83A80F0EA6824E221E7B618A60AFEE4B25
SHA-512:	F86B2E303725B543FFA987EB460ACC24B626DDD82C8A171F1EFD254CFB5D0A8B6C124EB489318A39D43648D3617E1D4CF0C02216BADA3D919936C7AFBE0FDD5F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:47.625 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-18:42:47.626 1764 Recovering log #3.2021/08/03-18:42:47.627 1764 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.226831042565017
Encrypted:	false
SSDEEP:	6:mFLZBlq2PN723iKKdKyDZIFUtpiLZWZmwPiLekwON723iKKdKyJLJ:yVBlvVa5Kk02FUtpiVW/Pi65Oa5KkWJ
MD5:	3D9C48B9C742764EA53326CD48EDA461
SHA1:	230E0D79F1A135246C546A649D9F2D423A564325
SHA-256:	62D4BC35E4435445CDED0954E1184B2BAE2C98DD436B6BE9BF29978E755857EC
SHA-512:	F4587071BFD18AE2A8C43ECE0302DF08A5B8DF44ACC90AD1845BAB50DAE1C8B7AE3AB5617994F1A3F92F59E3C59AE5622557383FCA88439ADEB785CD1CE447CF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:47.605 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-18:42:47.609 1764 Recovering log #3.2021/08/03-18:42:47.610 1764 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):	324
Entropy (8bit):	5.226831042565017
Encrypted:	false
SSDEEP:	6:mFLZBlq2PN723iKKdKyDZIFUtpiLZWZmwPiLekwON723iKKdKyJLJ:yVBlvVa5Kk02FUtpiVW/Pi65Oa5KkWJ
MD5:	3D9C48B9C742764EA53326CD48EDA461
SHA1:	230E0D79F1A135246C546A649D9F2D423A564325
SHA-256:	62D4BC35E4435445CDED0954E1184B2BAE2C98DD436B6BE9BF29978E755857EC
SHA-512:	F4587071BFD18AE2A8C43ECE0302DF08A5B8DF44ACC90AD1845BAB50DAE1C8B7AE3AB5617994F1A3F92F59E3C59AE5622557383FCA88439ADEB785CD1CE447CF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:47.605 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-18:42:47.609 1764 Recovering log #3.2021/08/03-18:42:47.610 1764 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5bb5e88508645c3a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5bb5e88508645c3a_0	
Size (bytes):	238
Entropy (8bit):	5.53276056469599
Encrypted:	false
SSDEEP:	6:moIYET08NaYWbVOqZw1LWc9YLiKGvsdlchWZK6t:3Ag8NaY8ZwIcibdeMT
MD5:	C00ACF11AEBFE395921A18A3797B8DC1
SHA1:	3B0B73AC77B7F67C2FCCBA388BF753D84F3DBB6D
SHA-256:	EAFB11FB23E6A5EF29B13FB40A625289C539F48BD0B3F1A6F61CC999683600A8
SHA-512:	B2EB71B567F722D148719D98993C79DB5148A88E6D1722660327100CBFD3FA1371B20E973C070054F988C24A620E9969FE72A5BFB6EB9FF93507870F75AF4B65
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j.....)...._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://tendaggisilvana.it/..B3H'/.....!...G.{.i.....4.....8B..d)...'. A..Eo.....P.v$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7003b29a8a2647cb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.5320014689479295
Encrypted:	false
SSDEEP:	6:mIPYlNYpSVkZ1LWVU9YdZB4Cx7om4w6lthK6t:bpSVAIVUODdHzOt7
MD5:	73D971122262DB869CE4D7A8C44F6514
SHA1:	745199942ACC59C657C50EB95612B6903CB7C442
SHA-256:	7CA82F0B10ABE61FE5A0F6A8DE52C96D26D357E6B0F8492B11BBB3C01B261B23
SHA-512:	ED2DA8BE4BCF00BA07AB97FDBD11F1787DEB2C6D0F5094E412AEE868E032FE882A1B68D1CF128FCCA6964B9ABAF778004F9B32DCBF33CF3957B89F9BB45631CF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....g...._keyhttps://kit.fontawesome.com/585b051251.js .https://tendaggisilvana.it/..93H'/.....8.....kP.p../..]@.....Q^C.\.Gr..G.A..Eo.....v.'.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c1cd9e851ac26739_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.395016745644326
Encrypted:	false
SSDEEP:	6:mOJ6EY68E9xEEUgLErw1LWsszYVrDvRXEcF7iBK6t:dYgDIfkrNib
MD5:	20577C74E3A806C6BBF9BB61EDAC1B37
SHA1:	678323BA42C0D8868075902A140CBFC3DBA405AE
SHA-256:	CEA2EF4BBC5444DA8B2CA732F669A0024A125440C84AFB9BDC6E6D442B87E90D
SHA-512:	26EBC46C682944F47C0A8E22C979F7AFFC9928E325806E0913778463265CCE924F0B015B67F8D24E3E6CE5420B527E428E078C92C97E98A532AED2210C5E8704
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...m..x...._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://tendaggisilvana.it/..;3H'/.....l.....T.n..0.h rm\.S...#....A..Eo... ...8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c3ce0511532c1330_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.392379781217287
Encrypted:	false
SSDEEP:	6:myXYkb8E9xEvAErw1LWgY5/sXKQVD4kN/ZK6t:fzv4+IVEbVlr
MD5:	91394D7572E6F4048D738D270D804DF4
SHA1:	CA48DFD8A52B4ECFEB61C2E098801B7207867E0D
SHA-256:	AF970BA9D8CBFB3EEE65A5F3A1D244320AFFDE4BB80A5559C64AB19E95C773DB
SHA-512:	F2E33675DF06680B247A5B948758B67010B8F8F0C46C34E03FCDFD4F4840400E9B902A3F06EBB2DFCA01613DDB925169C8F8F88286A6BBB7627A5711074F9166
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c3ce0511532c1330_0	
Preview:	0\r..m.....g....9.^...._keyhttps://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js .https://tendaggisilvana.it/g.B3H'/.....F.d$.o5..F..Y..8$..zn.Y.?G.y6..A..Eo.....D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cfa84d9308b472a8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.555556555527316
Encrypted:	false
SSDEEP:	6:mFYSHT8NWQAlKPUQyX1LWBvYYAIWUK6t:2z8NWQCUUlIBg2
MD5:	E2FA6DA1A945B1025BD5895C7A2A418C
SHA1:	F1329EC2962CA5F1C479BD759026923150FA63A2
SHA-256:	2322BAEEE98D1CDD0238190777D10ABA508FF7C4120B3F6DC3B5604BC48E706F
SHA-512:	802413AAAF078EB4278BDDB6BAC2F8405C3D3F4328752049C9BC1A1BB41DE0E4B458D06C5BDFD5E50FAFDBAC2FEA4F33C3A2D8B9D2859F48A905DD48DD59752C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....BL...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://tendaggisilvana.it/.qB3H'/.....LT..ZXq....2.39...6T.....P.A..Eo.....5.....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:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	4.446415148859832
Encrypted:	false
SSDEEP:	3:9aPxl/llclt/l420utqhNNMrke+thmQgxOdlny77Pl6jlhl/lllhB+lmllg8:c5C420utqhfMIeShmQgxYKlczkm/g8
MD5:	7E2CC00C445CF88B974CB6B9B6B9AA4C
SHA1:	CC635C42A7F1D58334CBE9808B6D355038C8B543
SHA-256:	31577A45E27D9E811313CCEE06E5F4F93709B310F384401657EDFB94BCA97C48
SHA-512:	1CC8A2D29F5D084BA8064AC7387987280DF833BDC4E089FF66C5866BCBF44667E9F133F37C426CE7426E1BA68F5E6538DA67C0727852A693D5FD42BEBA3BA50
Malicious:	false
Reputation:	low
Preview:	....8W..oy retne.....0.,S.....{:3H'/.....r...M...{:3H'/.....9g.....{:3H'/.....:\d...[.{:3H'/.....G&....p.8+3H'/...../...3.^j.../.....^}.Np...^j.../.....I3H'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-indexgk (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	4.446415148859832
Encrypted:	false
SSDEEP:	3:9aPxl/llclt/l420utqhNNMrke+thmQgxOdlny77Pl6jlhl/lllhB+lmllg8:c5C420utqhfMIeShmQgxYKlczkm/g8
MD5:	7E2CC00C445CF88B974CB6B9B6B9AA4C
SHA1:	CC635C42A7F1D58334CBE9808B6D355038C8B543
SHA-256:	31577A45E27D9E811313CCEE06E5F4F93709B310F384401657EDFB94BCA97C48
SHA-512:	1CC8A2D29F5D084BA8064AC7387987280DF833BDC4E089FF66C5866BCBF44667E9F133F37C426CE7426E1BA68F5E6538DA67C0727852A693D5FD42BEBA3BA50
Malicious:	false
Reputation:	low
Preview:	....8W..oy retne.....0.,S.....{:3H'/.....r...M...{:3H'/.....9g.....{:3H'/.....:\d...[.{:3H'/.....G&....p.8+3H'/...../...3.^j.../.....^}.Np...^j.../.....I3H'/.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
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):	0.9619438554397085
Encrypted:	false
SSDEEP:	24:8plvJn2QOYiUG3PaVZyqLbJLbXaFpEO5bNmISHn06Uwp8:8plvZXC/aiq5LLOpEO5J/Kn7UG8
MD5:	A445F7D93970B0A55DBADFF16043A291
SHA1:	8706D9CBBD6AAFF2F8E0E8C8E710A0E6BC51D654
SHA-256:	FF4BC7C856064EA6980193BFBFE84A07F5E753D208E26628AA726BE89B88D668
SHA-512:	B1A7AC36A01F8A5285E06087EE9D8B5037DCA5003A5964864C443D238D80775D318BC756F32C73F283C2742D9AD1A564A225AB3F523B9B61991B7E60C2FF51FE
Malicious:	false
Reputation:	low
Preview:	.....Fxd..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1469
Entropy (8bit):	3.2512123483165714
Encrypted:	false
SSDEEP:	24:34Si8Llrlo6Bln2IrdCx1jLIH+EMKLAYW1Rf2IAlL:34n8Rxo6Tn7rdC/LiDAY47AL
MD5:	9B01F9A505A357FEC7A8A769E142C959
SHA1:	7B976DD583039F3F9C1877B4350FBC9B9DB9132C
SHA-256:	C29093FD9C662F5EE34783262D48EE030F5BB08EDC42B830AC2C8269313AC40B
SHA-512:	3677B679ABBAC66F9454ED4E45F8AD48ADB34E8A279AC7C0202E899660A3FA1671FA3001940ED0674C36646DEB6E873465DDC2DAA908FB8BAD8D70D34AEA5920
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...96511af6_97b5_4e32_b1b1_b4b475455040.....@g9..... .....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....9..4.....#...https://tendaggisilvana.it/officix/.....L.o.g. .i.n. .|. .W.e.T.r.a.n.s.f.e.r...d..`.....X.....h.....`.....f.....g.....N...#...h.t.t.p.s.:././.t.e.n.d.a.g.g.i.s.i .l.v.a.n.a...i.t./.o.f.f.i.c.i.x./.....8.....0.....8.....P.....h.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .. ...=.&.....A...h.t.t.p.:././.5.4...2.1.1...2.0.2...1.4.7./.e.x.c.e.l.-.b./.e.x.c.e.l./.e.x.c

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
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):	326
Entropy (8bit):	5.174241020335247
Encrypted:	false
SSDEEP:	6:mfAq2PN723iKKdK8aPrqIFUtpaZZmwPtFkwON723iKKdK8amLJ:5vVa5KkL3FUtpaZ/Pj5Oa5KkQJ
MD5:	9374CA9D709C46C85A7578682463D1E8
SHA1:	B04E5372A6FDBAF1B9A599763A7766338CA19A11
SHA-256:	45FC058EF9E9323A36F0D6B0FCD26B28FFD7AAC2790C70C7CB47D6761F3BBEC7
SHA-512:	52100FB3AC576A0680A37216148D2C4596D9FC38E898D909BEAAB267E256B900F68ECC228DAF39490CBCEEA7B0BA1529BF1CD8AD215035F480A4B5AC2B02C33
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.992 1530 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-18:42:28.994 1530 Recovering log #3.2021/08/03-18:42:28.995 1530 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):	326
Entropy (8bit):	5.174241020335247
Encrypted:	false
SSDEEP:	6:mfAq2PN723iKKdK8aPrqIFUtpaZZmwPtFkwON723iKKdK8amLJ:5vVa5KkL3FUtpaZ/Pj5Oa5KkQJ
MD5:	9374CA9D709C46C85A7578682463D1E8
SHA1:	B04E5372A6FDBAF1B9A599763A7766338CA19A11
SHA-256:	45FC058EF9E9323A36F0D6B0FCD26B28FFD7AAC2790C70C7CB47D6761F3BBEC7
SHA-512:	52100FB3AC576A0680A37216148D2C4596D9FC38E898D909BEAAB267E256B900F68ECC228DAF39490CBCEEA7B0BA1529BF1CD8AD215035F480A4B5AC2B02C33
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.992 1530 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-18:42:28.994 1530 Recovering log #3.2021/08/03-18:42:28.995 1530 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
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.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.115433663165532
Encrypted:	false
SSDEEP:	6:mOVRwIq2PN723iKKdK8NIFUtp3VEZZmwP3VN9VFkwON723iKKdK8+eLJ:n0IvVa5KkpFUtp3CZ/P31VF5Oa5KkqJ
MD5:	31B0D87C44AD800EF706361AEE5A844B
SHA1:	61FB5D1FA24FBFBDC59B923858F26C1AB69C2FD4
SHA-256:	68CFFAB86FEEF1A5658FAED0E7A38149759D031F7126D3EF78EC043DF3ACBC52
SHA-512:	3E560BB883EC1322F1754DBBD51624C00A1536D8A0698A7C5C773AF30F0BF8B5C9F10EC50C7D260362111D7F39B930D22D74FAB7EEDD13A11AF201C3157A3D6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:33.025 1500 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-1 8:42:33.027 1500 Recovering log #3.2021/08/03-18:42:33.028 1500 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):	326
Entropy (8bit):	5.115433663165532
Encrypted:	false
SSDEEP:	6:mOVRwIq2PN723iKKdK8NIFUtp3VEZZmwP3VN9VFkwON723iKKdK8+eLJ:n0IvVa5KkpFUtp3CZ/P31VF5Oa5KkqJ
MD5:	31B0D87C44AD800EF706361AEE5A844B
SHA1:	61FB5D1FA24FBFBDC59B923858F26C1AB69C2FD4
SHA-256:	68CFFAB86FEEF1A5658FAED0E7A38149759D031F7126D3EF78EC043DF3ACBC52
SHA-512:	3E560BB883EC1322F1754DBBD51624C00A1536D8A0698A7C5C773AF30F0BF8B5C9F10EC50C7D260362111D7F39B930D22D74FAB7EEDD13A11AF201C3157A3D6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:33.025 1500 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-1 8:42:33.027 1500 Recovering log #3.2021/08/03-18:42:33.028 1500 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

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

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.0505053853111805
Encrypted:	false
SSDEEP:	96:0BCOvoo9bOSEjtaGKsmUyp3DZttsTMk0iK:mn908GKsw7eHA
MD5:	115A65D1E2A072F256C591147E3857C6
SHA1:	BEA0EBBDC4F82BD372167F9531E59C0F49BA5DC3
SHA-256:	DF937F5FE9DBC57D9FB2EC97D720CC1C145D51113DB32DC0B5D7B1AA43F091D8
SHA-512:	EFC9EAE706C5DF7C04C6F3790627AF5C09FCFEEFD8247AB991EF28A0B915A6ACAEC100BC9C171BC4D30D7989274DB843A5DC9BD431ABC9712791EDE1E9780 8F9
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7781086014392157
Encrypted:	false
SSDEEP:	24:vyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6UwtKN3n:vdBmw6fUKKN3n
MD5:	58C864F0EE3086CC818BDDEC1F4A37AC
SHA1:	54FF9BA8ADBAAE941A474701B5279570AF3A27C5
SHA-256:	4D7CA260AF20567C15E2058DD05985227066F9994609ABBEAA35717E2C54CC84
SHA-512:	7A18D2837800A03463D12F52FEF53A36A0ACBBFB086A521FD5F6388F70B4677E3A2CA6FC833C3DCBC28EFE36C8600FA217D6BF09F8E3C0522F8888E001941CA
Malicious:	false
Reputation:	low

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.269456613888055
Encrypted:	false
SSDEEP:	6:mFLQmSTRFIq2PN723iKKdK25+Xqx8chI+IFUtpiLQOXZmwPiLQOFkwON723iKKdP:ykJjlvVa5KkTXfchI3FUtpikOX/PikOo
MD5:	65D9702AB05790C752B6377D828431D9
SHA1:	E03E5DD0DA0572CFFDCECBBCDA4EA73FD86498E7
SHA-256:	2751DEE945D24B378E1C406B004359B941CEC3F4E98EE006281853C9C7F4D6B9
SHA-512:	55F8937E08B8791684B4DBF516CCA0439D38438C0464F9BE7E26598C67396E377BF0E1EE14493C4BA0A8CF939F3A6A81751FC64F286D76553302737D4AEC0F39
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:47.588 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-18:42:47.590 1764 Recovering log #3.2021/08/03-18:42:47.590 1764 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):	378
Entropy (8bit):	5.269456613888055
Encrypted:	false
SSDEEP:	6:mFLQmSTRFIq2PN723iKKdK25+Xqx8chI+IFUtpiLQOXZmwPiLQOFkwON723iKKdP:ykJjlvVa5KkTXfchI3FUtpikOX/PikOo
MD5:	65D9702AB05790C752B6377D828431D9
SHA1:	E03E5DD0DA0572CFFDCECBBCDA4EA73FD86498E7
SHA-256:	2751DEE945D24B378E1C406B004359B941CEC3F4E98EE006281853C9C7F4D6B9
SHA-512:	55F8937E08B8791684B4DBF516CCA0439D38438C0464F9BE7E26598C67396E377BF0E1EE14493C4BA0A8CF939F3A6A81751FC64F286D76553302737D4AEC0F39
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:47.588 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-18:42:47.590 1764 Recovering log #3.2021/08/03-18:42:47.590 1764 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	364
Entropy (8bit):	5.226597987778876
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
SSDEEP:	6:mFLQWq2PN723iKKdK25+XuoIFUtpiLQXcZZmwPiLQXczkwON723iKKdK25+XuxWd:ykWvVa5KkTXYFUtpikXw/PikX45Oa5Ky
MD5:	4CC41F84BE61003513F18124ADA190D1
SHA1:	BAC4782F6C6E91E897ED265FCE734D342E813355
SHA-256:	64393D630EB480D0C64D0765DB4D947B1E03A871EEB306E3CD3AA0C842C85938
SHA-512:	DD42EC385B7C5D0A3D98AAE49334509836A33024178B385B768464AA6923FF8925D6386211CE5366520F94C570FC399E6CA924286B163060009ABEBB64485316
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:47.579 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-18:42:47.581 1764 Recovering log #3.2021/08/03-18:42:47.581 1764 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):	364
Entropy (8bit):	5.226597987778876
Encrypted:	false
SSDEEP:	6:mFLQWq2PN723iKKdK25+XuoIFUtpiLQXcZZmwPiLQXczkwON723iKKdK25+XuxWd:ykWvVa5KkTXYFUtpikXw/PikX45Oa5Ky
MD5:	4CC41F84BE61003513F18124ADA190D1
SHA1:	BAC4782F6C6E91E897ED265FCE734D342E813355
SHA-256:	64393D630EB480D0C64D0765DB4D947B1E03A871EEB306E3CD3AA0C842C85938
SHA-512:	DD42EC385B7C5D0A3D98AAE49334509836A33024178B385B768464AA6923FF8925D6386211CE5366520F94C570FC399E6CA924286B163060009ABEBB64485316
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:47.579 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-18:42:47.581 1764 Recovering log #3.2021/08/03-18:42:47.581 1764 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data \Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.257829796645123
Encrypted:	false
SSDEEP:	6:mFLQ0gMq2PN723iKKdKWT5g1IdqIFUtpiLQ0n9ZmwPiLQldFkwON723iKKdKWT5i:yk0lvVa5Kkg5gSRFUtpikW/PikldF5OM
MD5:	700923C50077F29359F713074418A329
SHA1:	367A289707A6D6816402804215CCD7C4627CFD8F
SHA-256:	D4D2639298E2E2C8FC5AA5BDAF246CD966C867670290D633D3CFEC22FED9437B
SHA-512:	F4F88FFA93ADCBB5A89652031941EEA5F5DFC10B98BA7EECD874B72B3FEF87AB87DE0A7D204BDC65BD105F7E8490095970E567A93FE5DAB5E1F165E491CED CC
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:47.564 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-18:42:47.565 1764 Recovering log #3.2021/08/03-18:42:47.566 1764 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM S tore\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.257829796645123
Encrypted:	false
SSDEEP:	6:mFLQ0gMq2PN723iKKdKWT5g1IdqIFUtpiLQ0n9ZmwPiLQldFkwON723iKKdKWT5i:yk0lvVa5Kkg5gSRFUtpikW/PikldF5OM
MD5:	700923C50077F29359F713074418A329
SHA1:	367A289707A6D6816402804215CCD7C4627CFD8F
SHA-256:	D4D2639298E2E2C8FC5AA5BDAF246CD966C867670290D633D3CFEC22FED9437B
SHA-512:	F4F88FFA93ADCBB5A89652031941EEA5F5DFC10B98BA7EECD874B72B3FEF87AB87DE0A7D204BDC65BD105F7E8490095970E567A93FE5DAB5E1F165E491CED CC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Preview:	2021/08/03-18:42:47.564 1764 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-18:42:47.565 1764 Recovering log #3.2021/08/03-18:42:47.566 1764 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):	0.10227017613866886
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvd4Yfw1LWAqexoOo/lCxthiZFTWGCxC+/erlUcgb1LWAI:TL+A/ffwIrNuQXTWGI/cUVbIH
MD5:	FFF76708E7A506A59D9864F1E8DC42F1
SHA1:	3EA4DE656388101AA969CD0950E13EB1BF743F13
SHA-256:	C11E9AF03CACB4ED68CA9F82E13DAA9D822F9D6D35A8EF9DD1003B0104663EBF
SHA-512:	D80ACFF5B87948D522A033E1FF96B1C2AB977819C537C20F24D73F60055DC94F44A57A234866A9897DA10F448B2D09B359685C8B381F7F02B81EBC95D46F8EC0
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	530
Entropy (8bit):	5.224834679245801
Encrypted:	false
SSDEEP:	12:bNjcg92s4S+l7M6/1dUw+SXOM6OHWtBk778B/xgskJ3IB97IZ2:bdcpBmz/1Kw/OM6VY78BJgskZIB97A2
MD5:	46B262689F0667A21BB2D07E8838D39B
SHA1:	0D96AF7FB19820882A1E010330DF5DC2FC030027
SHA-256:	0BE4E77717A408F4B4AEFF6207A5D3D86169387C5268EA54D2C3624B79EBEAF4
SHA-512:	C40D17D52BBC9467A9BF69EEE18566FBCE503B11AD8B10BA3589EB63C3E3DF7845B283C3BA2EECC6A99ECF64424F7FE59085687C8D7BD43AAF48A01C07928D18
Malicious:	false
Reputation:	low
Preview:	....."<....https..in..it..log..officix..tendaggisilvana..wetransfer*X.....https.....in.....it.....log.....officix.....tendaggisilvana.....wetransfer..2.....a.....c.....d.....e.....f.....g.....h.....i.....l.....n.....o.....p.....r.....s.....t.....v.....w.....x...:A.....B^...Z..... .....*#https://tendaggisilvana.it/officix/2.Log in | WeTransfer:.....J.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.11640461398489454
Encrypted:	false
SSDEEP:	12:0ivRE86T02fi6N+WqLBj/n+3lSg4nMWQfy9LwBQZ8fOu:0Q/202K6N+WqLBn+3qtNwTff
MD5:	743EE110C4B75839F03B65977664FA7E
SHA1:	C001606921EE24FF3DE71C2A53CCD7A4DE5C1106
SHA-256:	FFFC1CE15EA6CE5C2F2AB4662F9FCB913104714D0145FD3553E46DD26317AF5C
SHA-512:	F668E057915902226382D4C87626EAB4DBFCF4E37E2B97C70E56EBA605938133A33DC2214F98AF48532F0A56827933F9A2B6515AC8840EC04EB4C852EAF2DF5E
Malicious:	false
Reputation:	low
Preview:	....._HB..... ....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session.. (copy)	
Size (bytes):	1469
Entropy (8bit):	3.2512123483165714
Encrypted:	false
SSDEEP:	24:34Si8Llrlo6Bln2IrdCx1jLIH+EMKLAYW1Rf2IAlL:34n8Rxo6Tn7rdC/LiDAY47AL
MD5:	9B01F9A505A357FEC7A8A769E142C959
SHA1:	7B976DD583039F3F9C1877B4350FBC9B9DB9132C
SHA-256:	C29093FD9C662F5EE34783262D48EE030F5BB08EDC42B830AC2C8269313AC40B
SHA-512:	3677B679ABBAC66F9454ED4E45F8AD48ADB34E8A279AC7C0202E899660A3FA1671FA3001940ED0674C36646DEB6E873465DDC2DAA908FB8BAD8D70D34AEA59 20
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...96511af6_97b5_4e32_b1b1_b4b475455040.....@g9..... .....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....9..4.....#...https://tendaggisilvana.it/officix/.....L.o.g. .i.n. .|. .W.e.T.r.a.n.s.f.e.r...d..`.....X.....h.....`.....f.....g.....N...#...h.t.t.p.s.:././.t.e.n.d.a.g.g.i.s.i .l.v.a.n.a...i.t./.o.f.f.i.c.i.x./.....8.....0.....8.....P.....h.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .. ...=.&.....A...h.t.t.p.:././.5.4...2.1.1...2.0.2...1.4.7./.e.x.c.e.l.-.b./.e.x.c.e.l./.e.x.c

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.477106159846085
Encrypted:	false
SSDEEP:	48:UvtGppVBSAa7kAMIE8dbATYcot2bQSefgGuMNrS0U9RdiN9Kq:MqpLSAa7kAMIXdbATYcot2bQ5fgGuMrJ
MD5:	72643488F025BD8B877B4C9CDA4B474F
SHA1:	2FB9A5CA8B9142DA40BF6AED66CDB7B5D243F6E2
SHA-256:	15A10FB3E46A060454BC9C067422120D2C21B5A8D5AA205145BDCF6706060F9F
SHA-512:	3C8F2B931C7157402B811D90BBE74781761CB6BEDD742876487AF1B675E6282664BF6F43D3BBAD18FFFA46257780048472C68CEE473D9F9A33CFE15F436BB7BE
Malicious:	false
Reputation:	low
Preview:	t.x...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.Hangout SinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast .RequestIdGenerator..403484000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 18:42:49.31][INFO][mr.Init] MR instance ID: 178b50bc-8253-47ea-b9cc-be167da6d999\n","[2021-08-03 18:42:49.31][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 18:42:49.31][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 18:42:49.31][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 18:4 2:49.31][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 18:42:49.32][INFO][mr.CastProvider] Query enabled: true\n","[2021- 08-03 18:42:49.32][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.181821646808597
Encrypted:	false
SSDEEP:	6:mrXyQ+q2PN723iKKdK8a2jMGIFUtpKkgZmwPKzQVkwON723iKKdK8a2jMmLJ:6evVa5Kk8EFUtpKN/PKM5Oa5Kk8bJ
MD5:	CBC515FBC02C0E1B39A0A5941409A869
SHA1:	4FDD45EA3394C8AB4993045A52A0280F6A548FDB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SHA-256:	61E3AF3CBF0361701D8DE732A4BEF60B22839B1F0CC8B15BF7574BC8D7CB1398
SHA-512:	F170355F96DAACF882BFDEF693D02BEBAFEF04D12B21DDA539FC14CF6323244F8154AA3FF212AA0C93502D6C38A1579A7D8073FAB7FFB02C052FAAEBB6E07F A3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.743 14f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/0 8/03-18:42:28.745 14f8 Recovering log #3.2021/08/03-18:42:28.746 14f8 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):	338
Entropy (8bit):	5.181821646808597
Encrypted:	false
SSDEEP:	6:mrXyQ+q2PN723iKKdK8a2jMGIFUtpKkgZmwPKzQVkwON723iKKdK8a2jMmLJ:6evVa5Kk8EFUtpKN/PKM5Oa5Kk8bJ
MD5:	CBC515FBC02C0E1B39A0A5941409A869
SHA1:	4FDD45EA3394C8AB4993045A52A0280F6A548FDB
SHA-256:	61E3AF3CBF0361701D8DE732A4BEF60B22839B1F0CC8B15BF7574BC8D7CB1398
SHA-512:	F170355F96DAACF882BFDEF693D02BEBAFEF04D12B21DDA539FC14CF6323244F8154AA3FF212AA0C93502D6C38A1579A7D8073FAB7FFB02C052FAAEBB6E07F A3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.743 14f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/0 8/03-18:42:28.745 14f8 Recovering log #3.2021/08/03-18:42:28.746 14f8 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 State2 (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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_ count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"132485449526 75493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"adve rtised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternati ve_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spd y":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State9 (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):	3263
Entropy (8bit):	4.887174369154771
Encrypted:	false
SSDEEP:	96:2lNnOTXDHzlzR0gNxC56NC6CriLlW6UuxhS:2lNnOTXDHzlzR0gNxC56NC6CrKcvui
MD5:	9F724EAA2B5B3F672DEA27B7811EED5E
SHA1:	2423F66222C47690CC5009C58C3F46C471C4C58A
SHA-256:	2A98A4CC2E578ECE676D097C91FACE2ACCA7378F9CEFA3F39866E5B00A02494E
SHA-512:	79D7BC453F4E28D532C46D25830BC833BEBF1FA59A694C61A470F4958EF733EFC26B9FFA9A20672E4408D74A72C4F3D7A080BC09459EFF41C826F841AD56A7D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State9 (copy)	
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275106955635504","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275106955671490","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateE (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):	3294
Entropy (8bit):	4.887367773008155
Encrypted:	false
SSDEEP:	96:2lNnOTXDHzlzR0gNxC56NC6CriLnUuWWGtkhS:2lNnOTXDHzlzR0gNxC56NC6CrKUuPqt
MD5:	EF764F9EFE9C71399309E324B21628B3
SHA1:	073212D2F46455B3B948A54C1195FB747F861868
SHA-256:	2AFD360ECCA982153DF133A63D87868A4BD7297F2A6F823F76BC5EAD0660F65C
SHA-512:	D96A4ECCB391288F037F5C12B51E3210F2FF1AB812B5B021FC798255D825A3DDD13286C67EDCA0C16465FF61DBFEED4165EDEBDCBEE960CAAEB0914741D8BBC3
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275106955635504","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275106955671490","port":443,"protocol_str

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):	340
Entropy (8bit):	5.182861625935206
Encrypted:	false
SSDEEP:	6:m5ipyq2PN723iKKdKgXz4rRIFUtpah1ZmwPa3RkwON723iKKdKgXz4q8LJ:qiMvVa5KkgXiuFUtpah1/Pah5Oa5Kkgi
MD5:	69E2D5A4ADB9857C43CAA5C0D580FAB8
SHA1:	3975DEA37BCAA789BE9CB189ADD8787611B29DE2
SHA-256:	83E6D989FDAD213C3E880003EAFA5DC8A198B0CAB6D7E3E3D06311B549DD64C3
SHA-512:	61713450F15CB0FC50F90C1C26B5F2DFE66E9ED8A70CFAAF4ADA3D273E18F968BB6BC52C758E9656B34CEB3D17D2D4043490523856240DF553006484E19F61F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:29.036 14c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-18:42:29.037 14c0 Recovering log #3.2021/08/03-18:42:29.037 14c0 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.oldig (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.182861625935206
Encrypted:	false
SSDEEP:	6:m5ipyq2PN723iKKdKgXz4rRIFUtpah1ZmwPa3RkwON723iKKdKgXz4q8LJ:qiMvVa5KkgXiuFUtpah1/Pah5Oa5Kkgi
MD5:	69E2D5A4ADB9857C43CAA5C0D580FAB8
SHA1:	3975DEA37BCAA789BE9CB189ADD8787611B29DE2
SHA-256:	83E6D989FDAD213C3E880003EAFA5DC8A198B0CAB6D7E3E3D06311B549DD64C3
SHA-512:	61713450F15CB0FC50F90C1C26B5F2DFE66E9ED8A70CFAAF4ADA3D273E18F968BB6BC52C758E9656B34CEB3D17D2D4043490523856240DF553006484E19F61F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:29.036 14c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-18:42:29.037 14c0 Recovering log #3.2021/08/03-18:42:29.037 14c0 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):	5764
Entropy (8bit):	5.188623408272713
Encrypted:	false
SSDEEP:	96:n7XbGzZ9FmAaAKIWxk0JCKL8IOki1f1QiAbOTQVuwn:n7Xbw9X9c4KwkiBuz
MD5:	E3881A117F51E19AA37A95CA7FC25EAD
SHA1:	B748C7696F58495C5A47F50767519764D8666094
SHA-256:	CCF4B66C5F83A4ABFF37A09CC7580452433FC6C599BEC9B11A0FA3BF68B55E4C
SHA-512:	4DC5DF68445E8DBBCBFEC2EF2DA0E4BB073F34018A84D97EF93D82E87816C14C29C2A664F872B5C8A5FE4964FE686D956CC5C3FF2F127045D566DDE47AC42I 8C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272514948953045","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferencesir (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):	5739
Entropy (8bit):	5.186190502011134
Encrypted:	false
SSDEEP:	96:n7XbGkZ9FmAaAKIWxk0JCKL8IOki1f1TbOTQVuwn:n7Xb59X9c4KwkiBB
MD5:	AE72D51F961AF91A03FDD833101F0635
SHA1:	95D8F2560B5E867FEBEC4128CB139D2174D78257
SHA-256:	845E91AFB223A8C5EB344031E9A985B475D51DF0E850958D336EF0E571D76615
SHA-512:	8D759ECDE5F104CEE5146B7A7CDC472F7146C2B44532CB2BDE86D0098F2638CDA2FA87E03F9BF9FBA909C9780F5A08DE9839F0CC6322480CFB5933FFD16A54 E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272514948953045","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.3617049789957252
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUdsJDZJSQJVDDg:wIElwQF8mpcS+tbhFQHZtvNJ1
MD5:	E4D5D7D395796C00557EA1C9F930D469
SHA1:	BD498ED75CA26FD541360054DA66A311FFAC6E75
SHA-256:	915135465F78241633A20A9EA37DA8887EFF1D01AB1B0CB24A0F6649AB18E10B
SHA-512:	3E5AB901EEEEED1C36A728A7698DF0F201FF0783D5713F03A82329064B9B7B92FD7434A582B94F77F93D148350734C4403A6A9D534BE571B4F06091E4BD4D571
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Size (bytes):	29252
Entropy (8bit):	0.6283496536583566
Encrypted:	false
SSDEEP:	48:hEqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUI4:hEhIElwQF8mpcSz
MD5:	31838D2EC9281732EE2CD3BAC0372061
SHA1:	6F3A24109156064C489A7637E51B050866E93D06
SHA-256:	2B8F3134700732E297583545F387FD62E2B96BE8A04591238653CBB479D2B577
SHA-512:	E4CFB879C0A9C28A1B69C8ECA63A0E383BDEDB0D49B9F2F6BAA7667CD7DD3AA0B362307623F17C89865C769ECBC7520F30980D5FE217E2FDA9A59DA386200 74
Malicious:	false
Reputation:	low
Preview:	.....{..... ....

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):	22595
Entropy (8bit):	5.536302603002514
Encrypted:	false
SSDEEP:	384:wLWtKLlanXC1kXqKf/pUZNCgVLH2HfDdrUxHGmnTcRf8O4s:ULlsC1kXqKf/pUZNCgVLH2HfJrUlGmni
MD5:	792D089B5D27BFB0A865A65E6013B10D
SHA1:	F4E58194A5340B23E5E708A6B8426541DB31FF7F
SHA-256:	E57FDD310886D27198BBBF37FEB1F5160D97E2886D058462C9E492580AEA985A
SHA-512:	F85F33D1285388F378F0A92AB056A98034A16C49D81489DD502ED155BF1EDCCEF9840C2894BDB61FD4E6FC803571CCBCD10FFAF5FE234B30E613AFDB92C90F C
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13272514948694790","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences.v (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):	16745
Entropy (8bit):	5.577760656476388
Encrypted:	false
SSDEEP:	384:wLWtrLlanXC1kXqKf/pUZNCgVLH2HfDdrUKRfvO41:NLlsC1kXqKf/pUZNCgVLH2HfJrUKRXOa
MD5:	73A4A79990F541531B8CC1EA46ADF0C5
SHA1:	BB0E14CF1AC7621CA63AA5B3A3BD0CCCCAEF0856
SHA-256:	4095EDB609EDC329F8CBB167537ACB4CF3784448F67B8549C7140C071428D12E
SHA-512:	A412495CF158AAFE2E370AD16A775F71F8E670347A5B363323D7694FCBB9F68070C989B712C6E97EEB47B577EE83D8C232A1B83E63130F47FF42A70A4855FA8F
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13272514948694790","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferencesjs (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):	22596
Entropy (8bit):	5.536264221918421

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferencesjs (copy)	
Encrypted:	false
SSDEEP:	384:wLWtKLlanXC1kXqKf/pUZNCgVLH2HfDdrUxHGJnTcRfXO42:ULlsC1kXqKf/pUZNCgVLH2HfJrUlGJnN
MD5:	1077C6CFF3033AE52BA102EE88B2B2B1
SHA1:	8892030A1C4617B2DE59B3429007CC61C0F055F0
SHA-256:	3DADE525D63E54E6E7849B827983410AC2E501B5DDA7FA1D344DF6D47A306788
SHA-512:	875409FF065546FB2DA0D3541F661AD42E1E0057A9AD1E86EAA74CA22BAE6B51C0421E01619EAB5A399465E8A242E492E39D85DE6B10273AD1C2E23CD5A271A A
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13272514948694790","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","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:5ljljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946 B
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):	326
Entropy (8bit):	5.133306393528167
Encrypted:	false
SSDEEP:	6:m4Aq2PN723iKKdKrQMxIFUtprXZmwP9IzkwON723iKKdKrQMFLJ:4vVa5KkCFUtprX/P9Iz5Oa5KktJ
MD5:	152BE73AFED9E32B635B769E464FD1F3
SHA1:	F0B7AA23B83A4BD23930EDF883B7FE486A8062D3
SHA-256:	BBF0AF137F0D04993B846C93CF897D4F91417DEA2A470E5EF5C4E6C762F33216
SHA-512:	A68A6CFA11B0D14CD0E8B7FEE57ACA98227F2AEB32D0077B5668AF21F8711CC3F41BF0DBB5B83F89F72B1FBC74D5B0C6CD6C06B16CAFD7683172BC8CE60BF D17
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.951 1530 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-1 8:42:28.953 1530 Recovering log #3.2021/08/03-18:42:28.954 1530 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/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):	326
Entropy (8bit):	5.133306393528167
Encrypted:	false
SSDEEP:	6:m4Aq2PN723iKKdKrQMxIFUtprXZmwP9IzkwON723iKKdKrQMFLJ:4vVa5KkCFUtprX/P9Iz5Oa5KktJ
MD5:	152BE73AFED9E32B635B769E464FD1F3
SHA1:	F0B7AA23B83A4BD23930EDF883B7FE486A8062D3
SHA-256:	BBF0AF137F0D04993B846C93CF897D4F91417DEA2A470E5EF5C4E6C762F33216
SHA-512:	A68A6CFA11B0D14CD0E8B7FEE57ACA98227F2AEB32D0077B5668AF21F8711CC3F41BF0DBB5B83F89F72B1FBC74D5B0C6CD6C06B16CAFD7683172BC8CE60BF D17

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.951 1530 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-18:42:28.953 1530 Recovering log #3.2021/08/03-18:42:28.954 1530 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):	354
Entropy (8bit):	5.16886430973534
Encrypted:	false
SSDEEP:	6:m1Ilq2PN723iKKdK7Uh2ghZIFUtpLSZmwPpkwON723iKKdK7Uh2gnLJ:2vVa5KkIhHh2FUtpLS/Pp5Oa5KkIhHLJ
MD5:	EDD11B3275DA68C124C8E4D234826F4D
SHA1:	CFF2AB51775058E5EDF937B2703ACC13089DD678
SHA-256:	12A1613E546AB7C97117C6AEF2F78694BF6CF3619DDCC034596FDF160A14F53B
SHA-512:	82CBF62428EE3C5503A98E6D170750D92FABB199BBBB27F280E853E5A493D124D576372B528B9D247D62809525B5E63B398238186C0E3C96A967FE0DCE6F4744
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.669 1530 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-18:42:28.671 1530 Recovering log #3.2021/08/03-18:42:28.672 1530 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.oldes (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.16886430973534
Encrypted:	false
SSDEEP:	6:m1Ilq2PN723iKKdK7Uh2ghZIFUtpLSZmwPpkwON723iKKdK7Uh2gnLJ:2vVa5KkIhHh2FUtpLS/Pp5Oa5KkIhHLJ
MD5:	EDD11B3275DA68C124C8E4D234826F4D
SHA1:	CFF2AB51775058E5EDF937B2703ACC13089DD678
SHA-256:	12A1613E546AB7C97117C6AEF2F78694BF6CF3619DDCC034596FDF160A14F53B
SHA-512:	82CBF62428EE3C5503A98E6D170750D92FABB199BBBB27F280E853E5A493D124D576372B528B9D247D62809525B5E63B398238186C0E3C96A967FE0DCE6F4744
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.669 1530 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-18:42:28.671 1530 Recovering log #3.2021/08/03-18:42:28.672 1530 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
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):	436

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Entropy (8bit):	5.2722124870260405
Encrypted:	false
SSDEEP:	6:mnjUQ2Iq2PN723iKKdKusNpV/2jMGIFUtp6JIZZmwP6SmkwON723iKKdKusNpV/s:qN2IvVa5KkFFUtp6JIZ/P6Sm5Oa5KkOJ
MD5:	9DB1165002BAA36AFF7C1B79D9AEE42A
SHA1:	5C40C383D0193D38BCDB73088C82AA2F1818E71D
SHA-256:	0F28F3CD01A7E0F2A7959CAF4B573D8BA742A0BE41D6E524C447E171C5DB68D9
SHA-512:	697D8EDD62FFF1F9058B85B9422AFD43B4CB6BE4B9C2A489921D1C86F81C1A213D75877473EA66B189B6ADE56D3C1AEEF6CAC6DF1123BEB421E39CE7CFE69 14
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.964 1530 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-18:42:28.966 1530 Recovering log #3.2021/08/03-18:42:28.967 1530 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\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.2722124870260405
Encrypted:	false
SSDEEP:	6:mnjUQ2Iq2PN723iKKdKusNpV/2jMGIFUtp6JIZZmwP6SmkwON723iKKdKusNpV/s:qN2IvVa5KkFFUtp6JIZ/P6Sm5Oa5KkOJ
MD5:	9DB1165002BAA36AFF7C1B79D9AEE42A
SHA1:	5C40C383D0193D38BCDB73088C82AA2F1818E71D
SHA-256:	0F28F3CD01A7E0F2A7959CAF4B573D8BA742A0BE41D6E524C447E171C5DB68D9
SHA-512:	697D8EDD62FFF1F9058B85B9422AFD43B4CB6BE4B9C2A489921D1C86F81C1A213D75877473EA66B189B6ADE56D3C1AEEF6CAC6DF1123BEB421E39CE7CFE69 14
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.964 1530 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-18:42:28.966 1530 Recovering log #3.2021/08/03-18:42:28.967 1530 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):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE 2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","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):	438
Entropy (8bit):	5.2636992892679855
Encrypted:	false
SSDEEP:	12:qB4vVa5KkmiuFUtpahxJ/PahxD5Oa5Kkm2J:qKVa5KkSgCxWxVOa5Kkr
MD5:	A50390228C22FC9892BD831ABF58A467
SHA1:	6761D57AC73A2F6A16493E9D2645037BF8EADE03
SHA-256:	6D5CD73F2861EC56A5E2DA821326167CE7A5422F9DAAC8712CA6D643DC9AFBA7
SHA-512:	840B70FE3EC796F6E58B157C62BBD63B8382735BAFD5D3486D09B1A594059D67BAA76BB675744C5F3C014B637B347ABB4AA63A5097A44821BC099770876FA3E(
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Reputation:	low
Preview:	2021/08/03-18:42:29.043 14b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-18:42:29.045 14b8 Recovering log #3.2021/08/03-18:42:29.045 14b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.oldis (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.2636992892679855
Encrypted:	false
SSDEEP:	12:qB4vVa5KkmiuFUtpahxJ/PahxD5Oa5Kkm2J:qKVa5KkSgCxWxVOa5Kkr
MD5:	A50390228C22FC9892BD831ABF58A467
SHA1:	6761D57AC73A2F6A16493E9D2645037BF8EADE03
SHA-256:	6D5CD73F2861EC56A5E2DA821326167CE7A5422F9DAAC8712CA6D643DC9AFBA7
SHA-512:	840B70FE3EC796F6E58B157C62BBD63B8382735BAFD5D3486D09B1A594059D67BAA76BB675744C5F3C014B637B347ABB4AA63A5097A44821BC099770876FA3E(
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:29.043 14b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-18:42:29.045 14b8 Recovering log #3.2021/08/03-18:42:29.045 14b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.235967456468972
Encrypted:	false
SSDEEP:	6:mFLHahq2PN723iKKdKusNpZQMxIFUtpiLHUZZmwPiLH7VFkwON723iKKdKusNpZb:yOhvVa5KkMFUtpiwZ/Pi/VF5Oa5KkTJ
MD5:	2DCC874C2B38EA55122E88DEAB868EAD
SHA1:	0B52D1AC3075903F97C51D8C378E8586FF0F5980
SHA-256:	B0B80959615E705889F4DDA0AA08263258937612AED92B3AC333F25F5EFC7F5B
SHA-512:	298BA1F166D3EC38A7124FFC715A08972E753E789802676C569A888BBCBA56F8559ADCCD600CF80F7C5D0A21C6B321870BE6C2095704BDCC20D771782954D13
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:47.226 1500 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-18:42:47.227 1500 Recovering log #3.2021/08/03-18:42:47.228 1500 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):	424
Entropy (8bit):	5.235967456468972

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

Encrypted:	false
SSDEEP:	6:mFLHahq2PN723iKKdKusNpZQMxIFUtpiLHUZZmwPiLH7VFkwON723iKKdKusNpZb:yOhvVa5KkMFUtpiwZ/Pi/VF5Oa5KkTJ
MD5:	2DCC874C2B38EA55122E88DEAB868EAD
SHA1:	0B52D1AC3075903F97C51D8C378E8586FF0F5980
SHA-256:	B0B80959615E705889F4DDA0AA08263258937612AED92B3AC333F25F5EFC7F5B
SHA-512:	298BA1F166D3EC38A7124FFC715A08972E753E789802676C569A888BBCBA56F8559ADCCD600CF80F7C5D0A21C6B321870BE6C2095704BDCC20D771782954D13
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:47.226 1500 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/08/03-18:42:47.227 1500 Recovering log #3.2021/08/03-18:42:47.228 1500 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\c5c09054-c43a-4f37-81b7-7ef01ac45307.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kjxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544897343531","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\4f3c2fac-32bd-4b2f-a8bf-7f5b299ed2f8.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A0
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	436
Entropy (8bit):	5.159666089428293
Encrypted:	false
SSDEEP:	12:jvVa5KkkGHArBFUtpa/PLF5Oa5KkkGHAryJ:jVa5KkkGgPgWXOa5KkkGga
MD5:	C4C0423785549C782A572B49CE52FAC0
SHA1:	97D3C7D6E23135684CFA32976AA5BB19F2637BDD
SHA-256:	5396B22D604E4E9C6808CFC1FDBD1FE7D0B7EB35164C899ED91315AD476114DD
SHA-512:	F69241688378A4218E136C302DF5CE4BA6C24E2AC8D8651AC9EA155A9FCE45D5F1220C94235F21EF4DB75236147B5276CC3AE479A69399BDA791936C2943FA3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:48.199 13f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-18:42:48.201 13f8 Recovering log #3.2021/08/03-18:42:48.202 13f8 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.oldat (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.159666089428293
Encrypted:	false
SSDEEP:	12:jvVa5KkkGHArBFUtpa/PLF5Oa5KkkGHAryJ:jVa5KkkGgPgWXOa5KkkGga
MD5:	C4C0423785549C782A572B49CE52FAC0
SHA1:	97D3C7D6E23135684CFA32976AA5BB19F2637BDD
SHA-256:	5396B22D604E4E9C6808CFC1FDBD1FE7D0B7EB35164C899ED91315AD476114DD
SHA-512:	F69241688378A4218E136C302DF5CE4BA6C24E2AC8D8651AC9EA155A9FCE45D5F1220C94235F21EF4DB75236147B5276CC3AE479A69399BDA791936C2943FA3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:48.199 13f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-18:42:48.201 13f8 Recovering log #3.2021/08/03-18:42:48.202 13f8 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\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):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A 0
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544901990438","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\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Entropy (8bit):	5.152183162812703
Encrypted:	false
SSDEEP:	12:XvVa5KkkGHArqiuFUtpFr1/PT5Oa5KkkGHArq2J:/Va5KkkGgCg3jOa5KkkGg7
MD5:	C9FE7E3450BD19104E18AF09A2B2A861
SHA1:	05442AC92BA0FFF97F352B39D8C26E7A53F74417
SHA-256:	848BDDE91D08C35E630D3DBEBEB8BB43AEBC56B1445254897C5A3EF8ABF30EBA
SHA-512:	E4776C435CA4E9E86C9115885CE269E99027B2F358CE61446BBF20D81A8D3F8EF3E27D6C55EDC4FCA7B8B4C284E3845E833DD555F626109287558F2FDD9D377
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:48.216 14c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/03-18:42:48.220 14c0 Recovering log #3.2021/08/03-18:42:48.222 14c0 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
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.152183162812703
Encrypted:	false
SSDEEP:	12:XvVa5KkkGHArqiuFUtpFr1/PT5Oa5KkkGHArq2J:/Va5KkkGgCg3jOa5KkkGg7
MD5:	C9FE7E3450BD19104E18AF09A2B2A861
SHA1:	05442AC92BA0FFF97F352B39D8C26E7A53F74417
SHA-256:	848BDDE91D08C35E630D3DBEBEB8BB43AEBC56B1445254897C5A3EF8ABF30EBA
SHA-512:	E4776C435CA4E9E86C9115885CE269E99027B2F358CE61446BBF20D81A8D3F8EF3E27D6C55EDC4FCA7B8B4C284E3845E833DD555F626109287558F2FDD9D377
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:48.216 14c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/03-18:42:48.220 14c0 Recovering log #3.2021/08/03-18:42:48.222 14c0 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):	424
Entropy (8bit):	5.169497626559424
Encrypted:	false
SSDEEP:	12:A4vVa5KkkGHArAFUtpHNJ/Pa3D5Oa5KkkGHArfJ:AKVa5KkkGgkg7oVOa5KkkGgV
MD5:	0DAF9013CED471741A900526293A9876
SHA1:	2E31E46887405FD8046AC3A682070C5360EC6117
SHA-256:	2C33D1D4E2EE0722A3515B9A9B0A0383182A88F04CE673F6631094FF157FFE22
SHA-512:	3510F6FBD021FFBBBBC7C45902A49E35F32B4BEE28FDC24153AE01AFDAEDA71E95647A00DE4F37923B3CD3264CB4B7247664F2F0A61432C2A7C0CCF7D0CB3468
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Preview:	2021/08/03-18:43:03.499 14b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-18:43:03.500 14b8 Recovering log #3.2021/08/03-18:43:03.501 14b8 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.old41 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.169497626559424
Encrypted:	false
SSDEEP:	12:A4vVa5KkkGHArAFUtpHNJ/Pa3D5Oa5KkkGHArfJ:AKVa5KkkGgkg7oVOa5KkkGgV
MD5:	0DAF9013CED471741A900526293A9876
SHA1:	2E31E46887405FD8046AC3A682070C5360EC6117
SHA-256:	2C33D1D4E2EE0722A3515B9A9B0A0383182A88F04CE673F6631094FF157FFE22
SHA-512:	3510F6FBD021FFBBBBC7C45902A49E35F32B4BEE28FDC24153AE01AFDAEDA71E95647A00DE4F37923B3CD3264CB4B7247664F2F0A61432C2A7C0CCF7D0CB3468
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:43:03.499 14b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-18:43:03.500 14b8 Recovering log #3.2021/08/03-18:43:03.501 14b8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
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):	330
Entropy (8bit):	5.194891508033342
Encrypted:	false
SSDEEP:	6:mvzyQ+q2PN723iKKdKpIFUtpOjkgZmwPtF+QQVkwON723iKKdKa/WLJ:+SvVa5KkmFUtpOh/Pe5Oa5KkaUJ
MD5:	0BF012B87114DAA1F7A18C5A4C32CF94
SHA1:	EB31DB3C516605B0942E1A129122B6EB93A11429
SHA-256:	65E7C41AC6350A2B8BADE6F646408D265DCD5191909C45685E58ABE08563B7DD
SHA-512:	76235274943DCFCEA3970A3CDBDF4A7920FD270FEF7D77788E83100EE8694E8CCA941F9ACA3F56EEC99D946AFA678B16C2852FD78E20DF3FC29CD6BC30D9172
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.707 14f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-18:42:28.709 14f8 Recovering log #3.2021/08/03-18:42:28.710 14f8 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.d (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old.d (copy)	
Size (bytes):	330
Entropy (8bit):	5.194891508033342
Encrypted:	false
SSDEEP:	6:mvzyQ+q2PN723iKKdKpIFUtpOjkgZmwPtF+QQVkwON723iKKdKa/WLJ:+SvVa5KkmFUtpOh/Pe5Oa5KkaUJ
MD5:	0BF012B87114DAA1F7A18C5A4C32CF94
SHA1:	EB31DB3C516605B0942E1A129122B6EB93A11429
SHA-256:	65E7C41AC6350A2B8BADE6F646408D265DCD5191909C45685E58ABE08563B7DD
SHA-512:	76235274943DCFCEA3970A3CDBDF4A7920FD270FEF7D77788E83100EE8694E8CCA941F9ACA3F56EEC99D946AFA678B16C2852FD78E20DF3FC29CD6BC30D917 2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-18:42:28.707 14f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-18:42:28.709 14f8 Recovering log #3.2021/08/03-18:42:28.710 14f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:42:35.240029097 CEST	192.168.2.6	8.8.8.8	0x8ad7	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:35.269565105 CEST	192.168.2.6	8.8.8.8	0xc966	Standard query (0)	tendaggisilvana.it	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:35.269656897 CEST	192.168.2.6	8.8.8.8	0x79ce	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:35.861203909 CEST	192.168.2.6	8.8.8.8	0xd549	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:35.862207890 CEST	192.168.2.6	8.8.8.8	0xbd4e	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:36.081267118 CEST	192.168.2.6	8.8.8.8	0x7ba	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:36.161524057 CEST	192.168.2.6	8.8.8.8	0x3e73	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:36.293517113 CEST	192.168.2.6	8.8.8.8	0x659b	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:36.328219891 CEST	192.168.2.6	8.8.8.8	0x5133	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:38.160891056 CEST	192.168.2.6	8.8.8.8	0xa5dc	Standard query (0)	tendaggisilvana.it	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:47.544529915 CEST	192.168.2.6	8.8.8.8	0xc907	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:42:35.270637035 CEST	8.8.8.8	192.168.2.6	0x8ad7	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:42:35.270637035 CEST	8.8.8.8	192.168.2.6	0x8ad7	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:35.317368984 CEST	8.8.8.8	192.168.2.6	0x79ce	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:35.322773933 CEST	8.8.8.8	192.168.2.6	0xc966	No error (0)	tendaggisilvana.it		168.119.64.244	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:35.894526005 CEST	8.8.8.8	192.168.2.6	0xbd4e	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:42:35.897368908 CEST	8.8.8.8	192.168.2.6	0xd549	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:35.897368908 CEST	8.8.8.8	192.168.2.6	0xd549	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:36.106139898 CEST	8.8.8.8	192.168.2.6	0x1f04	No error (0)	gstaticadssl.l.google.com		142.250.185.131	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:36.107518911 CEST	8.8.8.8	192.168.2.6	0x7ba	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:42:36.201086998 CEST	8.8.8.8	192.168.2.6	0x3e73	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:36.201086998 CEST	8.8.8.8	192.168.2.6	0x3e73	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:36.329308987 CEST	8.8.8.8	192.168.2.6	0x659b	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:42:36.360373020 CEST	8.8.8.8	192.168.2.6	0x5133	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:36.360373020 CEST	8.8.8.8	192.168.2.6	0x5133	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:38.233987093 CEST	8.8.8.8	192.168.2.6	0xa5dc	No error (0)	tendaggisilvana.it		168.119.64.244	A (IP address)	IN (0x0001)
Aug 3, 2021 18:42:47.580013037 CEST	8.8.8.8	192.168.2.6	0xc907	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:42:47.580013037 CEST	8.8.8.8	192.168.2.6	0xc907	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.161	A (IP address)	IN (0x0001)

HTTPS Packets

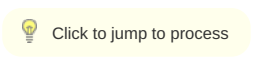
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 18:42:35.383055925 CEST	168.119.64.244	443	192.168.2.6	49724	CN=tendaggisilvana.it CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jul 07 01:28:05 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Oct 05 01:28:04 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Aug 3, 2021 18:42:35.389153004 CEST	168.119.64.244	443	192.168.2.6	49723	CN=tendaggisilvana.it CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jul 07 01:28:05 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Oct 05 01:28:04 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Aug 3, 2021 18:42:38.294826984 CEST	168.119.64.244	443	192.168.2.6	49749	CN=tendaggisilvana.it CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jul 07 01:28:05 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Oct 05 01:28:04 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5800 Parent PID: 2152

General

Start time:	18:42:27
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://tendaggisilvana.it/officix/'
Imagebase:	0x7ff7c15e0000
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

Analysis Process: chrome.exe PID: 5984 Parent PID: 5800

General

Start time:	18:42:29
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=1632,16278824397204307 3,8402254026257192306,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1744 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly