ID: 458966
Cookbook: browseurl.jbs
Time: 23:15:02
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

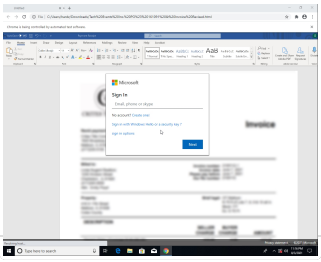
Windows Analysis Report https://aeriallightingandelectr…

Overview

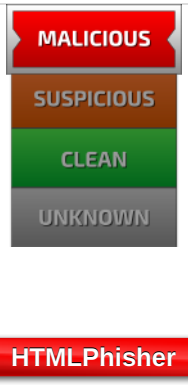
General Information

Sample URL:	https://aeriallightingandelectric-my.sharepoint.com/:u:/g/personal/khardy_a...erialelectric_com/ESDO6oK0Y2FPjomZ3thjzpYB912czBooPXA5DhMbhXvPhA?download=1
Analysis ID:	458966
Infos:	

Most interesting Screenshot:



Detection



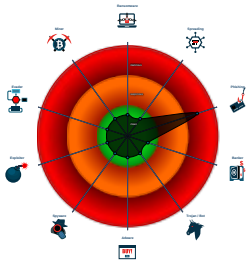
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- No HTML title found
- None HTTPS page querying sensitiv…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5284 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://aeriallightingandelectric-my.sharepoint.com/:u:/g/personal/khardy_aerialelectric_com/ESDO6oK0Y2FPjomZ3thjzpYB912czBooPXA5DhMbhXvPhA?download=1' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4244 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1736,4776280355382224090,2163248144403128918,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1792 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6600 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=quarantine.mojom.Quarantine --field-trial-handle=1736,4776280355382224090,2163248144403128918,131072 --lang=en-US --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=4608 /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

Phishing:

Yara detected HtmlPhish10

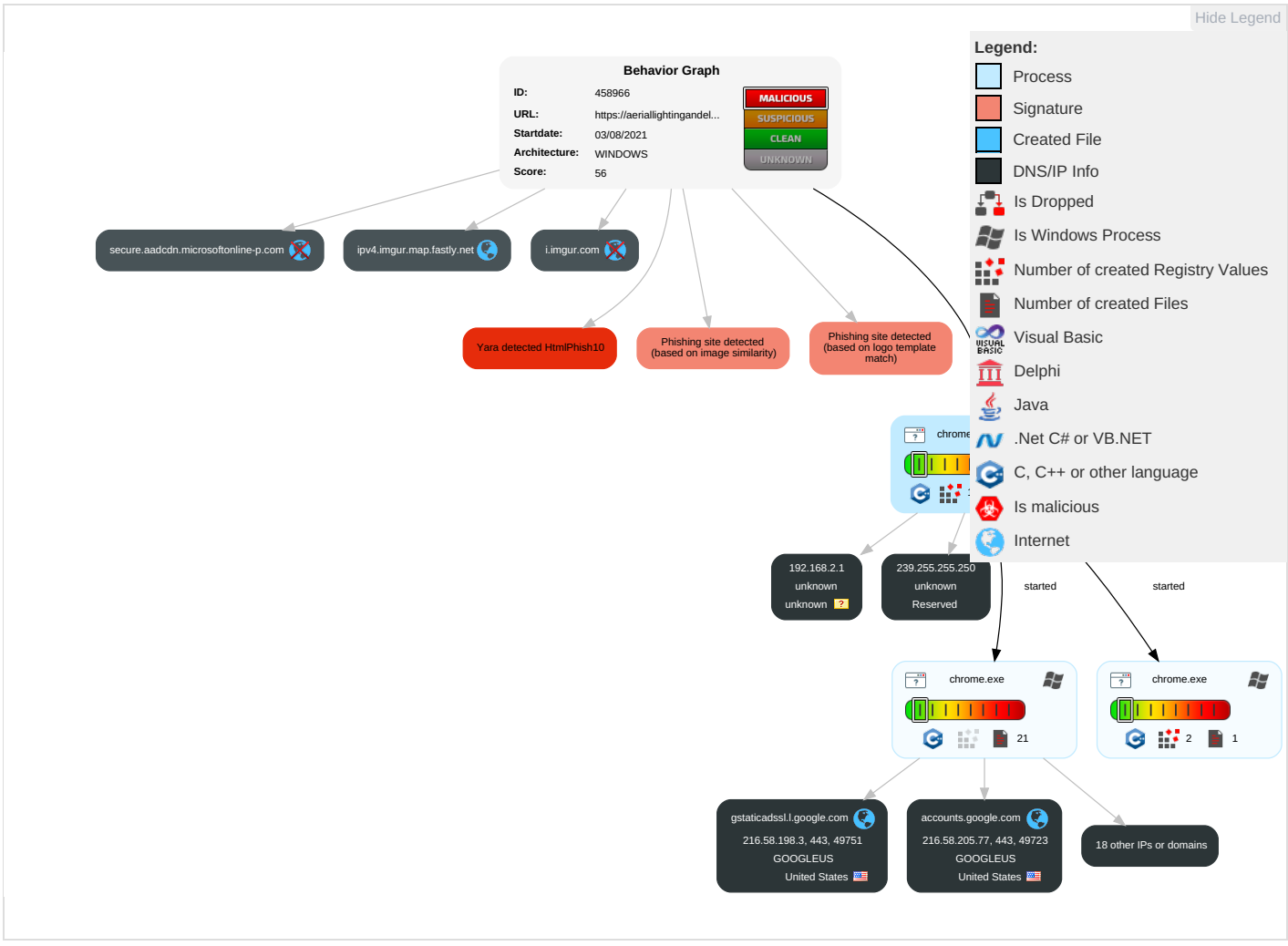
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

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

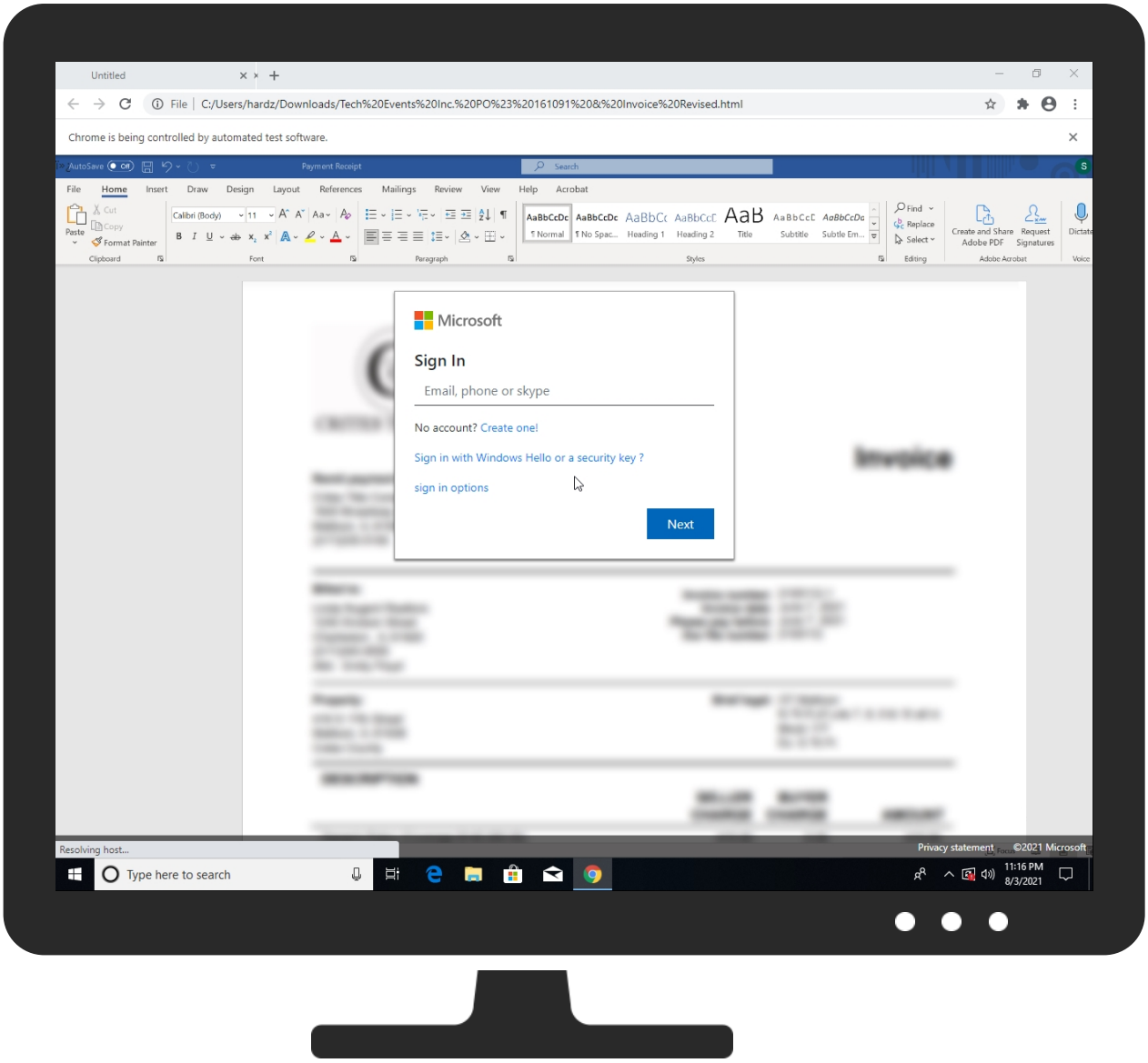
Behavior Graph



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://aeriallightingandelectric-my.sharepoint.com/:u:/g/personal/khardy_aerialelectric_com/ESDO6oK0Y2FPjomZ3thjzpYB912czBooPXA5DhMbhXvPhA?download=1	0%	Virustotal		Browse
http://https://aeriallightingandelectric-my.sharepoint.com/:u:/g/personal/khardy_aerialelectric_com/ESDO6oK0Y2FPjomZ3thjzpYB912czBooPXA5DhMbhXvPhA?download=1	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://aeriallightingandelectric-my.sharepoint.com	0%	Avira URL Cloud	safe	
http://https://aeriallightingandelectric-my.sharepoint.com/personal/khardy_aerialelectric_com/Documents/Tec	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	
http://https://aeriallightingandelectric-my.sharepoint.com/:u:/g/personal/khardy_aerialelectric_com/ESDO6oK	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	216.58.198.3	true	false		high
accounts.google.com	216.58.205.77	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
i.gyazo.com	104.19.142.111	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
clients.l.google.com	216.58.208.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
ipv4.imgur.map.fastly.net	151.101.112.193	true	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
i.imgur.com	unknown	unknown	false		high
aeriallightingandelectric-my.sharepoint.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Downloads/Tech%20Events%20Inc.%20PO%23%20161091%20&%20Invoice%20Revised.html	true		low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
216.58.198.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
151.101.112.193	ipv4.imgur.map.fastly.net	United States		54113	FASTLYUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
216.58.208.174	clients.l.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
104.19.142.111	i.gyazo.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458966
Start date:	03.08.2021
Start time:	23:15:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://aeriallightingandelectric-my.sharepoint.com/:u:/g/personal/khardy_aerialelectric_com/ESDO6oK0Y2FPjomZ3thjzpYB912czBooPXA5DhMbhXvPhA?download=1
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:	23
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:	mal56.phis.win@35/223@14/11
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:16:01	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):	451644
Entropy (8bit):	5.009884856905657
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4py:NfOCzvRKhGvwr
MD5:	3C34D7735D837B7231E361F4C6432B8D
SHA1:	C4DF4FF967106705762AF22CA2EE23C92EC6CBF3
SHA-256:	F2AB8BBD5DDF2816097E2037BE01164F7AC3513B4C3BF874C5FDCF9E2C88179B
SHA-512:	933DAEF699F3349A53EE402A87243C6A563208E2EBD7A61A05413ED3E1C8C913C58F021175A8AE8A1F21EF980FE6F1F979A93DDF6D8A1AA8B5FB6F16BCB32A26
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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1392054451166236
Encrypted:	false
SSDEEP:	6:kKAMCdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:o75kPlE99SNxAhUe0et
MD5:	F66A39E206A979A6E639C3E7CA077F43
SHA1:	0DE7EBE51C2223C70BAF756183EB69B264174D9D
SHA-256:	5626995E68ACBD8A45EAA24F6546780C547C34EBA96BA0B4E0D8752C4E81C44C
SHA-512:	E4A57296033450F570D63A370BA972810ED23969A27A7A1CE20DC488FFAFADD484FFD165F74406868BA57219B074D87C772BA0574D5C2184384C8BB1ED737FA5
Malicious:	false
Reputation:	low
Preview:	p..... ....P.2....(..... ....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\17cf0fb9-0746-4578-8d33-0d156de8bd92.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):	165963
Entropy (8bit):	6.049811535886827
Encrypted:	false
SSDEEP:	3072:xGaYTJQE+mugy9+QV1T7IRwdfLSNPIFcbXafIB0u1GOJmA3iuR9:8xaV+QfT7GSmhWaqfIlUOoSiuR9
MD5:	B47843A2CCFC3A51B0FBBCF6A41ED870
SHA1:	8720C9BBDC27A4887A63F07325321D814F7D894B
SHA-256:	DF764F15AEC8D38B3A2D44737F4E62D645B05F650B6DA2051133CC500EFFC655
SHA-512:	826E9219865D98130FDCE9F1B5A4C4A2E1FF6FE5E1CDBEB1381F350780D6D05F43EF95E8B825282D17DA337F80BB4671D68EABCB31BC8E6033425E825C297A4 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":1.628057757934339e+12,"network":1.628025359e+12,"ticks":7007826017.0,"uncertainty":4452420.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016268842"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\354c7e11-3d64-4a12-bd54-ebddfd567b8c.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):	174336
Entropy (8bit):	6.079337851095721
Encrypted:	false
SSDEEP:	3072:DcfGaYTJQE+mugy9+QV1T7IRwdfLSNPIFcbXafIB0u1GOJmA3iuR9:AuxaV+QfT7GSmhWaqfIlUOoSiuR9
MD5:	93E937FDAAFEE7B0A3D8B6620F8FC383
SHA1:	27E40371EBB907FE54822F99716D7CB7E7B70EF5
SHA-256:	1FF1A828C4F254980192001A2B91C46928D5E3305F7E3AA4382E276F0584C12D
SHA-512:	37BDF572AE58C4AEA633F80208E61B5A7D88DE93C098E0F91AAB95013B2F528654889F0B1113AEEBF975164CE4760FF593CB97ECC7E5AC6380D33D8D340D756
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":1.628057757934339e+12,"network":1.628025359e+12,"ticks":7007826017.0,"uncertainty":4452420.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\3ede8b4a-5cb3-48c4-8ad2-6739f7918b47.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	99532
Entropy (8bit):	3.7498385549581434

C:\Users\user\AppData\Local\Google\Chrome\User Data\3ede8b4a-5cb3-48c4-8ad2-6739f7918b47.tmp	
Encrypted:	false
SSDEEP:	384:frRAYgKNvGpSEVFHs/Ngr5vcY3zQWPHKfGYPar1Koqx6fz+GG5r1omhtHZaQMMPJ:4Wq1ZCAQr8eHOIerHH+sKicMJI
MD5:	3E3B5C0395BA1BBC98F85046060FEC7A
SHA1:	79914C66179615B663D861286DF63BA837545EB9
SHA-256:	1F4A6F132D3E0C6C2B223404E72F598EB61897F670628150705AB67A8E04232E
SHA-512:	069DC1A46E03E56A2B3089372E22648076533DB88973057B4FCDFC280F717BBD2473D6BC916F4F4D2CB631FB5C337C723D513A4C62AEC6F90B836868322DA81(
Malicious:	false
Reputation:	low
Preview:	.....*...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\48d0d273-ac5a-4969-b18e-3a4acb39e086.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	98812
Entropy (8bit):	3.7499195588411824
Encrypted:	false
SSDEEP:	384:brRAYgKNvGpSEVFHs/Ngr5vcY3zQWPHKfGYPar1Koqx6fz+GG5r1omh2ZaQMMPO1:EWq1ZCAjr8eHOIerHH+sKicMJx
MD5:	62BAA68B056A7FF9006012007A7AE9BE
SHA1:	D38EA2E11786ED7F9F52E34B60D935A21238F3FF
SHA-256:	40FE4FDD6FE7B6A39C028A22AB502B61DADBCF6EE6F69B4C82C05129DA95BA75
SHA-512:	48F72E5C2A07CA25194F5D909689F9B7FF6E03D084ACA40EC39F76322209EA2A115C895306CA631235862E8745D2034B783149EA720A23D13ED192810B5964A3
Malicious:	false
Reputation:	low
Preview:	.....*...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\65f23d2b-90c4-4e1b-ad3f-294f58f1c7d2.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):	174336
Entropy (8bit):	6.079337893179464
Encrypted:	false
SSDEEP:	3072:cVZGaYTJQE+mugy9+QV1T7IRwdfLSNPIFcbXafIB0u1GOJmA3iuR9:aUxaV+QfT7GSmhWaqfIlUOoSiuR9
MD5:	3325B0E36B74A6A24DF00F926DF6E01C
SHA1:	F2A614B4958AE1253613C89132DAC6DF173BA5EF
SHA-256:	F1A3A103F934AD19087B4A99001B6C66C510AD8BA741226DDD496F5944AF2D85
SHA-512:	2FDCF76F599FD3ED5D241AB25949155C34C5892C93D3F4F9768187C8357AD1C8847F8BA721ECB7670D1FEDA0982A53556EFE9792E3C1E1ED08894D552D667E2
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":1.628057757934339e+12,"network":1.628025359e+12,"ticks":7007826017.0,"uncertainty":4452420.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016268842"},"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):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000002.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Xv:1qIF/
MD5:	206702161F94C5CD39FADD03F4014D98
SHA1:	BD8BFC144FB5326D21BD1531523D9FB50E1B600A
SHA-256:	1005A525006F148C86EFCBFB36C6EAC091B311532448010F70F7DE9A68007167
SHA-512:	0AF09F26941B11991C750D1A2B525C39A8970900E98CBA96FD1B55DBF93FEE79E18B8AAB258F48B4F7BDA40D059629BC7770D84371235CDB1352A4F17F80E145
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000002.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2345
Entropy (8bit):	6.1047505734054415
Encrypted:	false
SSDEEP:	48:yZ/XwyjAmpEbzXlMgv874BqsXwyjAmpEbzXlMgv87fqZHtHcqZHtHtV2:eu3vMEu3vZLT2
MD5:	CB932B70F7ADECDC1AF1E0D9DE15C461
SHA1:	12A7710C29169609628D1BE705997917FD08EBCB
SHA-256:	6DAF276F06BD627773B2D0D6C7D06B28A562220077A9ACDBF02A78D679B7ADAD
SHA-512:	83C7C4028349BEA4F4C8927D95083BE5BC8322F1A8DAAE1BFD3A368BC5DF1CE9D57F355DB22723623EC6DA230B16C76ED58834B108DF8AA09732A1381F855D2
Malicious:	false
Reputation:	low
Preview:	.....-download,3472d65f-6338-460e-8f73-1f1b075762ce.....$3472d65f-6338-460e-8f73-1f1b075762ce....."".....https://aeriallightingandelectric-my.sharepoint.com/:u:/g/personal/khardy_aerialelectric_com/ESDO6oK0Y2FPjomZ3thjzpYB912czBooPXA5DhMbhXvPhA?download=1...https://aeriallightingandelectric-my.sharepoint.com/personal/khardy_aerialelectric_com/Documents/Tech%20Events%20Inc.%20PO%23%20161091%20%26%20Invoice%20Revised.html?originalPath=aHR0cHM6Ly9hZXJpYWxsaWdodGluZ2FuZGVsZWN0cmljLW15LnNoYXJlcG9pbnQuY29tLzp1Oi9nL3BlcnNvbmFsL2toYXJkeV9hZXJpYWxlbGVjdHJpY19jb20vRVNETzZvSzBZMkZQam9tWjN0aGp6cFlCOTEyY3pCb29QWEE1RGhNYmhYdlBoQT9ydGltZT1IanVTNDhOVzJVZw....".."..https://aeriallightingandelectric-my.sharepoint.com/:u:/g/personal/khardy_aerialelectric_com/ESDO6oK0Y2FPjomZ3thjzpYB912czBooPXA5DhMbhXvPhA?download=1*.0.B*"{82EACE20-63B4-4F61-8E89-99DED863CE96},1"J.Tue, 03 Aug 2021 18:33:12 GMTP.Z.text/htmlb.text/htmlj.....r.....x.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\330b4640-eae5-47bf-9937-eec04ba62744.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\330b4640-eae5-47bf-9937-eec04ba62744.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5487
Entropy (8bit):	5.179934973927058
Encrypted:	false
SSDEEP:	96:nYCmTP9/SHgoeXcKIkok0JCKL8r0bOTQVuwn:nYCs9aHaXcN4KGe
MD5:	AEE7807F188FE5DAD2567AB56E8491DA
SHA1:	4462B59F806DF15D567AFA6DAC4163E87232486E
SHA-256:	32DA22C7CC81721EEC0873D1C400E1AC67C0D557BA00AD0155006ABDEC9BAF00
SHA-512:	69A5DACE79D1EED16C5058DC775934DDE0DF148AC648F9BC3D7B278E89F8E6EC9322AB56386C67FAEE41698C9E41D82537BCA44093A35BE36D94B836917B53 4
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272531353690745","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"co untryid_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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\34a09cc3-5620-4c00-a74f-ace7356cd8e9.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):	5.535847986061201
Encrypted:	false
SSDEEP:	384:E30tbLlyKvX61kXqKf/pUZNCgVLH2HfDArU6HGIXnTjmr3qVX4B:nLld/61kXqKf/pUZNCgVLH2HfsrUKGIg
MD5:	48DAAF38CA21FF574F454101E7ED6010
SHA1:	BA88610D09A92DB9B66DA338220A596DDEBBB20E
SHA-256:	03F2CC5A7B05D22017D317759A304E377041BADB05F47679A5D17A6BE7B55ED4
SHA-512:	2360A6A6C0041B87169D5C95F558228F8EC503ABA172582880E271A6D64F5329857DB820E48DDC34D2B33AD72839BB38892DC2BAD09EB25652B3A36570D433D5
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":"13272531353262882","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 ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3543d666-fc01-4525-bf8e-e88203c45e9c.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):	5461
Entropy (8bit):	5.177148927949988
Encrypted:	false
SSDEEP:	96:nYCmqP9/SHgoeXcKIkok0JCKL8VbOTQVuwn:nYCf9aHaXcN4K6
MD5:	7BA11185D24A959E3092ECD881FAA943
SHA1:	1D34ADA36E35A9DD2FE5C738131FD985709EC0D4
SHA-256:	EF6500A11C3E1F0DAC94B9ABEB2DFE583533297EFDD7B4E06846EA8BE8266912
SHA-512:	3DAD110C6AC23234109E572DA0DEFCC7D88354F8F4B1A5741652F05345E040BAA92C3EDA7DB7CC430B617D96BAC2E3652E9EB74C6E86BF8B635935D7BBEAD 2C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272531353690745","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"co untryid_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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41409979-6a65-4759-a2f3-834d61c549ee.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41409979-6a65-4759-a2f3-834d61c549ee.tmp	
Category:	modified
Size (bytes):	3019
Entropy (8bit):	4.880735283194612
Encrypted:	false
SSDEEP:	48:Y2TntwXGDHz5spEITspEsRLspD8pRSRWz5e86NlsW8zsI6q7s8MHVh8VsNyKse3H:JTnOXGDHzaEIUEsSDoRHz5j6NtqxFGVf
MD5:	CCC27DDFB9FA66C28D217F604FA5878B
SHA1:	DF2A1DEFE9B0F06486FC5CA1CD0991A3D26C19C5
SHA-256:	ACC7E231EF79C96D20DD00A6A0D5DB098C126F678CD92581FDEC452A9F9F02DC
SHA-512:	CB15E309A658B6C0BE59B358D84CF34F28794844B636DCCC576331342018AB7FB967925CC92830E73BA0EA273FE6AD2A1D5FE21B9DE13F0516EECF0DC62489
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.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":"13275123358383833","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275123358387738","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expira

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\945a4cdd-9723-4a61-8c49-2d1858e0d946.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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.213194713887498
Encrypted:	false
SSDEEP:	6:mk0uzjyq2PWXp+N23iKKdK9RXXTZIFUtp76cz1ZmwP76clRkwOWXp+N23iKKdK9l:r0UOva5Kk7XT2FUtp7l1/P7V5f5Kk7XH
MD5:	9D3F0C52CA3F2E50D404EA68B4FF2529
SHA1:	7CBDC3B2DD7B3EC923E5A26FC0FA8FD9E2D1B298
SHA-256:	A867F50648316907EDB8EFFF21A11A071FBF2F179AA414A8347B71194A830629
SHA-512:	D977AAF7DC97B5D306E6C0B5E75A747B0078C6D143D163075E38FB13517A09142474DA9A2139146D800C156D023E0FE5B9A2E3F4748A07E2740F2125F420C1BE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.147 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-23:16:02.149 1a14 Recovering log #3.2021/08/03-23:16:02.149 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.213194713887498
Encrypted:	false
SSDEEP:	6:mk0uzjyq2PWXp+N23iKKdK9RXXTZIFUtp76cz1ZmwP76clRkwOWXp+N23iKKdK9l:r0UOva5Kk7XT2FUtp7l1/P7V5f5Kk7XH
MD5:	9D3F0C52CA3F2E50D404EA68B4FF2529

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
SHA1:	7CBDC3B2DD7B3EC923E5A26FC0FA8FD9E2D1B298
SHA-256:	A867F50648316907EDB8EFFF21A11A071FBF2F179AA414A8347B71194A830629
SHA-512:	D977AAF7DC97B5D306E6C0B5E75A747B0078C6D143D163075E38FB13517A09142474DA9A2139146D800C156D023E0FE5B9A2E3F4748A07E2740F2125F420C1BE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.147 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-23:16:02.149 1a14 Recovering log #3.2021/08/03-23:16:02.149 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.167531968470579
Encrypted:	false
SSDEEP:	6:mkqjyq2PWXp+N23iKKdKyDZIFUtp7fz1ZmwP7oFlRkwOWXp+N23iKKdKyJLJ:r3va5Kk02FUtp7fz1/P7oF5f5KkWJ
MD5:	043DDC227A583C8F3C2646C6B70DE4EB
SHA1:	F73BAB65BFB0A7E84DEB104C5C23EC9045E9F326
SHA-256:	0D97E4A07300944D49EBD0E2EDB7E81EFE1429F5DA010FF0FC33156DA99F22B8
SHA-512:	92D89847D608814FB7C0ED69BFDB63272E10955369064E9FC3E881F3C90C79307D51EB141E6291A5AFBF4320B215D238AFB497CD1E91DB302668DD62F428BDF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.133 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-23:16:02.136 1a14 Recovering log #3.2021/08/03-23:16:02.139 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.167531968470579
Encrypted:	false
SSDEEP:	6:mkqjyq2PWXp+N23iKKdKyDZIFUtp7fz1ZmwP7oFlRkwOWXp+N23iKKdKyJLJ:r3va5Kk02FUtp7fz1/P7oF5f5KkWJ
MD5:	043DDC227A583C8F3C2646C6B70DE4EB
SHA1:	F73BAB65BFB0A7E84DEB104C5C23EC9045E9F326
SHA-256:	0D97E4A07300944D49EBD0E2EDB7E81EFE1429F5DA010FF0FC33156DA99F22B8
SHA-512:	92D89847D608814FB7C0ED69BFDB63272E10955369064E9FC3E881F3C90C79307D51EB141E6291A5AFBF4320B215D238AFB497CD1E91DB302668DD62F428BDF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.133 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-23:16:02.136 1a14 Recovering log #3.2021/08/03-23:16:02.139 1a14 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\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Xv:1qIF/
MD5:	206702161F94C5CD39FADD03F4014D98
SHA1:	BD8BFC144FB5326D21BD1531523D9FB50E1B600A
SHA-256:	1005A525006F148C86EFCBFB36C6EAC091B311532448010F70F7DE9A68007167
SHA-512:	0AF09F26941B11991C750D1A2B525C39A8970900E98CBA96FD1B55DBF93FEE79E18B8AAB258F48B4F7BDA40D059629BC7770D84371235CDB1352A4F17F80E145
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000002.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	1.9363503904622605
Encrypted:	false
SSDEEP:	96:dNw+RjobqV8lKxBQGaVlNwTRjobqV8lKxBQGaVaNpe0:duNw8l+Ofu2w8l+Ooi0
MD5:	C43F70C69F51CDCEF9D84D8FA446D250
SHA1:	4837806E5831411B5F97480B0CE0CAC0D3061975
SHA-256:	BE3A187D76DCA3E98C6851090779D0181F51D3CCB80E92FD91FB3FA1E888181F
SHA-512:	FE20480037458890A6DD37668A78CE14899AE599337151464D5FF4EBFBADFA15BCFACBF34DFEF3B1ED1505E321C23C65301A6E9C0133F0ADC0EC96B413FF093C
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):	25672
Entropy (8bit):	1.4280055565201129
Encrypted:	false
SSDEEP:	48:d8NOZ4q5LLOpEO5J/Kn7UFX/mDRYyobMHRn8cOk/x1tdWdbCH6VnnXtqekLLOpEA:qO4cNw5/mDRjobqV8lKxBQGaVdMNwF
MD5:	704F4430166B2415351C3EBB11723FF9
SHA1:	2D62CEE50EF8B3575D0796CA966AB8623E5E8043
SHA-256:	D4B82483E7BBC3692CD892BBEE3DC57B3C6B2D4DB963A8C9937CD6362FF6062C
SHA-512:	D43B3006FEAD2211A9A40C2A3639168C2FD273F95CAEE4910B9B6F6364610AF10117929A279D216B7CA1D2B37CAE92D73D7D9E78198414302D9479B94CF38BC
Malicious:	false
Reputation:	low
Preview:	.....~..J..... ....

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):	1766
Entropy (8bit):	3.570070320831956
Encrypted:	false
SSDEEP:	24:34StylrlA5l1tZmgFbrr+6yeAfLHkaS6Ow/Le6K+6yeAQC0lL:34RxiMg86y3l5rwTn6yY1L
MD5:	5CBA1E07CCCE09F2829EC476F58A381B
SHA1:	908481703378623A74A6F484B32D4205F72A0420
SHA-256:	6267D2B67AD2B494DED95ACF6EB89FB191AD3D6C774BFEFDBD62DDEFDD115D6A
SHA-512:	4E94E3A292CFEA711D13AE09FA59744681030F88E33F7119B5CA72567A3AB8BF0BF4F78E33E06F8D85CCDD8877C74BB250D3EE46D0F9D3150358B1F01CCC4CAB
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...2aa2da33_64dd_48c2_90f1_406dd562921e.....Ffp..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....!.....1.,.....$...aac8d093_1794_435a_9e15_550b0c14e192.....+.....c...file:///C:/Users/user/Downloads/Tech%20Events%20Inc.%20PO%23%20161091%20&%20Invoice%20Revised.html.....M.i.c.r.o.s.o.f.t. .W.o.r.d. .O.n.l.i.n.e...t...p.....h.....h.....`.....0.....8.....3.....3..... .....c...f.i.l.e.:././/.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.o.w.n.l.o.a.d.s./.T.e.c.h.%.2.0.E.v.e.n.t.s.%.2.0.I.n.c...%.2.0.P.O.%.2.3.%.2.0.1.6.1.0.9.1.%.2.0.&.%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.230336777749265
Encrypted:	false
SSDEEP:	6:mNEN+q2PWXp+N23iKKdK8aPrqIFUtpeGZmwPe7DtVkwOWXp+N23iKKdK8amLJ:rIva5KkL3FUtpb/PKDT5f5KkQJ
MD5:	BAF848745A989E2E53FE6C6F1750797B
SHA1:	5327D988A73964D5C7AB4FC09552BD7D8123F372
SHA-256:	5A748323C237A7D0820415698A89907C22B710BE61065BCD8BA5C21361B87533
SHA-512:	9D07244F5F18AAAF2A4D1D4EC211C1F69F45446069D3821715DB99B1E17C32B055A631EA50DA18509D610A29FEEA75AE005124685ED1CA746D12E47C95AE335
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.701 428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-23:15:53.703 428 Recovering log #3.2021/08/03-23:15:53.704 428 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):	317
Entropy (8bit):	5.230336777749265
Encrypted:	false
SSDEEP:	6:mNEN+q2PWXp+N23iKKdK8aPrqIFUtpeGZmwPe7DtVkwOWXp+N23iKKdK8amLJ:rIva5KkL3FUtpb/PKDT5f5KkQJ
MD5:	BAF848745A989E2E53FE6C6F1750797B
SHA1:	5327D988A73964D5C7AB4FC09552BD7D8123F372
SHA-256:	5A748323C237A7D0820415698A89907C22B710BE61065BCD8BA5C21361B87533
SHA-512:	9D07244F5F18AAAF2A4D1D4EC211C1F69F45446069D3821715DB99B1E17C32B055A631EA50DA18509D610A29FEEA75AE005124685ED1CA746D12E47C95AE335
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.701 428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-23:15:53.703 428 Recovering log #3.2021/08/03-23:15:53.704 428 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
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.....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):	317
Entropy (8bit):	5.280490286629153
Encrypted:	false
SSDEEP:	6:mu+q2PWXp+N23iKKdK8NIFUtpyrJZmwPMtVkwOWXp+N23iKKdK8+eLJ:Qva5KkpFUtpyrJ/PQ5f5KkqJ
MD5:	81E068A0A417D57DDB32F6A71A3E0178
SHA1:	CF81E5A8C333651317AE4C05EE067F210273D08E
SHA-256:	4CCADF4604EC090C010C454BFB31A09C4201E87A1474DE3CE384145E318CC539
SHA-512:	CEAC6CF5B167EA4CABDA90B89339D3022BDAFAC94A2FB7747C66600D28294CEAA67C4594B3DB7487F19CFFEB2F740C7D2DA0D0462516C2673F59B4B79B644 17
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:57.958 428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-23 :15:57.959 428 Recovering log #3.2021/08/03-23:15:57.960 428 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):	317
Entropy (8bit):	5.280490286629153
Encrypted:	false
SSDEEP:	6:mu+q2PWXp+N23iKKdK8NIFUtpyrJZmwPMtVkwOWXp+N23iKKdK8+eLJ:Qva5KkpFUtpyrJ/PQ5f5KkqJ
MD5:	81E068A0A417D57DDB32F6A71A3E0178
SHA1:	CF81E5A8C333651317AE4C05EE067F210273D08E
SHA-256:	4CCADF4604EC090C010C454BFB31A09C4201E87A1474DE3CE384145E318CC539
SHA-512:	CEAC6CF5B167EA4CABDA90B89339D3022BDAFAC94A2FB7747C66600D28294CEAA67C4594B3DB7487F19CFFEB2F740C7D2DA0D0462516C2673F59B4B79B644 17
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:57.958 428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-23 :15:57.959 428 Recovering log #3.2021/08/03-23:15:57.960 428 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.261147785237251
Encrypted:	false
SSDEEP:	6:mLOyq2PWXp+N23iKKdK25+Xqx8chI+IFUtpoCz1ZmwPoClRkwOWXp+N23iKKdK2L:6va5KkTXfchI3FUtpoY1/Poq5f5KkTXc
MD5:	2FF88E457010D149CD67BE79325B457A
SHA1:	A8690F3F0987F0C6D1FD24D787D93EB3D16B72AC
SHA-256:	D7ED0F39CE294F0EACF31E81C2C40524AB333AD64AFC6B824FECD4E2222E8670
SHA-512:	90E208494E9A4BD20398D44CE366648FE2930F3FD5D633A212FA6FD816889E0408C43B315BFDF25DDD83927BED1F9F04DF268A5AE340211FC1DFD4AC8076D39

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.057 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-23:16:02.059 1a14 Recovering log #3.2021/08/03-23:16:02.059 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.261147785237251
Encrypted:	false
SSDEEP:	6:mLOyq2PWXp+N23iKKdK25+Xqx8chI+IFUtpoCz1ZmwPoClRkwOWXp+N23iKKdK2L:6va5KkTXfchI3FUtpoY1/Poq5f5KkTXc
MD5:	2FF88E457010D149CD67BE79325B457A
SHA1:	A8690F3F0987F0C6D1FD24D787D93EB3D16B72AC
SHA-256:	D7ED0F39CE294F0EACF31E81C2C40524AB333AD64AFC6B824FECD4E2222E8670
SHA-512:	90E208494E9A4BD20398D44CE366648FE2930F3FD5D633A212FA6FD816889E0408C43B315BFDF25DDD83927BED1F9F04DF268A5AE340211FC1DFD4AC8076D39
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.057 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-23:16:02.059 1a14 Recovering log #3.2021/08/03-23:16:02.059 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.186113098289197
Encrypted:	false
SSDEEP:	6:mMAyq2PWXp+N23iKKdK25+XuoIFUtp2Y1ZmwP2ORkwOWXp+N23iKKdK25+XuxWLJ:Dlva5KkTXYFUtpt1/Pt5f5KkTXHJ
MD5:	C549B5B9CED221ECA6F3BED037F0F76C
SHA1:	6B1EE1E5E30125ECD89F1107E83B7B4B4676A99D
SHA-256:	D1DD8D4A904076FADD11CA67649795F0DB5513B5B26B923F9CD73B005D5F70A8
SHA-512:	BEC7E26C3956D862CCADB68F0B85B49B2B4A70092D767EF497C0D8E0A398716E7DB1AB9EA775A82C0FE2EAED021613FC36DC20F7F8809F721532C61C76C3BA A6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.052 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-23:16:02.053 1a14 Recovering log #3.2021/08/03-23:16:02.053 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.186113098289197
Encrypted:	false
SSDEEP:	6:mMAyq2PWXp+N23iKKdK25+XuoIFUtp2Y1ZmwP2ORkwOWXp+N23iKKdK25+XuxWLJ:Dlva5KkTXYFUtpt1/Pt5f5KkTXHJ
MD5:	C549B5B9CED221ECA6F3BED037F0F76C
SHA1:	6B1EE1E5E30125ECD89F1107E83B7B4B4676A99D
SHA-256:	D1DD8D4A904076FADD11CA67649795F0DB5513B5B26B923F9CD73B005D5F70A8
SHA-512:	BEC7E26C3956D862CCADB68F0B85B49B2B4A70092D767EF497C0D8E0A398716E7DB1AB9EA775A82C0FE2EAED021613FC36DC20F7F8809F721532C61C76C3BA A6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.052 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-23:16:02.053 1a14 Recovering log #3.2021/08/03-23:16:02.053 1a14 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.19121905953605
Encrypted:	false
SSDEEP:	6:mPjyq2PWXp+N23iKKdKWT5g1IdqIFUtp3g/1ZmwPtpRkwOWXp+N23iKKdKWT5g1L:Xva5Kkg5gSRFUtp3g/1/PtP5f5Kkg5gZ
MD5:	6FAE262E335B92F63E098DFFEE5469F1
SHA1:	48AD73AA7343A7FE045C5CF526B5D58868CF11B3
SHA-256:	8CC921AA0743B6BC3F4D7277EA2FDE31F1EFA4A163B1E069272BE9F3D55843D4
SHA-512:	619B4FD0096AD67AD302282F606B8212FAC9F5577DA86E5C0BC92E797DCB2944690A64D380F2D19A77860E283B53365F54241F745BC118D8CEC5EC6C62754B46
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.025 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-23:16:02.030 1a14 Recovering log #3.2021/08/03-23:16:02.031 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.19121905953605
Encrypted:	false
SSDEEP:	6:mPjyq2PWXp+N23iKKdKWT5g1IdqIFUtp3g/1ZmwPtpRkwOWXp+N23iKKdKWT5g1L:Xva5Kkg5gSRFUtp3g/1/PtP5f5Kkg5gZ
MD5:	6FAE262E335B92F63E098DFFEE5469F1
SHA1:	48AD73AA7343A7FE045C5CF526B5D58868CF11B3
SHA-256:	8CC921AA0743B6BC3F4D7277EA2FDE31F1EFA4A163B1E069272BE9F3D55843D4
SHA-512:	619B4FD0096AD67AD302282F606B8212FAC9F5577DA86E5C0BC92E797DCB2944690A64D380F2D19A77860E283B53365F54241F745BC118D8CEC5EC6C62754B46
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.025 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-23:16:02.030 1a14 Recovering log #3.2021/08/03-23:16:02.031 1a14 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\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	296
Entropy (8bit):	0.4481240366544235
Encrypted:	false
SSDEEP:	3:8EfloVCKltl:8Rtl
MD5:	2C57F22CA34FBD5A1E24410310B8B32B
SHA1:	A2E84513B9078F376F10457AFB83A3A0E2D82DDC
SHA-256:	77424A0E38F8D9FFFBD11B534A3FBC1FF5A0531403EB17EFBF637C994EE64B13
SHA-512:	9E9703C04C1CEF8C79680E037EC4FC52CB436D839708AB9876F67846AC5EA34195C54DF4DFA494B971F5E4B0205613D11E8B0B07AD08E6E8DCE0EB15B51BC3F
Malicious:	false
Reputation:	low
Preview:	.'...(.....b.L'/.....

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):	45056
Entropy (8bit):	0.40239222892942006
Encrypted:	false
SSDEEP:	48:TYcXK3XzMvl60yjAmpEbF6XM96y4rJg6yY:+zGqIP9mNg2
MD5:	54A98F0440C99851D422CACE57880888
SHA1:	3090FB7D9E913B62CDB77C9FAB0634A22DABE676
SHA-256:	F9699DA73F7B84FB2B0FB49E19DF7C5DE2FED9E5F60F9070843DC5F4FD4517CC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
SHA-512:	EA637EB3CC10669AA96585BBD1A8D1A449E5FEEF98A3224E0798D3A266246D0A5DEF2B3D3272E4B67BC94AFF5C780311F9F791BF57D8F6DB636684B30AA30C8F
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):	783
Entropy (8bit):	5.3593829780203
Encrypted:	false
SSDEEP:	24:ty7k4TbRm0+lqlPC1rDY78BJgskfa9yBDOL+6yeAFYI:tyJWl1rHUX6yGI
MD5:	96F891047AE2410284B01A8A2D6944FA
SHA1:	C659F58B80F075771BE106E56AB4D64BBEA3009B
SHA-256:	F07308D147A31DF8176F0B58467DBDAAAA025AA9C3C6DE68D12C5BE5AAE16476
SHA-512:	CA42369941FC4E68B5650F43A51BF2CC61C6B85E4E38FCCB90D30F22C36C24B52535078404BCF5544F397D9873FFCA297AF32116EC504C1D3B966EDDC22DECB
Malicious:	false
Reputation:	low
Preview:	....."[....161091..c..downloads..events..file..user..html..inc..invoice..po..revised..tech..users*.....161091.....c.....downloads.....events.....file.....user.....html.....inc.....invoice.....po.....revised.....tech.....users..2.....0.....1.....6.....9.....a.....c.....d.....e.....f.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....w.....z...:w.....B..... .....*cfile:///C:/Users/user/Downloads/Tech%20Events%20Inc.%20PO%23%20161091%20&%20Invoice%20Revised.html2.:.....J.....!&-26?GO

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):	54912
Entropy (8bit):	0.10152593660697985
Encrypted:	false
SSDEEP:	12:xG9DWmpqLBj/2At7lf9f4pAvn9t404nMWQA9L0gBQZ8fO5GMr:MnqLBdthfd4S4lbN0gTfs
MD5:	5D618A108AA2034E399EB826320514AF
SHA1:	EF966A6AE891108465A4773CDEF461457D28C04A
SHA-256:	E517A0299B5F7A706B1A6B8F2F1EF4C865572DDF1416E5258DB280055812B7FB
SHA-512:	A0CD2B8945FBE94EC8A2065E7E27A269E7849273482590A68C1C2BCD63B8921DB8C13877869F95F57158F2B921241E332B6F99AFF19DC1581B683EC45E0BBEFE
Malicious:	false
Reputation:	low
Preview:	.....+=.` ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.24152726285211
Encrypted:	false
SSDEEP:	3:tUK6WW3ASWFv:mcSg
MD5:	36D4F59E6CB2112A3D2148E5A251F974
SHA1:	88E7E88B0B7C6FD897F335B3A914BFC4561547FE
SHA-256:	77ACF4A1F4F684195A82BEF639927A45FB0706994048AEF9A156A6B2754C0DC7
SHA-512:	1D07C7BBB70CB4D84B2BCEF2F713AA15A1D2595DF6D65281B0D3F86839604B8C781231A67FF000A667D71AAE405258661E6049911403971F7785DF04452470C4
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:59.441 428 Delete type=3 #1.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session, (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1766
Entropy (8bit):	3.570070320831956
Encrypted:	false
SSDEEP:	24:34StylrlA5l1tZmgFbrr+6yeAfLHkaS6Ow/Le6K+6yeAQC0lL:34RxiMg86y3l5rwTn6yY1L
MD5:	5CBA1E07CCCE09F2829EC476F58A381B
SHA1:	908481703378623A74A6F484B32D4205F72A0420
SHA-256:	6267D2B67AD2B494DED95ACF6EB89FB191AD3D6C774BFEFDBD62DDEFDD115D6A
SHA-512:	4E94E3A292CFEA711D13AE09FA59744681030F88E33F7119B5CA72567A3AB8BF0BF4F78E33E06F8D85CCDD8877C74BB250D3EE46D0F9D3150358B1F01CCC4C4B
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...2aa2da33_64dd_48c2_90f1_406dd562921e.....Ffp.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....!.....1.,.....$...aac8d093_1794_435a_9e15_550b0c14e192.....+.....c...file:///C:/Users/user/Downloads/Tech%20Events%20Inc.%20PO%23%20161091%20&%20Invoice%20Revised.html.....M.i.c.r.o.s.o.f.t. .W.o.r.d. .O.n.l.i.n.e...t...p.....h.....h.....`.....0.....8.....3.....3.....c...f.i.l.e.:././/.C.:./.U.s.e.r.s./.h.a.r.d.z./.D.o.w.n.l.o.a.d.s./.T.e.c.h.%.2.0.E.v.e.n.t.s.%.2.0.I.n.c...%.2.0.P.O.%.2.3.%.2.0.1.6.1.0.9.1.%.2.0.&.%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabske (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):	5.46772939653888
Encrypted:	false
SSDEEP:	48:oxcGyja7UMK8dbx3H+bQSefgGRNrS0U9RdiN9v:oma7UMJdbx3H+bQ5fgGrrS09
MD5:	5EDD214CB1CB221BBE1ED4596119DB1B
SHA1:	4BB0AE6BB04ADA044C6C76811938ABDB35298658
SHA-256:	3B856AE5E44FEDF833BE8A271AD99FA17A38F9439DECB3C307CD4D08E77DD68B
SHA-512:	F6A38CE37B4F6B7837250B817C77126C254A57A52FA52A2163EED6B11562EA2801E13565D71283002D1FFA4BB38619805DCDA4E1B05217D1CBE8EE1FA9EEEEC
Malicious:	false
Reputation:	low
Preview:	{..`...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..994526000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 23:16:05.02][INFO][mr.Init] MR instance ID: 78d691ff-bfa8-4de4-ac76-4f253cc3c8ad\n","[2021-08-03 23:16:05.02][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 23:16:05.02][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 23:16:05.02][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 23:16:05.02][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 23:16:05.03][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 23:16:05.03][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.180147845792007
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SSDEEP:	6:mJEvAVq2PWXp+N23iKKdK8a2jMGIFUtpalNAgZmwPaQpAIkwOWXp+N23iKKdK8as:tAva5Kk8EFUtpOX/PnZ5f5Kk8bJ
MD5:	082B079A0E4F1E82ADDD0DA4D4B28D5E
SHA1:	0A3ECA8E5B4478245F99B27A516E268A3F30309C
SHA-256:	7D6DD7D93F723AA1F5F25EACC622439E3329230278AF72DAE3120E670FA60164
SHA-512:	EC90852FD2C0B102EFD9A07E4BD34BEB1CC4BA62DA35AC1D8698EFEBD080CBB04B047EB26DE3163A88154E9F26EE88F795208FFF45B42AC049C5E70DBB45C7DE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.328 14d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:15:53.334 14d0 Recovering log #3.2021/08/03-23:15:53.337 14d0 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.oldTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.180147845792007
Encrypted:	false
SSDEEP:	6:mJEvAVq2PWXp+N23iKKdK8a2jMGIFUtpalNAgZmwPaQpAIkwOWXp+N23iKKdK8as:tAva5Kk8EFUtpOX/PnZ5f5Kk8bJ
MD5:	082B079A0E4F1E82ADDD0DA4D4B28D5E
SHA1:	0A3ECA8E5B4478245F99B27A516E268A3F30309C
SHA-256:	7D6DD7D93F723AA1F5F25EACC622439E3329230278AF72DAE3120E670FA60164
SHA-512:	EC90852FD2C0B102EFD9A07E4BD34BEB1CC4BA62DA35AC1D8698EFEBD080CBB04B047EB26DE3163A88154E9F26EE88F795208FFF45B42AC049C5E70DBB45C7DE
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.328 14d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:15:53.334 14d0 Recovering log #3.2021/08/03-23:15:53.337 14d0 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\MANIFEST-000002	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	4.948758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVqU0blS:oO7iblS
MD5:	22BF0E81636B1B45051B138F48B3D148
SHA1:	56755D203579AB356E5620CE7E85519AD69D614A
SHA-256:	E292F241DAAFC3DF90F3E2D339C61C6E2787A0D0739AAC764E1EA9BB8544EE97
SHA-512:	A4CF1F5C74E0DF85DDA8750BE9070E24E19B8BE15C6F22F0C234EF8423EF9CA3DB22BA9EF777D64C33E8FD49FADA6FCCA26C1A14BA18E8472370533A1C65DD0
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State3} (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):	3019
Entropy (8bit):	4.880735283194612
Encrypted:	false
SSDEEP:	48:Y2TntwXGDHz5spEITspEsRLspD8pRSRWz5e86NlsW8zsI6q7s8MHVh8VsNyKse3H:JTnOXGDHzaEIUEsSDoRHz5j6NtqxFGVf
MD5:	CCC27DDFB9FA66C28D217F604FA5878B
SHA1:	DF2A1DEFE9B0F06486FC5CA1CD0991A3D26C19C5
SHA-256:	ACC7E231EF79C96D20DD00A6A0D5DB098C126F678CD92581FDEC452A9F9F02DC
SHA-512:	CB15E309A658B6C0BE59B358D84CF34F28794844B636DCCC576331342018AB7FB967925CC92830E73BA0EA273FE6AD2A1D5FE21B9DE13F0516EECF0DC624893
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State3} (copy)	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.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":"13275123358383833","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275123358387738","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expira

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State44 (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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

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):	331
Entropy (8bit):	5.272074329837845
Encrypted:	false
SSDEEP:	6:mN1R+q2PWXp+N23iKKdKgXz4rRIFUtpeeZmwPe7DtVkwOWXp+N23iKKdKgXz4q8d:Dva5KkgXiuFUtpL/PyDT5f5KkgX2J
MD5:	287DEC59D5D5813F9C916905DC3D618B
SHA1:	C6EA1D757A02AB54672A18DD03BCCD2541B41C54
SHA-256:	91CF403B18C0E88E29CDBCE07979465B283EDF956861CAAAC906687A5749C2DC
SHA-512:	8724180279BB3A8387FAA1918BCD80895F75A0BE344CB04EE855ED34C89A9976E4CEAF7D3A351E02D42733533B409B5DE58831418472E3965BC09580F7E35D20
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.746 428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-23:15:53.747 428 Recovering log #3.2021/08/03-23:15:53.748 428 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.272074329837845
Encrypted:	false
SSDEEP:	6:mN1R+q2PWXp+N23iKKdKgXz4rRIFUtpeeZmwPe7DtVkwOWXp+N23iKKdKgXz4q8d:Dva5KkgXiuFUtpL/PyDT5f5KkgX2J
MD5:	287DEC59D5D5813F9C916905DC3D618B
SHA1:	C6EA1D757A02AB54672A18DD03BCCD2541B41C54
SHA-256:	91CF403B18C0E88E29CDBCE07979465B283EDF956861CAAAC906687A5749C2DC
SHA-512:	8724180279BB3A8387FAA1918BCD80895F75A0BE344CB04EE855ED34C89A9976E4CEAF7D3A351E02D42733533B409B5DE58831418472E3965BC09580F7E35D20
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.746 428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-23:15:53.747 428 Recovering log #3.2021/08/03-23:15:53.748 428 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5487
Entropy (8bit):	5.179934973927058
Encrypted:	false
SSDEEP:	96:nYCmTP9/SHgoeXcKIkok0JCKL8r0bOTQVuwn:nYCs9aHaXcN4KGe
MD5:	AEE7807F188FE5DAD2567AB56E8491DA
SHA1:	4462B59F806DF15D567AFA6DAC4163E87232486E
SHA-256:	32DA22C7CC81721EEC0873D1C400E1AC67C0D557BA00AD0155006ABDEC9BAF00
SHA-512:	69A5DACE79D1EED16C5058DC775934DDE0DF148AC648F9BC3D7B278E89F8E6EC9322AB56386C67FAEE41698C9E41D82537BCA44093A35BE36D94B836917B53 4
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272531353690745","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"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}},"co untryid_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","7355378"],"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):	57344
Entropy (8bit):	1.483732863099397
Encrypted:	false
SSDEEP:	192:wIElwQF8mpcS7R1odVX1oGTQUaSIElwQF8mpcSL+2R1odVQ+K1oGTEka1:KjwllQjejwYlET1
MD5:	857F398BF10F7090822AF384EC265CFD
SHA1:	BDAA2EE8156D13EE36ADFB74DF16178F010BF0DB
SHA-256:	3262E9113A19BE73573FD10A4C023237B4F4CCF1AA47574FD237CEA3A7873349
SHA-512:	A05685A693C5B330243F879806E0897D42748A4477DC68810DE590C3B1626A29016843EE43C3A1FECBF0FF8C781EF7F24B814FF4DD208B561BDE3D711DF719B6
Malicious:	false
Reputation:	low
Preview:	SQLite format 3......@ ....C..........g...^.........j... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	58504
Entropy (8bit):	1.0182091431778943
Encrypted:	false
SSDEEP:	192:ohIElwQF8mpcSm1oGT8YR1odVIa0CxIElwQF8mpcSZf:osl9jwX0CRf
MD5:	64838C0619A512BFB3B219055A32DA32
SHA1:	C65B28B5582A15D480B36B42C35163CB70B17903
SHA-256:	DF602F988A37F06D50D3B19B50977A6233031639BEAFF91384D3B162CB6FBA42
SHA-512:	5595020DA6FE947C9C65453F912A9C6013DCAA7032DB04817B15858C09B20FEA6205DB0E4F1F8465B2171E43836E2F8FB70D2F2808179F46326E8090447FD203
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):	22596
Entropy (8bit):	5.53574084969226
Encrypted:	false
SSDEEP:	384:E30tbLlyKvX61kXqKf/pUZNCgVLH2HfDArU6HGRXnTjmNqVX4/:nLld/61kXqKf/pUZNCgVLH2HfsrUKGRw

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
MD5:	1CFC2B1CE682F20C2B0E0E76AA65DBBE
SHA1:	EF18F0FAC634ED44001B6B6AC5157F9C45D9F924
SHA-256:	ACD4F6E26E236C56F051BBC9DBF8011D83CEEE052ED039C896DAACD463BD487E
SHA-512:	455E6EF47D9F3F1F5ACDA9BAF3E0A9565CB5458E70C263073F53E1410AF1BE76BC03570619EEF3F9A74913C2A53BB7A4138421EE04E34850EF8138251744F53B
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":"13272531353262882","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferencese (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):	19007
Entropy (8bit):	5.5668028644874115
Encrypted:	false
SSDEEP:	384:E30teLlyKvX61kXqKf/pUZNCgVLH2HfDArU6HGfsr5VX44:yLld/61kXqKf/pUZNCgVLH2HfsrUKGfO
MD5:	B946A1265555CD122DF860A025399EA1
SHA1:	77690C7D54E5B99630AB4EADCB78ACEBF605F443
SHA-256:	AD25AE1FEA09EB37F8D01E3872357726E1625C2CA00E2762A3283103ADFF928A
SHA-512:	55F58E0222D1DDCC2F3DF8788335642165E95F30F0B3E792BA6DEFB19FF621A5E5FB8843A892390466A80E6C682056063F9B1642BB41E746E7317171AE9FD460
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":"13272531353262882","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferenceswe (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):	5.535847986061201
Encrypted:	false
SSDEEP:	384:E30tbLlyKvX61kXqKf/pUZNCgVLH2HfDArU6HGIXnTjmr3qVX4B:nLld/61kXqKf/pUZNCgVLH2HfsrUKGIg
MD5:	48DAAF38CA21FF574F454101E7ED6010
SHA1:	BA88610D09A92DB9B66DA338220A596DDEBBB20E
SHA-256:	03F2CC5A7B05D22017D317759A304E377041BADB05F47679A5D17A6BE7B55ED4
SHA-512:	2360A6A6C0041B87169D5C95F558228F8EC503ABA172582880E271A6D64F5329857DB820E48DDC34D2B33AD72839BB38892DC2BAD09EB25652B3A36570D433D5
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":"13272531353262882","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.150235060066453
Encrypted:	false
SSDEEP:	6:mQcAq2PWXp+N23iKKdKrQMxIFUtpuZmwPCkwOWXp+N23iKKdKrQMFLJ:TcAva5KkCFUtpu/PC5f5KktJ
MD5:	859C9B92B254A8E22679BF13A730F90A
SHA1:	55047F2CF8DE45EA357A48103E4EFBD88151945C
SHA-256:	354FB57F75994968035841D9F01DBD6D7FCD36F89533B00A9F5B8ADBA4AB4575
SHA-512:	AF31832C5F86D5F5F869C9AE86B4187FF87D723FD6FA5DDB28D7FE20AFF07E16A3E1395671CBB9AA4255B982ADC0CC397DBA5F9F0ECF8FAD63E2883D1F9A05BC
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.601 e90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-23:15:53.603 e90 Recovering log #3.2021/08/03-23:15:53.603 e90 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.150235060066453
Encrypted:	false
SSDEEP:	6:mQcAq2PWXp+N23iKKdKrQMxIFUtpuZmwPCkwOWXp+N23iKKdKrQMFLJ:TcAva5KkCFUtpu/PC5f5KktJ
MD5:	859C9B92B254A8E22679BF13A730F90A
SHA1:	55047F2CF8DE45EA357A48103E4EFBD88151945C
SHA-256:	354FB57F75994968035841D9F01DBD6D7FCD36F89533B00A9F5B8ADBA4AB4575
SHA-512:	AF31832C5F86D5F5F869C9AE86B4187FF87D723FD6FA5DDB28D7FE20AFF07E16A3E1395671CBB9AA4255B982ADC0CC397DBA5F9F0ECF8FAD63E2883D1F9A05BC
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.601 e90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-23:15:53.603 e90 Recovering log #3.2021/08/03-23:15:53.603 e90 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.210715326012851
Encrypted:	false
SSDEEP:	6:mSkt+q2PWXp+N23iKKdK7Uh2ghZIFUtpD9ZmwP1BVkwOWXp+N23iKKdK7Uh2gnLJ:dkova5KklhHh2FUtpD9/P1P5f5KklhHd
MD5:	9D61BC1BB7924343E85E3D18890226CD
SHA1:	12D4234ABB0F95F9910EDC5CB4B0445DA7AAD3E0
SHA-256:	1CB3EB64843A09AE7C37944E322A876D791724F12ED95F160FE4741940D470B7
SHA-512:	CB29C101031B96AEE33ABCC1BFBB8FCB5988A3562BD6E9467D6BCD8484B7DE793E7E837DBF73A3B81906F167C4F3A1C8DA07D6D1D74FD2CD25A8A3CBBCFB7DCA
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.268 968 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-23:15:53.281 968 Recovering log #3.2021/08/03-23:15:53.287 968 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.210715326012851
Encrypted:	false
SSDEEP:	6:mSkt+q2PWXp+N23iKKdK7Uh2ghZIFUtpD9ZmwP1BVkwOWXp+N23iKKdK7Uh2gnLJ:dkova5KklhHh2FUtpD9/P1P5f5KklhHd
MD5:	9D61BC1BB7924343E85E3D18890226CD
SHA1:	12D4234ABB0F95F9910EDC5CB4B0445DA7AAD3E0
SHA-256:	1CB3EB64843A09AE7C37944E322A876D791724F12ED95F160FE4741940D470B7
SHA-512:	CB29C101031B96AEE33ABCC1BFBB8FCB5988A3562BD6E9467D6BCD8484B7DE793E7E837DBF73A3B81906F167C4F3A1C8DA07D6D1D74FD2CD25A8A3CBBCFB7DCA
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.268 968 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/08/03-23:15:53.281 968 Recovering log #3.2021/08/03-23:15:53.287 968 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\1a7f173a-6c6e-4132-af0a-621b557ce5c6.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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.285603715111434
Encrypted:	false
SSDEEP:	6:mY3Aq2PWXp+N23iKKdKusNpV/2jMGIFUtp0ZZmwP7fDkwOWXp+N23iKKdKusNpV0:v3Ava5KkFFUtpI/P7L5f5KkOJ
MD5:	A2E45D7531ECE4359B9542E37BD2A40F
SHA1:	3ACF68E469D0CE7033DF47E8D1DDF8D27355AD93

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
SHA-256:	C81AC9D53D5197F73C4FFD418597117674FA149BA3C525443CF9327A747E07BA
SHA-512:	E7AF8F9781621B8F4AF49236E522EEBEC49356CC1DDA374D3A76967F0F69CFF63442221C904DB931D65A3EBA549810DA4AAAF2758240368CDC10458398D134C
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.671 e90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:15:53.674 e90 Recovering log #3.2021/08/03-23:15:53.675 e90 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.285603715111434
Encrypted:	false
SSDEEP:	6:mY3Aq2PWXp+N23iKKdKusNpV/2jMGIFUtp0ZZmwP7fDkwOWXp+N23iKKdKusNpV0:v3Ava5KkFFUtpI/P7L5f5KkOJ
MD5:	A2E45D7531ECE4359B9542E37BD2A40F
SHA1:	3ACF68E469D0CE7033DF47E8D1DDF8D27355AD93
SHA-256:	C81AC9D53D5197F73C4FFD418597117674FA149BA3C525443CF9327A747E07BA
SHA-512:	E7AF8F9781621B8F4AF49236E522EEBEC49356CC1DDA374D3A76967F0F69CFF63442221C904DB931D65A3EBA549810DA4AAAF2758240368CDC10458398D134C
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.671 e90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:15:53.674 e90 Recovering log #3.2021/08/03-23:15:53.675 e90 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent 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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.300894557371995
Encrypted:	false
SSDEEP:	6:mN/DM+q2PWXp+N23iKKdKusNpqz4rRIFUtpezLSgZmwPexGDMVkwOWXp+N23iKKi:YM+va5KkmiuFUtp6b/PnMV5f5Kkm2J
MD5:	2074BB5F1BAE00CCD94AD9C641AB5BB8
SHA1:	2B85CAA830EA3A532F18049732C13DBA23DA3E7B
SHA-256:	672FB030948A3DFB78976C1742FF28C464620266DE877B672243772BECB930E9
SHA-512:	BB34FB63CDE3B01301E8B15EC53CA35C5CC1DB3C51D5C627115A1C28B59FED828A1AD7B46CA4C54DCD257EDD2542B2E19128B4C61B3465DFAB4AACE550B877F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.736 5fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:15:53.740 5fc Recovering log #3.2021/08/03-23:15:53.742 5fc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.300894557371995
Encrypted:	false
SSDEEP:	6:mN/DM+q2PWXp+N23iKKdKusNpqz4rRIFUtpezLSgZmwPexGDMVkwOWXp+N23iKKi:YM+va5KkmiuFUtp6b/PnMV5f5Kkm2J
MD5:	2074BB5F1BAE00CCD94AD9C641AB5BB8
SHA1:	2B85CAA830EA3A532F18049732C13DBA23DA3E7B
SHA-256:	672FB030948A3DFB78976C1742FF28C464620266DE877B672243772BECB930E9
SHA-512:	BB34FB63CDE3B01301E8B15EC53CA35C5CC1DB3C51D5C627115A1C28B59FED828A1AD7B46CA4C54DCD257EDD2542B2E19128B4C61B3465DFAB4AACE550B877F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.736 5fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:15:53.740 5fc Recovering log #3.2021/08/03-23:15:53.742 5fc 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):	415
Entropy (8bit):	5.23122784633012
Encrypted:	false
SSDEEP:	6:mKVQAq2PWXp+N23iKKdKusNpZQMxIFUtpbVvZmwPbVezkwOWXp+N23iKKdKusNpB:LVQAva5KkMFUtpbVv/PbVG5f5KkTJ
MD5:	87ECE11BBD4FB64CA182F7584B1B0AC0
SHA1:	46041B6606EBF9AA5E40FAB74032AFB5EFFDA491
SHA-256:	2D1D7A933A99E1BDE98B155E902DECD89F7958C015D5BE8FF47E61C9F5AB7579
SHA-512:	85EDFCD9B98D481C626A617DC6403BEDD2591688E70BE8103369A8D4B345DA3682F66D21E9E5D371C7D3DEE812B26E9B9AC00FDF5B6713581BCE62B44109EC
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:12.041 420 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-23:16:12.042 420 Recovering log #3.2021/08/03-23:16:12.043 420 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.oldga (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.23122784633012
Encrypted:	false
SSDEEP:	6:mKVQAq2PWXp+N23iKKdKusNpZQMxIFUtpbVvZmwPbVezkwOWXp+N23iKKdKusNpB:LVQAva5KkMFUtpbVv/PbVG5f5KkTJ
MD5:	87ECE11BBD4FB64CA182F7584B1B0AC0
SHA1:	46041B6606EBF9AA5E40FAB74032AFB5EFFDA491

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.oldga (copy)	
SHA-256:	2D1D7A933A99E1BDE98B155E902DECD89F7958C015D5BE8FF47E61C9F5AB7579
SHA-512:	85EDFCD9B98D481C626A617DC6403BEDD2591688E70BE8103369A8D4B345DA3682F66D21E9E5D371C7D3DEE812B26E9B9AC00FDF5B6713581BCE62B44109EC C
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:12.041 420 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\ def\Session Storage/MANIFEST-000001.2021/08/03-23:16:12.042 420 Recovering log #3.2021/08/03-23:16:12.043 420 Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\7c113c4e-18f4-469a-8717-2d32ada07747.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):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","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
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):	427
Entropy (8bit):	5.1850689866458035
Encrypted:	false
SSDEEP:	12:KOva5KkkGHArBFUtp1X/Ps5f5KkkGHAryJ:/a5KkkGgPgHWf5KkkGga
MD5:	99E161EE588470C71AD8D19CD3483959
SHA1:	AF2C09F61AA3A4E8F9229887831C5D85D56B15E4
SHA-256:	D013C03AA1B929E83506B61FAC2215B57D9185F4F2506B11E113AF30F79C5EA8
SHA-512:	FC844D7EDB9E446EB8B3D7CF8E897895DD08FDEE48559BDA180A8BF4CAB681EA244BF43780F557A195B42AAE79E7ECBC2ECACD62172638E41A0421C28CDCA 2EB
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.433 428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:16:02.438 428 Recovering log #3.2021/08/03-23:16:02.440 428 Reusing old log C:\Users\user\AppD ata\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.1850689866458035
Encrypted:	false
SSDEEP:	12:KOva5KkkGHArBFUtp1X/Ps5f5KkkGHAryJ:/a5KkkGgPgHWf5KkkGga
MD5:	99E161EE588470C71AD8D19CD3483959
SHA1:	AF2C09F61AA3A4E8F9229887831C5D85D56B15E4
SHA-256:	D013C03AA1B929E83506B61FAC2215B57D9185F4F2506B11E113AF30F79C5EA8
SHA-512:	FC844D7EDB9E446EB8B3D7CF8E897895DD08FDEE48559BDA180A8BF4CAB681EA244BF43780F557A195B42AAE79E7ECBC2ECACD62172638E41A0421C28CDCA 2EB
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.433 428 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-23:16:02.438 428 Recovering log #3.2021/08/03-23:16:02.440 428 Reusing old log C:\Users\user\AppD ata\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):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.231030064997892
Encrypted:	false
SSDEEP:	12:VOva5KkkGHArqiuFUtpP/PFR5f5KkkGHArq2J:VMa5KkkGgCg/f5KkkGg7
MD5:	05987742377B8FCF500CE6A5ED4EC120
SHA1:	45F02099CD7E3856AACD095682AFD5587368F66B
SHA-256:	7B4AAA2BC50BDF29616D7AE7D702E7C787DC1A612747EB5D3A096DB7E6C51893
SHA-512:	1E9FF92F2169515F7D4F3EB83B3D385DE44521E878D6DBB8F31B000B84941D47155241C95C235FC7AA984E518002E8BA226684C4879E8BDBD83BA89F50ED1C7
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.436 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/08/03-23:16:02.441 15d8 Recovering log #3.2021/08/03-23:16:02.443 15d8 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.oldnW (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.231030064997892
Encrypted:	false
SSDEEP:	12:VOva5KkkGHArqiuFUtpP/PFR5f5KkkGHArq2J:VMa5KkkGgCg/f5KkkGg7
MD5:	05987742377B8FCF500CE6A5ED4EC120

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

SHA1:	45F02099CD7E3856AACD095682AFD5587368F66B
SHA-256:	7B4AAA2BC50BDF29616D7AE7D702E7C787DC1A612747EB5D3A096DB7E6C51893
SHA-512:	1E9FF92F2169515F7D4F3EB83B3D385DE44521E878D6DBB8F31B000B84941D47155241C95C235FC7AA984E518002E8BA226684C4879E8BDBD83BA89F50ED1C7
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:02.436 15d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-23:16:02.441 15d8 Recovering log #3.2021/08/03-23:16:02.443 15d8 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):	415
Entropy (8bit):	5.192657818071155
Encrypted:	false
SSDEEP:	12:uOva5KkkGHArAFUtpRh/PR75f5KkkGHArfJ:uMa5KkkGgkg7ntf5KkkGgV
MD5:	33BD16C8E6740189A7D4706304CBD63D
SHA1:	D2557CC01294740148529FF0A5FBA574D5C46353
SHA-256:	0340957DDCAB0D8B0B889D14165F867CD8FB2E830CA59C979B7D22C3C40F396F
SHA-512:	6B593E978CE5F507BC9D586452AED4A25C1E96345EC65C32AC2664CEAD2380C10F889DA96F6CA5C87F640D70A571F96B1829F49BF4CB7AEB45FCEB65F8E3AD86
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:17.718 420 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-23:16:17.720 420 Recovering log #3.2021/08/03-23:16:17.720 420 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.192657818071155
Encrypted:	false
SSDEEP:	12:uOva5KkkGHArAFUtpRh/PR75f5KkkGHArfJ:uMa5KkkGgkg7ntf5KkkGgV
MD5:	33BD16C8E6740189A7D4706304CBD63D
SHA1:	D2557CC01294740148529FF0A5FBA574D5C46353
SHA-256:	0340957DDCAB0D8B0B889D14165F867CD8FB2E830CA59C979B7D22C3C40F396F
SHA-512:	6B593E978CE5F507BC9D586452AED4A25C1E96345EC65C32AC2664CEAD2380C10F889DA96F6CA5C87F640D70A571F96B1829F49BF4CB7AEB45FCEB65F8E3AD86
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old.c (copy)	
Preview:	2021/08/03-23:16:17.718 420 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-23:16:17.720 420 Recovering log #3.2021/08/03-23:16:17.720 420 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.218162804115324
Encrypted:	false
SSDEEP:	6:mJLvIq2PWXp+N23iKKdKpIFUtpazgZmwPaVkwOWXp+N23iKKdKa/WLJ:jva5KkmFUtpb/Pg5f5KkaUJ
MD5:	4234DFC56E29A98F2DCC5EE300001C03
SHA1:	C18DC511226023AD9520D9D02A4EA8015CFA5F67
SHA-256:	65CD267B8856B2A16B44B563CAA0F58E3DD6FEC5FE2B75054286AA3A0BB2B5DE
SHA-512:	0EE437B8AE0447CD39D6F7DA613BAB5167AD242A3992B8B2F9CC75BB6643D806F9DCED2A993E07C0E240C7ED22F7565A3495D6564049C129B18F00CCE3475E 7
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.319 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-23:15:53.323 f0 Recovering log #3.2021/08/03-23:15:53.326 f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LeveIDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.oldg (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.218162804115324
Encrypted:	false
SSDEEP:	6:mJLvIq2PWXp+N23iKKdKpIFUtpazgZmwPaVkwOWXp+N23iKKdKa/WLJ:jva5KkmFUtpb/Pg5f5KkaUJ
MD5:	4234DFC56E29A98F2DCC5EE300001C03
SHA1:	C18DC511226023AD9520D9D02A4EA8015CFA5F67
SHA-256:	65CD267B8856B2A16B44B563CAA0F58E3DD6FEC5FE2B75054286AA3A0BB2B5DE
SHA-512:	0EE437B8AE0447CD39D6F7DA613BAB5167AD242A3992B8B2F9CC75BB6643D806F9DCED2A993E07C0E240C7ED22F7565A3495D6564049C129B18F00CCE3475E 7
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:15:53.319 f0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-23:15:53.323 f0 Recovering log #3.2021/08/03-23:15:53.326 f0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LeveIDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Size (bytes):	399
Entropy (8bit):	5.302458910766631
Encrypted:	false
SSDEEP:	6:mKaq2PWXp+N23iKKdKks8Y5JKKhdIFUtp1ZmwPnkwOWXp+N23iKKdKks8Y5JKKTd:Dava5KkkOrsFUtp1/Pn5f5KkkOrzJ
MD5:	41E164C1F126C2D46094A573FEE07183
SHA1:	E865249DB7CD228C2E72C380DDDBAEF48ACC5837
SHA-256:	C7449B00AB2701A1A9F79F761CED91B0A8FC43E230B68BE726AD6417EED9D537
SHA-512:	6D97FCBD3CCC62665D8AEE01D27FB4FFD444E227AF9B0550696A0E6991746E4AA0E22EDC5970FA7D4D122738A9E88E2D54E3E60EFD52FEB8C8A8315CA4D09(12
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:05.008 420 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbm eomcjbeemfm/MANIFEST-000001.2021/08/03-23:16:05.011 420 Recovering log #3.2021/08/03-23:16:05.011 420 Reusing old log C:\Users\user\AppData\Local\Goog le\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.302458910766631
Encrypted:	false
SSDEEP:	6:mKaq2PWXp+N23iKKdKks8Y5JKKhdIFUtp1ZmwPnkwOWXp+N23iKKdKks8Y5JKKTd:Dava5KkkOrsFUtp1/Pn5f5KkkOrzJ
MD5:	41E164C1F126C2D46094A573FEE07183
SHA1:	E865249DB7CD228C2E72C380DDDBAEF48ACC5837
SHA-256:	C7449B00AB2701A1A9F79F761CED91B0A8FC43E230B68BE726AD6417EED9D537
SHA-512:	6D97FCBD3CCC62665D8AEE01D27FB4FFD444E227AF9B0550696A0E6991746E4AA0E22EDC5970FA7D4D122738A9E88E2D54E3E60EFD52FEB8C8A8315CA4D09(12
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:05.008 420 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbm eomcjbeemfm/MANIFEST-000001.2021/08/03-23:16:05.011 420 Recovering log #3.2021/08/03-23:16:05.011 420 Reusing old log C:\Users\user\AppData\Local\Goog le\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2046
Entropy (8bit):	5.600799189528797
Encrypted:	false
SSDEEP:	48:Yj4VwUvgEx1jrU76UUhUeURKUnqPeUer2UefpwUPsYUeuSd2wU0nNwUgS2Uenw:mXUvX1HUeUUDURKUqPeU9UEqUEYUeumP
MD5:	9B864DBE569FAA7A122C85C3ADA9DAAC
SHA1:	97BD0EDD63818CC84C82F2EF588048219D5E2021
SHA-256:	96EFD410F2C66EED51AECC78665CC13373849FB94FFED78BCEE52D9088091025
SHA-512:	98340F751F4661B4F915F2E5A518EB743282D620C7C99002795D6958932AF128FD5AD05B49DEA44B204B988AF6412A161F7A91B99D3F45A579FD48EB6B9C3A71
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1643837761.361938,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains" :false,"sts_observed":1628057761.361943},{"expiry":1628058061.362795,"host":"GGApl7UvK2CYbnERSYSoCoHcYUdXwzjjAzjTFCIkpg0=","mode":"force-https","sts_i nclude_subdomains":false,"sts_observed":1628057761.362799},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"f orce-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1659593761.366166,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt 4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628057761.36617},{"expiry":1659593761.377536,"host":"nAuqgR4iEWti7SOdT3UHP l6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628057761.377541},{"expiry":1633014092.4175,"host":"0J7rA WV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:/OTo0S6w:/OTpSb
MD5:	68BE685AEFC5265FC658E2243E31E121
SHA1:	A896F8B399A8A95BD4BF39396A6B43FC9220B8F7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
SHA-256:	C1547BF022CA81FF2EB039C96BEC75C4F854EEC56EF617E88E3A21D5BC304125
SHA-512:	B3811B0AF2BF9191E9ECD23245EB5988B8B34F1FFE60F0D8147A5D4BCC499007A7E79E063C7E7AFA0B706AB07A1326B16B6C15DED301F255731F006BEBFB6352
Malicious:	false
Reputation:	low
Preview:	.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bfe09756-85ae-47cf-b286-22464b42090d.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):	2046
Entropy (8bit):	5.600799189528797
Encrypted:	false
SSDEEP:	48:Yj4VwUvgEx1jrU76UUhUeURKUnqPeUer2UefpwUPsYUeuSd2wU0nNwUgS2Uenw:mXUvX1HUeUUDURKUqPeU9UEqUEYUeumP
MD5:	9B864DBE569FAA7A122C85C3ADA9DAAC
SHA1:	97BD0EDD63818CC84C82F2EF588048219D5E2021
SHA-256:	96EFD410F2C66EED51AECC78665CC13373849FB94FFED78BCEE52D9088091025
SHA-512:	98340F751F4661B4F915F2E5A518EB743282D620C7C99002795D6958932AF128FD5AD05B49DEA44B204B988AF6412A161F7A91B99D3F45A579FD48EB6B9C3A71
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1643837761.361938,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628057761.361943},{"expiry":1628058061.362795,"host":"GGApl7UvK2CYbnERSYSoCoHcYUdXwzjjAzjTFCIkpg0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628057761.362799},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoealXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1659593761.366166,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628057761.36617},{"expiry":1659593761.377536,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628057761.377541},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ce8693e7-e6bb-4af8-a562-a675aeae98d8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.53574084969226
Encrypted:	false
SSDEEP:	384:E30tbLlyKvX61kXqKf/pUZNCgVLH2HfDArU6HGRXnTjmNqVX4/:nLld/61kXqKf/pUZNCgVLH2HfsrUKGRw
MD5:	1CFC2B1CE682F20C2B0E0E76AA65DBBE
SHA1:	EF18F0FAC634ED44001B6B6AC5157F9C45D9F924
SHA-256:	ACD4F6E26E236C56F051BBC9DBF8011D83CEEE052ED039C896DAACD463BD487E
SHA-512:	455E6EF47D9F3F1F5ACDA9BAF3E0A9565CB5458E70C263073F53E1410AF1BE76BC03570619EEF3F9A74913C2A53BB7A4138421EE04E34850EF8138251744F53B
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":"13272531353262882","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d8067526-5ee3-4f7e-8661-a60cba53725d.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):	19007
Entropy (8bit):	5.5668028644874115
Encrypted:	false
SSDEEP:	384:E30teLlyKvX61kXqKf/pUZNCgVLH2HfDArU6HGfsr5VX44:yLld/61kXqKf/pUZNCgVLH2HfsrUKGfO
MD5:	B946A1265555CD122DF860A025399EA1
SHA1:	77690C7D54E5B99630AB4EADCB78ACEBF605F443
SHA-256:	AD25AE1FEA09EB37F8D01E3872357726E1625C2CA00E2762A3283103ADFF928A
SHA-512:	55F58E0222D1DDCC2F3DF8788335642165E95F30F0B3E792BA6DEFB19FF621A5E5FB8843A892390466A80E6C682056063F9B1642BB41E746E7317171AE9FD460
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d8067526-5ee3-4f7e-8661-a60cba53725d.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":"13272531353262882","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\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.468550185085849
Encrypted:	false
SSDEEP:	3:tUK6wRUVu5lyZmwv3lwRScFCWSV8slwRdFhSWGv:mBW1ZmwP6jVvLetv
MD5:	F5487F9E105D643ABA3AACABA7C426B4
SHA1:	5AA1188A05AD7DD9186A7EDE96EA07A788DD532B
SHA-256:	14B620D3DBFDAA3D4E137261F6D681392C02287121362CE40A80BDE86EC0806D
SHA-512:	4CCE6A97297A52A6B1D38D642D1F955AC16E055E2792FDE71DE0F9B634FA3A59BDCB0D91A4EDCE7A94686E932E11625FAC07461657BC01A302BD0F513C1D8DE1
Malicious:	false
Reputation:	low
Preview:	2021/08/03-23:16:01.410 1a14 Recovering log #3.2021/08/03-23:16:01.479 1a14 Delete type=0 #3.2021/08/03-23:16:01.480 1a14 Delete type=3 #2.

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 23:15:57.983186007 CEST	192.168.2.3	8.8.8.8	0x90ba	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:15:57.995042086 CEST	192.168.2.3	8.8.8.8	0x3542	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:15:57.998364925 CEST	192.168.2.3	8.8.8.8	0xdec	Standard query (0)	aerialligh tingandelectric-my.sharepoint.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.092760086 CEST	192.168.2.3	8.8.8.8	0x7a86	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.094963074 CEST	192.168.2.3	8.8.8.8	0x2c60	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.132877111 CEST	192.168.2.3	8.8.8.8	0x6ee7	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.135799885 CEST	192.168.2.3	8.8.8.8	0x11dc	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.156285048 CEST	192.168.2.3	8.8.8.8	0x4e7	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.166704893 CEST	192.168.2.3	8.8.8.8	0x2aba	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:02.604135036 CEST	192.168.2.3	8.8.8.8	0xbae7	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:02.608442068 CEST	192.168.2.3	8.8.8.8	0x8c10	Standard query (0)	i.gyazo.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:02.613228083 CEST	192.168.2.3	8.8.8.8	0xde81	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:05.079418898 CEST	192.168.2.3	8.8.8.8	0xa8d8	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:05.082071066 CEST	192.168.2.3	8.8.8.8	0xe959	Standard query (0)	i.imgur.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 23:15:58.031929016 CEST	8.8.8.8	192.168.2.3	0x3542	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 23:15:58.042345047 CEST	8.8.8.8	192.168.2.3	0x90ba	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:15:58.042345047 CEST	8.8.8.8	192.168.2.3	0x90ba	No error (0)	clients.l.google.com		216.58.208.174	A (IP address)	IN (0x0001)
Aug 3, 2021 23:15:58.086045980 CEST	8.8.8.8	192.168.2.3	0xdec	No error (0)	aerialligh tingandelectric-my.sharepoint.com	aeriallightingandelectric.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:15:58.086045980 CEST	8.8.8.8	192.168.2.3	0xdec	No error (0)	aerialligh tingandelectric.sharepoint.com	1491-ipv4e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 23:15:58.086045980 CEST	8.8.8.8	192.168.2.3	0xdec	No error (0)	1491-ipv4e.clump.prod.aa-rt.sharepoint.com	20355-ipv4e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:15:58.086045980 CEST	8.8.8.8	192.168.2.3	0xdec	No error (0)	20355-ipv4e.farm.prod.aa-rt.sharepoint.com	20355-ipv4e.farm.prod.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:16:01.117602110 CEST	8.8.8.8	192.168.2.3	0x7a86	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:16:01.129926920 CEST	8.8.8.8	192.168.2.3	0x2c60	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.129926920 CEST	8.8.8.8	192.168.2.3	0x2c60	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.164985895 CEST	8.8.8.8	192.168.2.3	0x6ee7	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:16:01.168402910 CEST	8.8.8.8	192.168.2.3	0x11dc	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.168402910 CEST	8.8.8.8	192.168.2.3	0x11dc	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.196284056 CEST	8.8.8.8	192.168.2.3	0x4e7	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:16:01.201647997 CEST	8.8.8.8	192.168.2.3	0x2aba	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:16:01.201647997 CEST	8.8.8.8	192.168.2.3	0x2aba	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:01.412435055 CEST	8.8.8.8	192.168.2.3	0x1d87	No error (0)	gstaticadssl.l.google.com		216.58.198.3	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:02.641223907 CEST	8.8.8.8	192.168.2.3	0xbae7	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:16:02.646187067 CEST	8.8.8.8	192.168.2.3	0x8c10	No error (0)	i.gyazo.com		104.19.142.111	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:02.646187067 CEST	8.8.8.8	192.168.2.3	0x8c10	No error (0)	i.gyazo.com		104.19.143.111	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:02.653650045 CEST	8.8.8.8	192.168.2.3	0xde81	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:16:02.653650045 CEST	8.8.8.8	192.168.2.3	0xde81	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)
Aug 3, 2021 23:16:05.113820076 CEST	8.8.8.8	192.168.2.3	0xa8d8	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:16:05.115423918 CEST	8.8.8.8	192.168.2.3	0xe959	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 23:16:05.115423918 CEST	8.8.8.8	192.168.2.3	0xe959	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	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 23:16:01.240935087 CEST	151.101.112.193	443	192.168.2.3	49746	CN=*.imgur.com, O="Imgur, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Mar 16 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Aug 3, 2021 23:16:05.161730051 CEST	151.101.112.193	443	192.168.2.3	49765	CN=*.imgur.com, O="Imgur, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Mar 16 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5284 Parent PID: 4232

General

Start time:	23:15:52
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://aeriallightingandelectric-my.sharepoint.com/:u:/g/personal/khardy_aerialelectric_com/ESDO6oK0Y2FPjomZ3thjzpYB912czBooPXA5DhMbhXvPhA?download=1'
Imagebase:	0x7ff77b960000
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: 4244 Parent PID: 5284

General

Start time:	23:15:54
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1736,4776280355382224090,2163248144403128918,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1792 /prefetch:8
Imagebase:	0x7ff77b960000
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: 6600 Parent PID: 5284

General

Start time:	23:16:00
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=quarantine.mojom.Quarantine --field-trial-handle=1736,4776280355382224090,2163248144403128918,131072 --lang=en-US --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=4608 /prefetch:8
Imagebase:	0x7ff77b960000
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