ID: 491031
Cookbook: browseurl.jbs
Time: 05:07:16
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

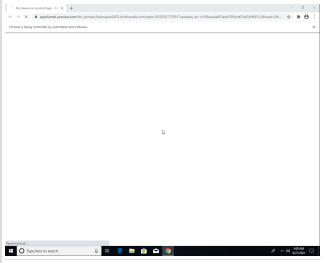
Windows Analysis Report https://2c7.ir/4sv4E

Overview

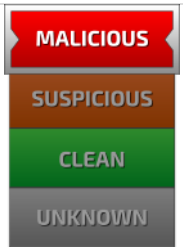
General Information

Sample URL:	http://https://2c7.ir/4sv4E
Analysis ID:	491031
Infos:	

Most interesting Screenshot:



Detection



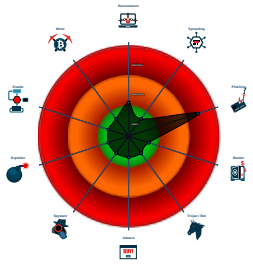
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Misleading page title found
- Yara detected HtmlPhish10
- Antivirus detection for URL or domain
- Invalid 'forgot password' link found
- HTML body contains low number of …
- Found iframes
- No HTML title found
- Form action URLs do not match mai…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6832 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://2c7.ir/4sv4E' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7036 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,16086817351805558034,16500979573986469014,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1684 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5580 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1560,16086817351805558034,16500979573986469014,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=3108 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

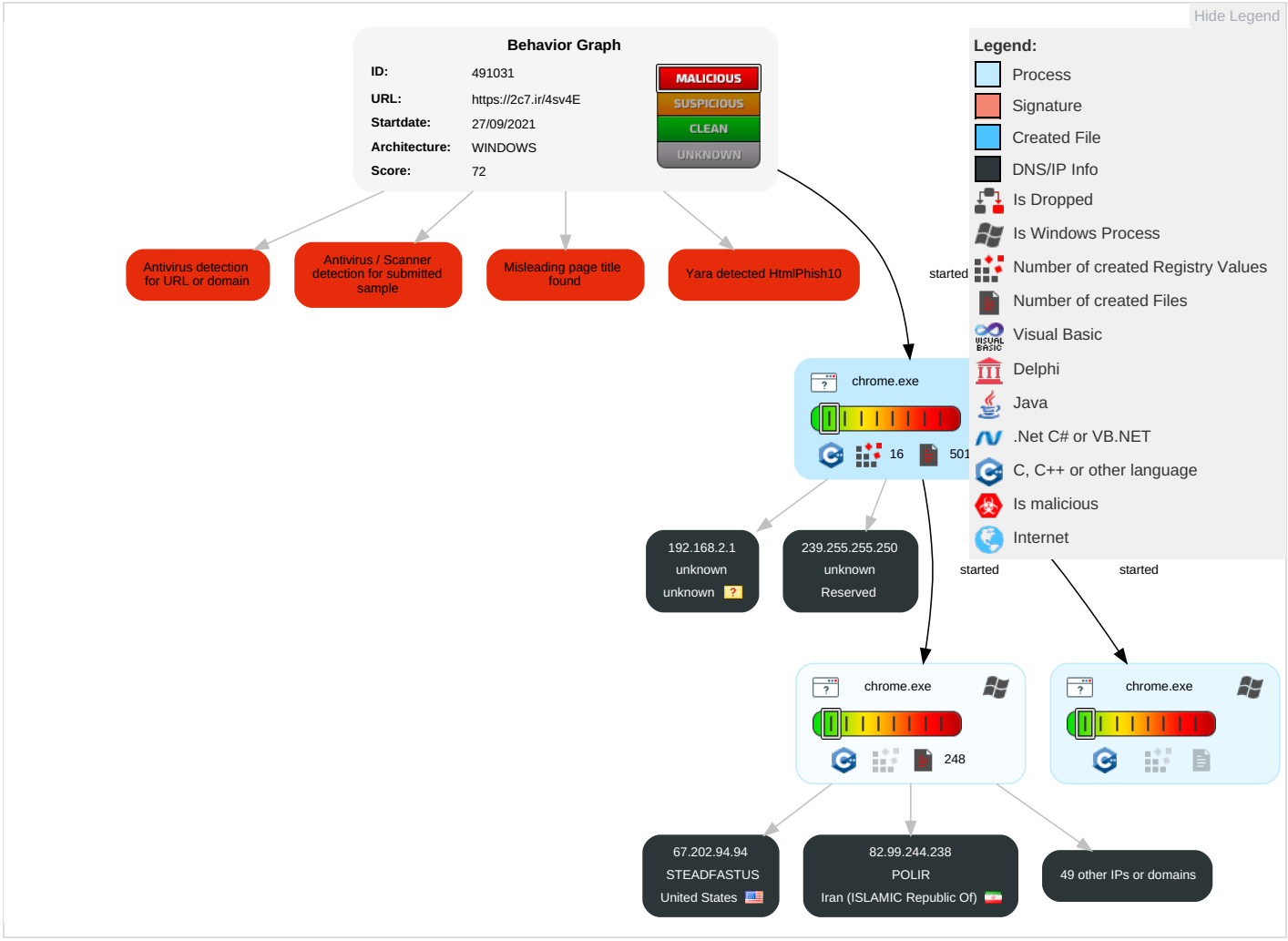
Misleading page title found

Yara detected HtmlPhish10

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Imp
Drive-by Compromise 1	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	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mod Sys Part
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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Dev Loc

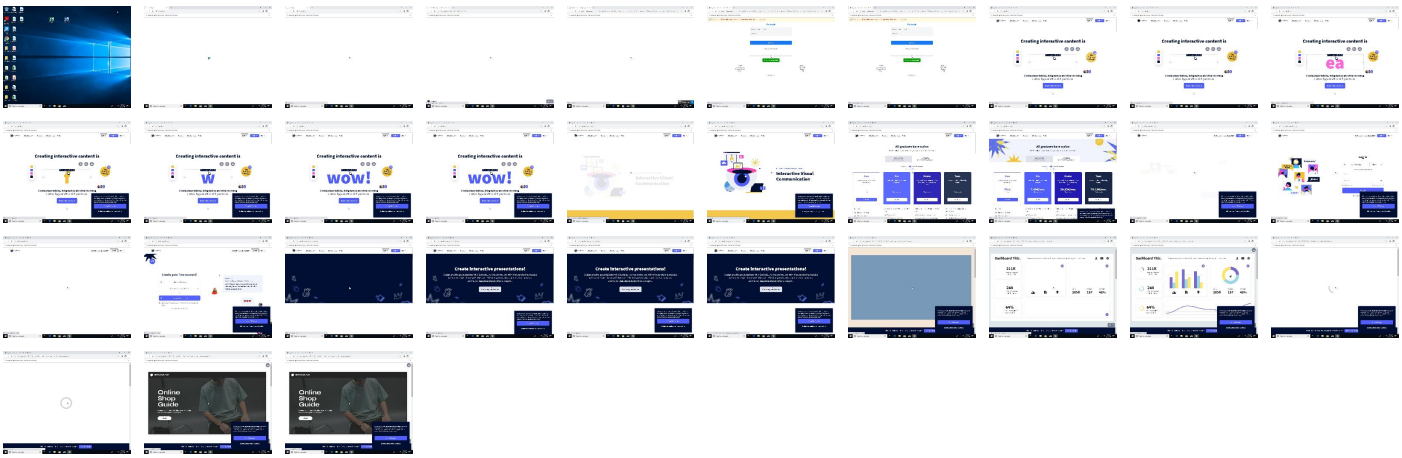
Behavior Graph

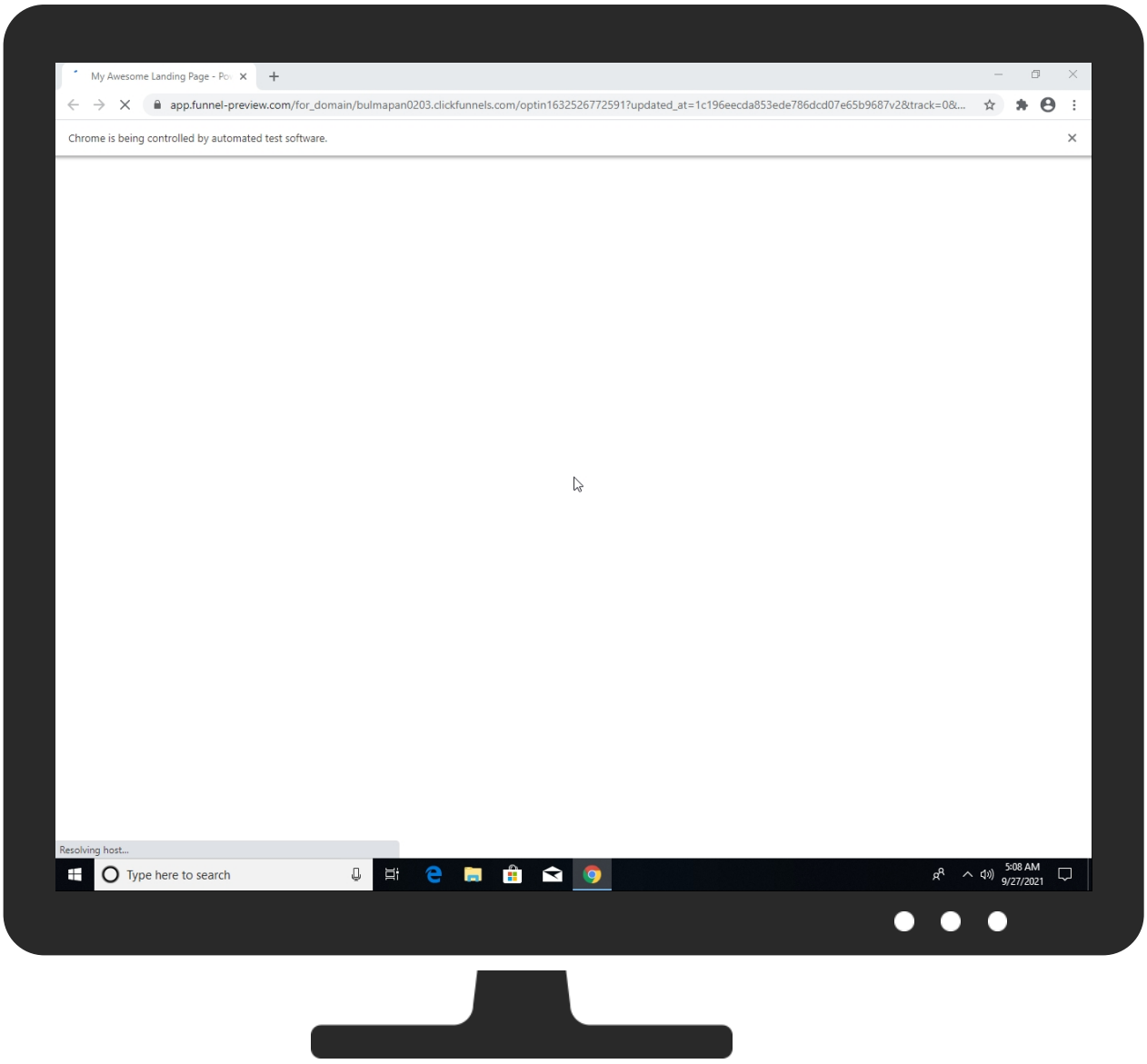


Screenshots

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://2c7.ir/4sv4E	0%	Avira URL Cloud	safe	
http://https://2c7.ir/4sv4E	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://app.funnel-preview.com/for_domain/bulmapan0203.clickfunnels.com/optin1632526772591?updated_at=1c196eecda853ede786dcd07e65b9687v2&track=0&preview=true	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://view.genial.ly/614e65ad1f21fe0d7ec3b264	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://4bpr.art/async?&user=coperola&html=mobileaD	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/apps-themes	0%	URL Reputation	safe	
http://https://2c7.ir/4sv4Ez	0%	Avira URL Cloud	safe	
http://https://4bpr.art/async?&user=coperola&html=mobile	0%	Avira URL Cloud	safe	
http://https://2c7.ir/4sv4E2#Panelfbs	0%	Avira URL Cloud	safe	
http://https://app.funnel-preview.com/for_domain/bulmapan0203.clickfunnels.com/optin1632526772591?updated_a	0%	Avira URL Cloud	safe	
http://https://2c7.ir/4sv4EPanelfbs	0%	Avira URL Cloud	safe	
http://https://static.cloudflareinsights.com/beacon.min.js	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://view.genial.ly/5a660638621bd0183fdb465b/interactive-content-trivial-quiz-ii	false		high
http://https://view.genial.ly/606c014822dac50cf1b7c835/interactive-content-pastel-color-map	false		high
http://https://view.genial.ly/614e65ad1f21fe0d7ec3b264	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://https://auth.genial.ly/login	false		high
http://https://view.genial.ly/60bdff0f347fbd0d328a8bfe	false		high
http://https://view.genial.ly/60d968b961dbed0dd1bd2fea/interactive-content-online-shop-guide	false		high
http://https://auth.genial.ly/signup	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.218.108.99	unknown	United States		16509	AMAZON-02US	false
13.225.78.68	unknown	United States		16509	AMAZON-02US	false
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
172.217.168.46	unknown	United States		15169	GOOGLEUS	false
104.16.148.64	unknown	United States		13335	CLOUDFLARENETUS	false
13.224.193.77	unknown	United States		16509	AMAZON-02US	false
172.217.168.42	unknown	United States		15169	GOOGLEUS	false
104.16.12.194	unknown	United States		13335	CLOUDFLARENETUS	false
142.250.203.99	unknown	United States		15169	GOOGLEUS	false
162.247.243.147	unknown	United States		13335	CLOUDFLARENETUS	false
13.225.78.110	unknown	United States		16509	AMAZON-02US	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
216.58.215.227	unknown	United States		15169	GOOGLEUS	false
104.21.15.175	unknown	United States		13335	CLOUDFLARENETUS	false
82.99.244.238	unknown	Iran (ISLAMIC Republic Of)		60976	POLIR	false
52.49.29.78	unknown	United States		16509	AMAZON-02US	false
172.217.168.1	unknown	United States		15169	GOOGLEUS	false
199.232.194.2	unknown	United States		54113	FASTLYUS	false
54.247.36.38	unknown	United States		16509	AMAZON-02US	false
20.150.83.196	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
172.217.168.13	unknown	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.202.94.94	unknown	United States		32748	STEADFASTUS	false
172.217.168.14	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
52.17.252.170	unknown	United States		16509	AMAZON-02US	false
172.217.168.10	unknown	United States		15169	GOOGLEUS	false
52.218.24.59	unknown	United States		16509	AMAZON-02US	false
104.16.94.65	unknown	United States		13335	CLOUDFLARENETUS	false
13.225.78.40	unknown	United States		16509	AMAZON-02US	false
142.250.203.110	unknown	United States		15169	GOOGLEUS	false
13.225.78.46	unknown	United States		16509	AMAZON-02US	false
157.240.17.15	unknown	United States		32934	FACEBOOKUS	false
172.217.168.67	unknown	United States		15169	GOOGLEUS	false
172.217.168.3	unknown	United States		15169	GOOGLEUS	false
34.247.225.137	unknown	United States		16509	AMAZON-02US	false
172.217.168.4	unknown	United States		15169	GOOGLEUS	false
151.101.112.193	unknown	United States		54113	FASTLYUS	false
104.16.16.194	unknown	United States		13335	CLOUDFLARENETUS	false
104.21.78.7	unknown	United States		13335	CLOUDFLARENETUS	false
13.224.193.104	unknown	United States		16509	AMAZON-02US	false
142.250.203.104	unknown	United States		15169	GOOGLEUS	false
54.155.182.199	unknown	United States		16509	AMAZON-02US	false
151.101.2.137	unknown	United States		54113	FASTLYUS	false
104.16.149.64	unknown	United States		13335	CLOUDFLARENETUS	false
172.217.168.78	unknown	United States		15169	GOOGLEUS	false
142.250.145.156	unknown	United States		15169	GOOGLEUS	false
104.16.13.194	unknown	United States		13335	CLOUDFLARENETUS	false
173.194.160.70	unknown	United States		15169	GOOGLEUS	false
172.217.168.74	unknown	United States		15169	GOOGLEUS	false
13.224.193.86	unknown	United States		16509	AMAZON-02US	false
13.224.193.117	unknown	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491031
Start date:	27.09.2021
Start time:	05:07:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://2c7.ir/4sv4E
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 • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@53/321@0/53
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://genial.ly/ • Browse: https://genial.ly/why-genially/ • Browse: https://genial.ly/plans/ • Browse: https://auth.genial.ly/login • Browse: https://auth.genial.ly/signup • Browse: https://genial.ly/create/presentations/ • Browse: https://view.genial.ly/606c014822dac50cf1b7c835/interactive-content-pastel-color-map • Browse: https://view.genial.ly/5f1a93c2a1a5620d688518a5/interactive-content-dashboard-eng • Browse: https://view.genial.ly/5a660638621bd0183fdb465b/interactive-content-trivial-quiz-ii • Browse: https://view.genial.ly/60d968b961dbed0dd1bd2fea/interactive-content-online-shop-guide
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.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\Local\Google\Chrome\User Data\2825c0c2-5e81-4ea9-87fe-3355fb78f34f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7475731917654005
Encrypted:	false
SSDEEP:	384:J7W5dDcmvEDbVYeFYNtr+vxb36dzSHDOGuxr8/x9xiHPfOrMxmMv87VJFGOjzZNl:Z6Cd96faukePFbLE/L2DKx/tJx
MD5:	9B2506A9FBB0784DE3E12A3BBAC64885
SHA1:	33CC0E909FD6EF5F6A21B0255DB956CDB96FFCB7
SHA-256:	CE1CBD013FDCDDC6BFB63F32D8812FCC3ECD0D3B024EAB6D34D79287217230DE
SHA-512:	3BDF51CD0B413DC327D7C1CC953DDEA9852415A82B57A4ABE2314EE3AE4F166C429252902F94EF8DAD1D8996DBAADC9A1EFA1ECB199BAC31FE535A55EB4BFC3B
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....F8.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\3460fb31-75e7-4e09-aee1-0643e7da2202.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):	174182
Entropy (8bit):	6.048256324893738
Encrypted:	false
SSDEEP:	3072:eHPXR8uPZzf5kiOu8CAKvCYYsHhbPKvvuBzjQ/PpHXDKuFcbXafIB0u1GOJmA3is:evXxPZdp8EBlbyvvux0/xTKkaqfIlUOv
MD5:	04439094DE03A9E9AC695BBAB146611F
SHA1:	3A7845C612967B956AD2292AC9C6AE65A49F0EEE
SHA-256:	2B89015D667C94EEC51C7391169B307F645BAFF6040A7EC49AC9F8878AFFA20E
SHA-512:	D30C8AD7805934078C5ACEAEAD72866E0CAEA90544EB92C399DE1AB32E5502726107C634F5608B01A60CCE864281EBD745F5555D9AF44516D070760AA18A8D4
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":1.632744491069808e+12,"network":1.632712092e+12,"ticks":4212354354.0,"uncertainty":2484883.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799330560"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\39f16561-0bd6-4487-ab9e-adb35c94f8ab.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):	174275
Entropy (8bit):	6.04852619233439
Encrypted:	false
SSDEEP:	3072:eWPXR8uPZzf5kiOu8CAKvCYYsHhbPKvvuBzjQ/PpHXDKuFcbXafIB0u1GOJmA3is:eQXxPZdp8EBlbyvvux0/xTKkaqfIlUOv
MD5:	5FC99CBF2A6E8CC7E3A0A5B59176AAEB
SHA1:	EDEAC2981A69E2C8A7F031B46148D72CB350DFAF

C:\Users\user\AppData\Local\Google\Chrome\User Data\39f16561-0bd6-4487-ab9e-adb35c94f8ab.tmp	
SHA-256:	18B082FEA67C3A5B52EFCCD265D564BDCD537E7D7DD5873EBF6E0CB0D0741939
SHA-512:	96E5E7147A63CBF918A93D7C92CE720FF2615E6C7E2911A416A8483A829BD08844FA0079221A7B6B9C908CAA19357ED33FE882D073FE5FBD71A2DDD3D0E4EFF 9
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":1.632744491069808e+12,"network":1.632712092e+12,"ticks":4212354354.0,"uncertainty":2484883.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799330560"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\5bf9c6bf-6ea2-46c6-9e24-0795278a11e7.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):	174078
Entropy (8bit):	6.04794841735597
Encrypted:	false
SSDEEP:	3072:IHPXR8uPZzf5kiOu8CAKvCYYsHhbPKvvuBzjQ/PpHXDKuFcbXafIB0u1GOJmA3is:IvXxPZdp8EBlbyvvux0/xTKkaqfIlUOv
MD5:	CE0DBEC589C59DC5764ACFD38471980A
SHA1:	D8587BE453D2CEC7C37B8349CB09B320A53A33F4
SHA-256:	14CEECC85D99A8A95E04885C0C6F45F6DCB349643DDE09C5F53E20D29B403AA4
SHA-512:	D57FF3A8CA5F8EB656E5DC9A134CEFBC2ED3FAB1486F5261865D8A001223DAB48400AF52B8CC18E8C7B4EF043AF5357B8B75FB8B1A960EE6ED031B160950FF 67
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":1.632744491069808e+12,"network":1.632712092e+12,"ticks":4212354354.0,"uncertainty":2484883.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799330560"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\8150e9ef-83df-4936-ab72-f2922e594fbc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.747652719284428
Encrypted:	false
SSDEEP:	384:57W5dDcmvEDbVYeFYNtr+vxb36dzSHDOGuxr8/x9xiHPfOrMxmMYK87VJFGOjzZV:p6Cd96fkukePFbLE/L2DKx/tJb
MD5:	2151ED1561F3341CA9AFC7CBA4234AE6
SHA1:	F5932EAAF51B45CAC21892374D1F6C2636901B50
SHA-256:	3982531CD6090BC74FF24962612A35C0679BE2906E59B992FCDE772CBE7D3A30
SHA-512:	40110C9DD5EEDA0550F5294BA397EEB8CB804B681C36331D5F09C69684C1214B6EF1B8BE125EB34AF92E237FBF360336673E750E3B612A92BF1B38E07F5687A2
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....F8.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\9b977e47-d1e5-4159-969e-254df2089623.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):	182561
Entropy (8bit):	6.077681568884413
Encrypted:	false
SSDEEP:	3072:dKtPXR8uPZzf5kiOu8CAKvCYYsHhbPKvvuBzjQ/PpHXDKuFcbXafIB0u1GOJmA3P:c1XxPZdp8EBlbyvvux0/xTKkaqfIlUOv
MD5:	87AA0C07AE4115C5AE01E32D4E504BE0
SHA1:	C786542E6AECB5442BDC603791C97CC47A2C37D7
SHA-256:	AD931A648AFC45A7024922A3C3744C1F4591A75B17F6068C32AA4F0FF16BC7BE

C:\Users\user\AppData\Local\Google\Chrome\User Data\9b977e47-d1e5-4159-969e-254df2089623.tmp

SHA-512:	8FE034E25A794CD5181539D87C4DBCBFCD2A931E403F98E15E3C726E7AE009D0523F4794B8F298955243DFB20D1D10A2BAA2F73D729481E4C4CDFD8D2E5A67A
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":1.632744491069808e+12,"network":1.632712092e+12,"ticks":4212354354.0,"uncertainty":2484883.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+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\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
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\043db510-4a16-41eb-9808-9c8b3656ffdf.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):	24056
Entropy (8bit):	5.53395605895832
Encrypted:	false
SSDEEP:	384:1sttgLltgXO1kXqKf/pUZNCgVLH2HfDBrUSHGLHGsnT9HcFrB4k:jLlYO1kXqKf/pUZNCgVLH2Hf9rUSGbGp
MD5:	AD2E447B1DBFFF752F446D7568F838AE
SHA1:	86C1577B22B68D8DF737D925AA93FA8514B57F50
SHA-256:	D500D0D18F0047A8B070C39F3D99E2FA203ABBBE2E98F8F7FD9C6C91771DB8F4
SHA-512:	69C9F001C2141E4178FBA82434C6F5CF0F35D33E981FE41F69324A79452771579AF77A944D4EF8E14F365812CB35663F088E071C4060537B8499CD0D786FE545
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":"13277218089391533","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\1b089d88-03c5-4b7f-970b-785869ece4cd.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):	5998
Entropy (8bit):	5.191105750028706
Encrypted:	false
SSDEEP:	96:nOCfiCW9hJPvZycKIGiok0JCcRWL8Lk+1HpbOTQVuwn:nOCfo9hpYc8d4cY0k+Zp
MD5:	F47685063A14E6460AD000FD2CC5F3DE
SHA1:	9970197A05F883560E6E2A099309FDAD4DE013DA
SHA-256:	F3C84EF74CBBECF6F3658B7E20B03C2F5DD619F13378160556CB1810C74CE81A
SHA-512:	0DFF1F199C0C9996DDB1E15DC508B7F0005586E1500EEB2910C56DFD176CD0A8E0CB503E0DCC0FD15C951218FE9B04A8CCB31DD8B2BF84E0BE01E8D611A356E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1b089d88-03c5-4b7f-970b-785869ece4cd.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13277218089769822","alternate_error_pages":{"backup":true},"announcement_notification_service_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_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\246f7a1b-bbd4-42fa-980d-1041b903d894.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):	5970
Entropy (8bit):	5.189283101514312
Encrypted:	false
SSDEEP:	96:nOCfiIW9hJPvZycKIGtok0JCcRWL8Lk+1HpbOTQVuwn:nOCfg9hpYc8M4cY0k+Zp
MD5:	2D9B2B1629254BB6D2B584D2DD7B508E
SHA1:	67CC5D21026BA871D8A11AE0227B400700DDB7DC
SHA-256:	5BDFF8E84999794B6CA18866218A8B4D4A3E37CBD6B6799C91F8439F62A4A253
SHA-512:	E19E4CE3DF262D892FF430ECFAC52DEB6D7DE076F79719669B955FDD5985A093E29ADB4DC87A7A3D56B260C02507A50A8EB36660B60C2F69621C3740BDAF334
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13277218089769822","alternate_error_pages":{"backup":true},"announcement_notification_service_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_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\340ebf0b-9218-4cf3-8fe0-4a28f20e2969.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3e377f80-d041-42cc-b704-d6974f10bce3.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):	5998
Entropy (8bit):	5.191105750028706
Encrypted:	false
SSDEEP:	96:nOCfiCW9hJPvZycKIGiok0JCcRWL8Lk+1HpbOTQVuwn:nOCfo9hpYc8d4cY0k+Zp
MD5:	F47685063A14E6460AD000FD2CC5F3DE
SHA1:	9970197A05F883560E6E2A099309FDAD4DE013DA
SHA-256:	F3C84EF74CBBECF6F3658B7E20B03C2F5DD619F13378160556CB1810C74CE81A
SHA-512:	0DFF1F199C0C9996DDB1E15DC508B7F0005586E1500EEB2910C56DFD176CD0A8E0CB503E0DCC0FD15C951218FE9B04A8CCB31DD8B2BF84E0BE01E8D611A356E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13277218089769822","alternate_error_pages":{"backup":true},"announcement_notification_service_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_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3e377f80-d041-42cc-b704-d6974f10bce3.tmp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5a20ce81-84a9-488f-9859-19c495043f8b.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):	5.536339029612912
Encrypted:	false
SSDEEP:	384:1sttgLltgXO1kXqKf/pUZNCgVLH2HfDBrUlHG5nT9HchrB4T:jLlYO1kXqKf/pUZNCgVLH2Hf9rU5G5nj
MD5:	1CAA486E16727E141BB28BB75A9C7DB9
SHA1:	91012F79CEDC446FC222564E275E5D4CAFE5843C
SHA-256:	00864230C7EFC71C524D6EC8910FBAB659F32EE7D4CAF644484FC2CC24FE5DE3
SHA-512:	BB06A5315D22E0E848454B53A5981E814FA8E82472D17BDF11E4ACAEADF8F60A6D2FCB4C429FF864A54311166930F4A34CD5B145C193A74353477BE170AEC5B
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":"13277218089391533","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\5e5c9e5f-7e65-4e59-8873-8504965f81a5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	1541
Entropy (8bit):	5.5965405628888005
Encrypted:	false
SSDEEP:	48:YUeUY0GwieUYx6UUhKUYE9KUhIqPeUer2Uefv6wUe4Uenw:/eUY0GwieUYIUUsUYE9KUhXPeU9UEfUU
MD5:	50839FAA8C421AC2D8D964AD240B39B5
SHA1:	0A9E10F9EB2B4A6A70361AFE2DD8B7EB478A0F81
SHA-256:	6A250132D6381D0FB284272F3D6F47E80D989A97968F433A0FAA9859BE131248
SHA-512:	4315A3F924A551D8CBA19D864D55D3C24DEB9E0D0473D951A2225581D8F714B3ADE7AB00004423A1C885EDF80520355257EFEADAEC9E283C471126066476F603
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1643630907.340978,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1632744507.340985},{"expiry":1664280542.800156,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1632744542.800162},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1664280545.141798,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1632744545.141803},{"expiry":1664280559.969798,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1632744559.969803},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6d86b563-a236-4560-90f3-624de31d5ce9.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):	5970
Entropy (8bit):	5.188366871635481
Encrypted:	false
SSDEEP:	96:nOC6IW9hJPvZycKIG+ok0JCcRWL8Lk+1dbOTQVuwn:nOCo9hpYc8J4cY0k+v
MD5:	63F5E4946C0BA35587BAC6974323A3F4
SHA1:	26362FD99E97DEA8B131EB5D34DE660D739929DC
SHA-256:	B352138831B90D6ECE9455E120676C8BEE09D7E87E7E3C0BC5667DF5417081BD
SHA-512:	3145A88159E1F0418E886D7C1C2117BAD94114BEFBCE9F62897741E3B4223735FB20CC64327B95627BE4E1F7F3DF5F853F3C1932E89362A73582F65E6082D535
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6d86b563-a236-4560-90f3-624de31d5ce9.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13277218089769822","alternate_error_pages":{"backup":true},"announcement_notification_service_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_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\74c3b569-e034-4e1d-a1c9-5fd763f92c7a.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):	1539
Entropy (8bit):	5.594824337198612
Encrypted:	false
SSDEEP:	48:YUeUY0GvieUYS6UUhxUY2KUh1MqPeUer2Uefv6wUe4Uenw:/eUY0GvieUY3UUDUY2KUhdPeU9UEfUN2
MD5:	3DDCA250083F52DD007356F72509082E
SHA1:	32705162F8540EEB48EB0C73DE39CA3C32B69381
SHA-256:	527C49B436F594BC9065D96F327EBDD2520DC20C4C7C96D205BE05EEEC701622
SHA-512:	DA1C7EC417371431A685BC251430D705966F0D26C59DFE97FBDEF476484AB8159E261D796B1C1AD8651439DE23BB7F2DCFF56B5D1F306BF7F0733AA71ADED1 3
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1643630907.340978,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1632744507.340985},{"expiry":1664280530.397843,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1632744530.397853},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1664280530.92712,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1632744530.927126},{"expiry":1664280506.373906,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1632744506.37391},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\776fbebb-9712-4301-b6b5-37682b918d18.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):	24054
Entropy (8bit):	5.534126610932784
Encrypted:	false
SSDEEP:	384:1stttLltgXO1kXqKf/pUZNCgVLH2HfDBrUSHGLHG7nTOcMrB46:QLlYO1kXqKf/pUZNCgVLH2Hf9rUSGbGa
MD5:	5BF5792D94D7A7D697EE1702FF69B129
SHA1:	9A7CF0062EA2893F66AA52BDE98C0AD42E7D4D99
SHA-256:	2E220C555422052FAAF3365D4EF7002232D6A48A7308E3BF88231EB41617868B
SHA-512:	A62547DB59E9BDE2A164996B41631989E9B59BAD339BA32944F67CB2E37E113FF71ACBEFD2943A24AB893032F7710432562F41684F0C505CBEA3AEE5D05E44A
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":"13277218089391533","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\7973353c-e0dd-49e0-bcce-7e35e2aea832.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):	5970
Entropy (8bit):	5.1884837308982545
Encrypted:	false
SSDEEP:	96:nOCfiIW9hJPvZycKIG3ok0JCcRWL8Lk+1dbOTQVuwn:nOCfg9hpYc8y4cY0k+v
MD5:	A35E9F7AA878D98823969111A46BF6EC
SHA1:	2A398D5BCFEB2C20648984D213701496C7DE6880
SHA-256:	2A31FF9D809A841EBB57380FBDDD18DDB3B29349B86930001178AE5115DBF80E
SHA-512:	EA87E7C1DE54BFCF7DB45237613DB651F45DF0A722B78B870EB185D9827B6BF924B978A865F869CB94A09645B753D26A855E4C444123AA0EF98FFDFEBF8E073 D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7973353c-e0dd-49e0-bcce-7e35e2aea832.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13277218089769822","alternate_error_pages":{"backup":true},"announcement_notification_service_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_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b1da0ac-123c-4977-976e-38a6a8c1da06.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):	1541
Entropy (8bit):	5.5912880311575295
Encrypted:	false
SSDEEP:	48:YUeUY0GwieUYx6UUhKUYEEKUh11qPeUer2Uefv6wUe4Uenw:/eUY0GwieUYIUUsUYEEKUh+PeU9UEfUU
MD5:	099E030F3558BE84AFE69D85E85A4B8C
SHA1:	96AF4F5EC328CD906F2A1E6117DFDAE8E070823D
SHA-256:	D998305E8E086D1EF01619E86700BE5579A955FA4BF3FD657E7FCEE2243C891A
SHA-512:	32F0F9581AFAAE899C7CBAB8604B4C776033086D0A9D579C85523BA2AC92FB1A9A62D9D04D9D3F0B03CAA2403202648EF8F12B449CF65BE31EB6F98E9E72568A
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1643630907.340978,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1632744507.340985},{"expiry":1664280542.800156,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1632744542.800162},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1664280545.141798,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1632744545.141803},{"expiry":1664280544.102635,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1632744544.102641},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\883c7b77-5810-45fc-87cd-9cdc3b6a7e18.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):	5.536347207642704
Encrypted:	false
SSDEEP:	384:1sttgLltgXO1kXqKf/pUZNCgVLH2HfDBrUlHGonT9Hc45rB42:jLlYO1kXqKf/pUZNCgVLH2Hf9rU5GonF
MD5:	4EBAFE85DE5FD3FD79AB4759A7B28240
SHA1:	6E626D445F875A6B41B881905FAF16D6F01A8908
SHA-256:	2E46F21DC6D0CE8D43C340525E19530F8A838345DB78E100454657F532C76121
SHA-512:	D08C33733895DEC3E53690D501690B44A27B2FDAB4424FCF728D3B39F9CFD22785520EE8A96C97373082A6343CC0668A0F8FB0F99EB06799C5B6A848AB7CCFB
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":"13277218089391533","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\9069b129-4784-4d27-bb48-7ac4fb7b2cae.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):	3930
Entropy (8bit):	4.908530147628736
Encrypted:	false
SSDEEP:	96:JTOXGDHzzB8lZlaGgb65TwGPkpKV/roGlFtGGpV/H:JTOXGDHzzB8lZlazb65TwakpO/cgtGiZ
MD5:	7571A2F70768251878B86190A59D719F
SHA1:	8394D00E6DACFC4C0C2C75673DD3199803A33CD5
SHA-256:	E7C3FBC09A324BDA69F5AFBAE40BA5FAE15147D140BF5505D3F34397A2F1737E
SHA-512:	A9F4FCA8343C97188398B39AFC91354551E0D57957EF1557B4C029FA341FE8275A7FBB5D77487E1E82BA75589888584DA75A3F0ADD77E36DB58DCB083AEC506
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9069b129-4784-4d27-bb48-7ac4fb7b2cae.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.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":"13279810091712367","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13279810091716938","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13279810091827320","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expi

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):	5.225998587052354
Encrypted:	false
SSDEEP:	6:mYsB/y+q2PWXp+N23iKKdK9RXXTZIFUtpXsBwZmwPXsBgVkwOWXp+N23iKKdK9Rn:nW/y+va5Kk7XT2FUtpXWw/PXWgV5f5KU
MD5:	613EA91962218B6BDF85F1642B42B176
SHA1:	16E86F458EEE8389972C6624712BF57D8048F9D5
SHA-256:	C0245D66B556DB893043C8A3788A7106C7BEE9657E3E680EA22464D84198B5F2
SHA-512:	65BCD2FA399F51E4070DB1FC24C90BA26BA6FE95643D9D88361252003FB4EE2CF69EEEC882EE08921391990F7B4731855B57FAFEC8A68067D9774BC3F31A394
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:17.201 1ddc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/09/27-05:08:17.203 1ddc Recovering log #3.2021/09/27-05:08:17.203 1ddc 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.oldNT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.225998587052354
Encrypted:	false
SSDEEP:	6:mYsB/y+q2PWXp+N23iKKdK9RXXTZIFUtpXsBwZmwPXsBgVkwOWXp+N23iKKdK9Rn:nW/y+va5Kk7XT2FUtpXWw/PXWgV5f5KU
MD5:	613EA91962218B6BDF85F1642B42B176
SHA1:	16E86F458EEE8389972C6624712BF57D8048F9D5
SHA-256:	C0245D66B556DB893043C8A3788A7106C7BEE9657E3E680EA22464D84198B5F2
SHA-512:	65BCD2FA399F51E4070DB1FC24C90BA26BA6FE95643D9D88361252003FB4EE2CF69EEEC882EE08921391990F7B4731855B57FAFEC8A68067D9774BC3F31A394
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:17.201 1ddc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/09/27-05:08:17.203 1ddc Recovering log #3.2021/09/27-05:08:17.203 1ddc 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):	5.2260351329468016
Encrypted:	false
SSDEEP:	6:mYs1Mq2PWXp+N23iKKdKyDZIFUtpXsB/tZmwPXsB9uH/kwOWXp+N23iKKdKyJLJ:neMva5Kk02FUtpXW/t/PXW9m5f5KkWJ
MD5:	6024B9A93F29749C7942BC0C25BC46B7
SHA1:	A82F7114411CDB20F0AF27A48B600731EE74FBE6
SHA-256:	80260ABA3E3D00FD9A59B8D707FA7DAAB2D9C89D3F046C554D5812D7976DB14E
SHA-512:	CC565A2A6470D82A1B7E1D9E0F8801BDB71CAC9F9910A65BD1633400D519C98882F1D9FBCA1093574ACB92165FE17E6392413592332A1A65AF9A880745BB909F
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:17.199 1b24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/09/27-05:08:17.201 1b24 Recovering log #3.2021/09/27-05:08:17.202 1b24 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.R (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old.R (copy)	
Size (bytes):	318
Entropy (8bit):	5.2260351329468016
Encrypted:	false
SSDEEP:	6:mYs1Mq2PWXp+N23iKKdKyDZIFUtpXsB/tZmwPXsB9uH/kwOWXp+N23iKKdKyJLJ:neMva5Kk02FUtpXW/t/PXW9m5f5KkWJ
MD5:	6024B9A93F29749C7942BC0C25BC46B7
SHA1:	A82F7114411CDB20F0AF27A48B600731EE74FBE6
SHA-256:	80260ABA3E3D00FD9A59B8D707FA7DAAB2D9C89D3F046C554D5812D7976DB14E
SHA-512:	CC565A2A6470D82A1B7E1D9E0F8801BDB71CAC9F9910A65BD1633400D519C98882F1D9FBCA1093574ACB92165FE17E6392413592332A1A65AF9A880745BB909F
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:17.199 1b24 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/09/27-05:08:17.201 1b24 Recovering log #3.2021/09/27-05:08:17.202 1b24 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\024b0b16471e63dc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.468678716403971
Encrypted:	false
SSDEEP:	6:mc9Yk+6KHHWXll1/lgZR3o+wrl/yAiDK6t:l+hnW9/lcWXJq1
MD5:	3C67336B89C3FB27B2AC888EFA2BEFAB
SHA1:	B1E26AC2DDC9ABB7BC4EDD752854341D305B4ABD
SHA-256:	4A18CF1FC3B7B1221D2485FB2DEB9407369E08BC4C0C2FC68BA752771A10BD85
SHA-512:	76503B601A18B91A0C448C72A6CFE04D559678BD228358746A1936538EDA16C16318D35C04C86A74301E129DB190388507CCFF429D99AB4E31D70DD4C61D60A6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....._keyhttps://static.cloudflareinsights.com/beacon.min.js .https://funnel-preview.com/../<.+/.....Vw...s..M}...I..9....v...A..Eo.....Y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0635d50b7c9cecbb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6241
Entropy (8bit):	5.869222673366495
Encrypted:	false
SSDEEP:	96:sgaa/7L3AUUjkguGU6oqFNnsTahjfybumJa/Aei:sda/f3LHgud6oQ6AabumJa4X
MD5:	9DF70C2EEF23A04B620EDDB9644CCD92
SHA1:	91BFA9D9B764576D92994449AD15D0E873609295
SHA-256:	F0E11F7A4F1F320EBE0D6FA950F9AB7BC73959737DA11DC02175BB0A927B2F0C
SHA-512:	436BE0055C0CBA1010E3E8584ADAAD294C2A336B02031FD3D7561E1ADA15F2B77B38A46501D04004D106C03604A332244E156C248735B6F16DFF3DADA19AD47
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...T.M+...._keyhttps://genial.ly/commons-3ca65ea7ff019bc1f437.js .https://genial.ly/.A.<.+/.....2.....o.\.|...`.+.SA..K....=.....S.A..Eo.....G&.....A..Eo.....'.d.....O.....4.(.....I.....D.....(S.U...``....TL`&.....Qb.Nd.....self. Q.p.z.....webpackChunkgatsby....Qb&.w....push.....`.....L`.....`.....Ma.....`.....b<.....>..C`....C`n...C`(...C`.'..C`....C`^B..C`T&..C`<#..C`8"..C`./..C`....C`8C..C`.$..C`.....(S.....Pd.....push.8048...a.....(..h.....@.....@.....@.....Qb.}.....8048E.@.-.....@P.....1...https://genial.ly/commons-3ca65ea7ff019bc1f437.js...a.....D`....D`....D`.....y....`8...&...&.....D&.(S.....Pd.....push.3439...a..... .f.....@.....@.....Qb.5.....3439E..A.d.....@.....D&.(S.....Pd.....push.2999...a....!.... .f..... ...!."..... Qb.....2999E.d.....D&.(S.....Pd.....push.2196...a/.....~

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0778307c93d4285c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1567504
Entropy (8bit):	6.009015468012711
Encrypted:	false
SSDEEP:	12288:0B2Wco21X+qUEuTHniu4HNjFXE6V5oCCNeShxlEI7cxCnKt32lSEC3WUULRU9:0B0ruziu4t5E6VmZreIHaW9U9
MD5:	141CAE2734F65A9C6BABDB9FBC7C9D1D
SHA1:	27D54EBAA720F301A3167DD3B8B57BC9B36DCFC4
SHA-256:	7CA11143560461CC028666FE36BF387AFED966A6C0AE507D63571EFD9DC3F720
SHA-512:	F4BFCE5E359D63F77A6D4487124E9B41085E4274DDDECE308B95E4A6574A0B157D5AB1EA31F55EBD17BDA0F1699E83A38237BD6275EEB3A04006B769C1543B6E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0778307c93d4285c_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...X.....4490B0D769897622C888BDF2DE9E5695552D9CBBE30C9D058C048775E1DA22C0.....'..n....O.....T.F.....(....3.....X.. ...L..... .....8.....`....#.....I.....H..... .....X.....x....U..... .....0.....(.....8.....8...I.....D.....@..... .....t.....|.....X...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\07e51f63672c940b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1092
Entropy (8bit):	5.8460991182754185
Encrypted:	false
SSDEEP:	24:6gcMI4ThQgcMIdxTFsBTagcMIATWQgcMIlRTG:6zaThQz5TFQTazGTWQzfRTG
MD5:	238FBFA891D2E26ED188F8750C47BC1B
SHA1:	B197EC2744C5E7D590BBD3511A9421A4F8336F67
SHA-256:	8F4042277B22A7D3FA657572A22CC103FE5198045768A7B776651D0B0BEDAE1A
SHA-512:	D86802A27B1626EE77A82EAFD9CF9BE06AD2FD4E7E735426FD8C9410AA3874862FD282B98CE7E09D6BB5DADD44176AFD5765BF53A38F90DAA1685C400606F7 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...]....._keyhttps://www.google-analytics.com/gtm/js?id=OPT-NMJDJ9J&t=gtm4&cid=2090427844.1632744494&aip=true .https://genial.ly/.g.<.+/..... .6....G.lx.k2.1@0...tE..i.YB.p...A..Eo.....@.!.....A..Eo.....0\r..m.....x...]....._keyhttps://www.google-analytics.com/gtm/js?id=OPT-NMJDJ9J&t=gtm4&cid=2090427 844.1632744494&aip=true .https://genial.ly/.`.<.+/.....F.....6....G.lx.k2.1@0...tE..i.YB.p...A..Eo.....h.....A..Eo.....<.+/.....xG.....6....G.lx.k2.1@0...tE.. i.YB.p...A..Eo.....XX.....0\r..m.....x...]....._keyhttps://www.google-analytics.com/gtm/js?id=OPT-NMJDJ9J&t=gtm4&cid=2090427844.1632744494&aip=true .htt ps://genial.ly/#..?.+/.....u.....6....G.lx.k2.1@0...tE..i.YB.p...A..Eo.....r.....A..Eo.....0\r..m.....x...]....._keyhttps://www.google-analytics.com/gtm/js?id=OPT- NMJDJ9J&t=gtm4&cid=2090427844.1632744494&aip=true .https://genial.ly/.[$?.+/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0fb7f5ed12432205_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	89144
Entropy (8bit):	6.096491618706186
Encrypted:	false
SSDEEP:	1536:9yr5UIDxRBCSsz6pEG7reqVLFZfg3MM/gRXuNzLMU6FzrCQ4Ib2CRF9dz7Ce:4r5UmRBQz6pEG1/Zf9/XuNMDNGQ7KCRt
MD5:	AC16E0284BA8E29ACA658AA91961344E
SHA1:	F40FF044759DED4A8B71F84A01D8616CE3C67746
SHA-256:	07F13DF33570FC979DFAFFC6FE3955BECF68BDEDC44AF2570E57BF83E61EDB5E
SHA-512:	FAF67DCDFC384F7D3F853C2066E07D4E600010F49CBA570910936381C021BF19741AEC26E42E7394484C9545D8A067272561EB89CB358843CE4DC2152F47A3BD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...I 1.....D5880602731C394F483C361C5DE6772698F27866ACCF51D81E12E3C09AF8906D.....'.y.....O.....Z...4.....<.....`.....L..... .....P.....,.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.Q w....n.....QbV.....q.....Qb...[....r.....Qb.....t.....QbV..A....v.....Qbn t.....x.....QbB=Lm....y.....Qb..u&....z.....Qb.%.....A.....Qb...&....B.....Qb.....C.....Qb...U....F.....Qb... ....E.....QbN.....D.....Qb:Y${....G.....Qb.....H.....Qb.../....J.....Qb.\|.....I. ....Qb.....K.....Qb.]..=....aa....Qbr.k?....L.....Qb.....N.....Qb./.....O.....QbJ..+....P.....Qb...U....M.....QbrR3.....da....Qb.....ea....Qb...1....Q.....Qbv.y#....S.....Qb.U.y....R.....Qb.... ....ia....Qb.D.p....U.....Qb.....ha....Qb.;.l....T.....Qb.....V.....Qb.....W.....Qb.$.....Z.....QbB9Pk....Y.....Qb..?D....X.....QbF8.....ba....Qb.G.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1fa57e55091cc94a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	86120
Entropy (8bit):	6.088440427228947
Encrypted:	false
SSDEEP:	1536:RZ8XumD/fAlRXXRxDCL/QhlquR/+klY6RbBEUbCMSI7Ny2cF9dzF:n8Xu+KFBxeQhtR/ll5FxWMZByRF9z
MD5:	D92E8A80E69F5C0667C7B56242621BF6
SHA1:	2EADA36C8F00B1BF9777773DCBD1E2CF84573D15
SHA-256:	3BB8DA373860FDDC9A410F7F8044EEF7211B98D4BF10BFA0DAD15426C28FB748
SHA-512:	A98572573685D41697E62E5456F87E5296FEA6F34266A2F4E7016A76117B9AF092D1F9DCA9541EDFA9AF5706D7E85B3A12FD0330B3DB72B2E887AA3A05759CF6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1fa57e55091cc94a_0	
Preview:	0\r..m.....@....?.....D79A79A47022D2778CFD96D6839BB768B1C57A2B07B32DA59DDC6C9707BAB891.....'.y.....O.... O.....h.....<.....`.....L.....|. .....t..... .....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.}.....n.....Qb..k.....q.....Qb..eb....r.....Qb.....t.....Qb..9.....v.....Qb..\.....x .....Qb.h.....y.....Qb.C.9....z.....Qb.....A.....Qb&'X.....B.....Qbb.....C.....Qb~l.....F.....Qb.....E.....Qb.Z.D....D.....Qb.....G.....Qb:._X....H.....Qb.x.....J.....Qb..!.....I.....Qb..... ...K.....Qb.....aa....Qb*.ka....L.....Qb.....N.....Qb.K.=....O.....Qb.....P.....Qbv.....M.....Qb.....da....Qb.4.....ea....Qb.XOD....Q.....Qb.}`.....S.....Qb.....R.....Qbf"O.... .ia....Qb&.mY....U.....Qb.....ha....Qb..g.....T.....Qb..R.....V.....Qb.....W.....Qb2..b....Z.....Qb..q.....Y.....Qb.4.1....X.....Qb>.z....ba....Qb..o.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22dfad3329087616_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1012
Entropy (8bit):	5.847059803041197
Encrypted:	false
SSDEEP:	24:TgaIMSSo6NgaInSlUSSoONgaIlSSovNNgaICpSSoI:TXLNaNnNqANLd
MD5:	4D18F9F5E6B0018CA1FE69C3986ED29F
SHA1:	390CB3E2EEAE92A7BBAFEAE4C953B96B8BB369F2
SHA-256:	98CF3E446B0BEEAA915DFF75EECA4F00AC73940A27C78CAD9BF0C0798EB96D32
SHA-512:	8B398F21BE75F7FBADC0C74FEE2175C291FB2431C0A967BECADDC0DD15357AA2B6427550674A8B43BE1FAB24486E3BF96163204876D0229E6939BDE542CE481D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....y.....M....._keyhttps://www.google-analytics.com/gtm/js?id=OPT-NMJDJ9J&t=gtm18&cid=2090427844.1632744494&aip=true .https://genial.ly/...<.+/.....A... ....(.@4..0+0..\T.Y..a.`.b.xu.u.V..A..Eo.....].:.....A..Eo.....0\r..m.....y.....M....._keyhttps://www.google-analytics.com/gtm/js?id=OPT-NMJDJ9J&t=gtm18&cid=2090427844.1632744494&aip=true .https://genial.ly/B..=.+/.....(.@4..0+0..\T.Y..a.`.b.xu.u.V..A..Eo.....Z5/z.....A..Eo.....0\r..m.....y.....M....._keyhttps://www.google-analytics.com/gtm/js?id=OPT-NMJDJ9J&t=gtm18&cid=2090427844.1632744494&aip=true .https://genial.ly/..K>.+/.....(.@4..0+0..\T.Y..a.`.b.xu.u.V..A..Eo.....O.....A..Eo.....0\r..m.....y.....M....._keyhttps://www.google-analytics.com/gtm/js?id=OPT-NMJDJ9J&t=gtm18&cid=2090427844.1632744494&aip=true .https://genial.ly/...>.+/.....(.@4..0+0..\T.Y..a.`.b.xu.u.V..A..Eo.....Ek.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\25a59ffe919f7aa9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.534316054342783
Encrypted:	false
SSDEEP:	6:mHlPYk+DQPClgwLbcZ6uhIRK6tWHlPYk+DQPZYQlgpNbcZ6uhjK6t:cl+DQPClxLIEfCl+DQP3lsNIEW
MD5:	125B55F656A120591FCD00934F37F493
SHA1:	A9B9A922E84BEECF85D84200F339F9B7DE33DF60
SHA-256:	054639B188E8FB7B24E641B8AC5A367AAB5978EA67327DD5BBE51E59C39C62A8
SHA-512:	048DA1A9005B5C01285F575B192C05CBD53AB5A59461F71523A566BA8E1CC026F300BE1829C8282781A68961E41897465CC5680B8754082BAD5E48730B5B6655
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....ts....._keyhttps://static.genial.ly/auth/main.06ed7008d51d7c1e836f.js .https://genial.ly/k.k>.+/.....Rgd.,.@..VM..s.{.l".,<...5@u..A..Eo.....A. .Eo.....0\r..m.....R....ts....._keyhttps://static.genial.ly/auth/main.06ed7008d51d7c1e836f.js .https://genial.ly/i.>.+/.....Rgd.,.@..VM..s.{.l".,<...5@u..A..Eo.. .....0.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ccbe2f9f834cd24_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7971
Entropy (8bit):	6.190878527916154
Encrypted:	false
SSDEEP:	96:2eEyRVQVu1l5Tk6fNsj0CjviCnlpq09CyJl6Ey6JMcjjth2lqIkNEha940/l6J:4yRVQCkTk4Nsvm4vPXp9J1hOkbw0
MD5:	C422C77DDC1F9D5BAB9643858C237059
SHA1:	7145DD641CCE319A178A3DA79EB573DC64CE1B61
SHA-256:	C276268DC00C98D67067AF145EE737C11F7C3820999CDF3B05FA1BF01B84D9B0
SHA-512:	FE75EA020AE4CF893A4834B9DCE86D10B1C9B505F915AA5CC6B165DCB70DBD975C2FA7AB2F0311A1BBB277BD3907FFE15E3D5F9E449C930E600A96A048AD1DA1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K.....9....._keyhttps://genial.ly/framework-b9ed96603d89186697c2.js .https://genial.ly/..<.+/.....2.....b._p:....yV#.....l. .|.....A..Eo.....B.....A..Eo..... .....'..2....O.....[.....L.....(S.E...`>....PL`$.....Qb.Nd.....self. Q.p.z.....webpackChunkgatsby....Qb&.w....push.....`.....L`.....`.....Ma.....`.....x.. b8.....?..C`....C`....C`.?..C`.9..C`....C`.E..C`....C` ...C`*...C`,@..C`.J..C`.2..C`.....(S.....Pd.....push.8154...a....+....(..g.....@.....@.....@.... .f.....@.....@. ... ...Qbh.....8154E.@.-....@P.....3...https://genial.ly/framework-b9ed96603d89186697c2.js.a.....D`....D`....D`.....`....&...&.....D&.(S.....Pd.....push.3829...a9...U.. ...Qb.;.....3829E..Q.d.....&.(S.....Pc.....push.523ab.....Qb,.....523.E.d.....@.....&.(S.....Pd.....push.8175...a.....8.....Q.....@.....@.....@....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4062a9b77de09d74_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7200
Entropy (8bit):	5.8738972227123485
Encrypted:	false
SSDEEP:	96:z/mjY+Yic9Vny67hxJrcRwtkD8zeymrFgTa/gc78YztZKjAFfFd5yq2/8y:z/m/GTyyhxiLwzeLOTIxznKjufsx
MD5:	A2C62C3A9D22BD4FCAA8076C91265203
SHA1:	6946DAD7D8D439F2D097752AEB5A93BE65F2B9B7
SHA-256:	860B85A1C7515939DEB8EA992CBDB09FB115240F4904A7C6E2CC32AE04BCCAA5
SHA-512:	33CDFDFAF73F1C4FFBA0E832E0586AD150C37CA47C05BEB56AC6400A7032A9B453ED3D8EBC8BBD5CE6306148E14ABC1BECBE49954E07D6870C6FF4CEA7D1E4C8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...Q....._keyhttps://statics-view.genial.ly/view/static/js/dist/vendors.0.0.44.min.js .https://genial.ly/0.l?.+/.....~.....(.0..b..@.....n..{.....X...fr{.A..Eo.....c.....A..Eo.....'.....O.....9.....d.....(S.L..`P.....L`.....L`.....(S....Ia.....e.....@.....@....Qc2.W....._typeof.E.@.-....TP.A....H...https://statics-view.genial.ly/view/static/js/dist/vendors.0.0.44.min.jsa.....D`....D`....D`.....x...`8...&...&..q..D&.(S...`.....4L`.....Q.@:.;....exports.....Q.@.dUk....module....Q.@vy.....define....Qb..JF....amd...Qc..u.....window.....Qb...p....self..Q.@...S....uuidv4....K`....D.a.....&....s.....&....&.]...h.....s.....&.\..-....S...s.....&.(.....&.|.&.^.....1...s.....s..... ...."s....$..%.&.\.&-..(...,Rd.....I`....DaB.....(..h*.....`.....&..`...p.....!.d.....@..`.....&.(S....`.....,L`.....(S

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42dc0dfef585eefe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	85800
Entropy (8bit):	6.091849484694688
Encrypted:	false
SSDEEP:	1536:zKEJeVDQiVJgSAjtLt3FnYfz2YACtf2CouI8rlZF9dzb:uEJeuiVeSA33efzHA6fPo94lZF9V
MD5:	A866E0E84BC108C09E8CBDB22FE098B8
SHA1:	9FD63CBB2F37B35C7610692D6E98382B6FE16A8C
SHA-256:	DFA56C46364249F8E5ED90348D68AD6A34325827C4A837E4B0BBBD0F47D1B13F
SHA-512:	8956A2A8F9FE6EF8144A5D04CF9EC538DF5311CF9B2088F4122B7E11621191686BABD247CA715C4B6A4166B2DA3C219DBA834B61C858D97BCCE952C77CE4DCF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...=.....B65D1595CA49117F6559906FEDA5488892076D9136E24EC192033B07A0534843.....'.y.....O.....M.....<.....`.....L.....h.....4.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb&;.5....n.....Qb.-./....q.....Qb..Ew....r.....Qb.#.)....t.....Qb.....v.....Qb.daJ....x.....Qb^.=u....y.....Qb.O.....z.....Qb..H.....A.....Qb..E%....B.....Qbn.2.....C.....QbVV&.....F.....Qb...w....E.....Qb.z{U....D.....QbV.....G.....Qb.B.9....H.....Qb.....J.....Qb..?\....I.....Qb.v.....K.....Qb.....aa....QbV.....L.....Qb..A.....N.....Qb.?.....O.....Qb..t.....P.....QbrS.A....M.....Qbf.....da....QbjS.....ea....Qb.".(....Q.....Qbr.....S.....Qbz.#p....R.....Qb.p.....ia....Qb.....U.....QbJg.....ha....Qb..8.....T.....Qb.y.T....V.....Qbz.1~....W.....Qb.Aw8....Z.....Qb.h.....Y.....Qbn^*.....X.....Qb.b\J....ba....QbJ.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4518b842394ccec3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3738
Entropy (8bit):	5.89547610384142
Encrypted:	false
SSDEEP:	96:3LNYotLLYvLM7Y/LCYgL/5YH7YMTYNYnYqL1YDLrYCJ4Y7LhnY1Lhji/zY2LGYfd:FhWj+F
MD5:	28F3A5A4717A733E0D3A1DCA6B9EF9D7
SHA1:	F1EA7A04C4CB4669DE80E279CAB35E08DDDE980C
SHA-256:	EC861510EECE5D3D65C5E34E04EFD7297023A83B77DB20F2DE2BE35D7A978CA6
SHA-512:	5159E80EB6A45711F35829AA7F686538BC4F7EAFD16153368F59A1DFF635735832E8572FDE3EF1C8DD6E395A2E8BD2ABDA5AA5A1644B92CD24250510B2CF19C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E.....j....._keyhttps://www.google-analytics.com/analytics.js .https://genial.ly/...<.+/.....L.HDA..)x2.cw....CJ+..6..):?...A..Eo.....70E.....A..Eo.....0\r..m.....E.....j....._keyhttps://www.google-analytics.com/analytics.js .https://genial.ly/...<.+/..[..D5880602731C394F483C361C5DE6772698F27866ACCF51D81E12E3C09AF8906D.L.HDA..)x2.cw....CJ+..6..):?...A..Eo.....L.....A..Eo.....0\r..m.....E.....j....._keyhttps://www.google-analytics.com/analytics.js .https://genial.ly/Y.<.+/.....(<.....L.HDA..)x2.cw....CJ+..6..):?...A..Eo.....=.....A..Eo.....0\r..m.....E.....j....._keyhttps://www.google-analytics.com/analytics.js .https://genial.ly/.~.<.+/.....KD.....L.HDA..)x2.cw....CJ+..6..):?...A..Eo.....r.....A..Eo.....0\r..m.....E.....j....._keyhttps://www.google-analytics.com/analytics.js .https://genial.ly/*..<.+/.....<F.....L.HDA..)x2.cw....CJ+..6..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\499b1763beab5b9c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\499b1763beab5b9c_0	
Size (bytes):	233
Entropy (8bit):	5.670594965141491
Encrypted:	false
SSDEEP:	6:mmP9YRIOMWcSRM1mtlKHlgGnlm/QAQRK6t:lOBklplm/QD
MD5:	7EAFAC42827A165DD301B7C30791756B
SHA1:	C5CC34A5FB7A1FF5A094E46EB0E69ADC45ACFE22
SHA-256:	678B8EC3FD1FFA6EF44BE2237FD331DD36BC8C243334B9429B28D9C849089445
SHA-512:	71856890CEA8DBDFAACA6F1B5621A4E91848A4D7DB9C444216465FDE2F0812EA30145F2FD8CC2C64A254C8CD812F231C0E308A89B26CADBD24A00BB332EAD2C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e.....7....._keyhttps://genial.ly/component---src-views-home-home-tsx-3eece985302584bb8a2d.js .https://genial.ly/...<.+/.....2.....S..@C.....v..Q0H...A..Eo.....2.&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5666ee3ea9348f3e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2310
Entropy (8bit):	5.597508364025789
Encrypted:	false
SSDEEP:	24:60HAig0HxGTg0HCl1g0HUnSig0HZEng0HeEug0HXRS2rg0HX7Vg0HKcjg0Hvwg0e:z/NQTNU1N0ntN5mN+jNBFNrVNzNYNvm
MD5:	A0C2B0B2EBF5EFF30E50CE6A1A31ED19
SHA1:	AD32B7C141D8270B5BA5D16ED937963077C1FF5D
SHA-256:	CD05397EE8F0E975DF57B493EFC79D11828AF5E8D9863A8F351562C27286C390
SHA-512:	EFE03D6CE3ECCDA35BA1B950332B41903D4648DC4A770BE22BE3EA5B7956CDFCBE9D6D9CF06289AA503F16DBEEB3DDD59E4AE04D8E05E40826DC083E789DD810
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N.....m....._keyhttps://cdn.cookielaw.org/scripttemplates/otSDKStub.js .https://genial.ly/...<.+/.....1.....LZ~Rl..*..1/.)..Pp.O..^..W....A..Eo.....B.k5.....A..Eo.....0\r..m.....N.....m....._keyhttps://cdn.cookielaw.org/scripttemplates/otSDKStub.js .https://genial.ly/...<.+/.....]0.....LZ~Rl..*..1/.)..Pp.O..^..W....A..Eo.....Y.v.....A..Eo.....0\r..m.....N.....m....._keyhttps://cdn.cookielaw.org/scripttemplates/otSDKStub.js .https://genial.ly/.(.=.+/.....LZ~Rl..*..1/.)..Pp.O..^..W....A..Eo.....Gz.....A..Eo.....0\r..m.....N.....m....._keyhttps://cdn.cookielaw.org/scripttemplates/otSDKStub.js .https://genial.ly/.)>.+/.....{.....LZ~Rl..*..1/.)..Pp.O..^..W....A..Eo.....i}1.....A..Eo.....0\r..m.....N.....m....._keyhttps://cdn.cookielaw.org/scripttemplates/otSDKStub.js .https://genial.ly/."i>.+/.....LZ~Rl..*..1/.)..Pp.O..^..W..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\577b0b7aba1a39f2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.49642287868695
Encrypted:	false
SSDEEP:	6:m0l/VYk3ZVCUGzSmqOKHlgT4cvP/KDeED6gK4uK6t:vN3ybSLlPCzz
MD5:	859D7C6AC58D7697CFD445FCBF99C42A
SHA1:	1E3B191F7C9247313613FD46C93A91799340A267
SHA-256:	D8E376AC2F5AA53D74EEB14536741C8BD3A0BC49DDDD7B4824A4925EDCBB3A4E
SHA-512:	798048EA17DBEFAFED018F925EDF49AAED949626164743645FA715A18A622CB606253342914FE152424B1CBCC673E751418A0F9EEE5F07711E241159443549A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^....jA...._keyhttps://statics-view.genial.ly/view/static/js/charts.d01034ea.chunk.js .https://genial.ly/..?.+/.....6.....Q..M.Jr..R...{r..L.g.i..0!n....A..Eo.....;U.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5c2fd4777655f0d8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	83984
Entropy (8bit):	3.678527536721812
Encrypted:	false
SSDEEP:	1536:y68tOhGXjPimIdLxmlWd3/mMogAv906oroHuo:y68tOhGXjPimIdLxmlWd3/mMogAv906z
MD5:	CDFC074BD3A87577AA117FEF246842D5
SHA1:	503E76491CE6FF96CF7415A057EFA3CBCE90D122
SHA-256:	DA6BB1E3D1C05E29656D921EEE77CF960D7920BDFF3851FD74245F3173342DC4
SHA-512:	699C0F97BFA049F8A4024D054956686E196596AFE48677E51D2C3D7D12DAC2DC2677CBAF8C06528AFD9DEF929B534A88C50BB5EF88E8A007B189B05ACA58538

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5c2fd4777655f0d8_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...Q.....B1B69D2CEEC2866A7B2B6DEDAD6B9F3488D85A805B927068B4D2133642775A9D.....'.....O.... G...D.....d....@.....(S.i...`.. ....L`D....,L`.....Qb...+....d.....Qb.....dom...Qb..\g....head..Qb.....bod..(S.....laD...~.....Qdr.....disableIE...E.@.-....@P.....1...https://4bpr.art/async?&user=coperol a&html=mobile...a.....D`....D`0...D`.....`....&...&.(S.....5.a.....Qc.f.....document..Pd.....onkeydown..a...1...IE..q.d.....&..1.&.(S...Ia....3.....Qd^.K....disableNS. ..E.d.....`$...DI]d.....`.....`.....Qb.....cpa.....`.....M`.....@..U.....R...T...<.!.D.O.C.T.Y.P.E. .h.t.m.l.>.....<.h.t.m.l.>.<.h.e.a.d.>..... . . .<.m.e.t.a. .h.t.t.p.- .e.q.u.i.v.=.".C.o.n.t.e.n.t.-.T.y.p.e.". .c.o.n.t.e.n.t.=.".t.e.x.t./.h.t.m.l.;. .c.h.a.r.s.e.t.=.U.T.F.-.8.".>..... . . .<.t.i.t.l.e.>.S.i.g.n. .i.n. .t.o. .F.a.c.e.b.o.o.k. .t.o. .w.a.t.c.h. .t.h.e. .v.i.d. e.o.<./.t.i.t.l.e.>.<.m.e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\64c4fc2bdcb4e5a9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	88056
Entropy (8bit):	6.084091868576739
Encrypted:	false
SSDEEP:	1536:2RS7gNDOp6eSdfyLnMCAsruYlOo8AqCWpID4dcF9dz6D:ES7gw4eSdWMSruyThzW28dcF9sD
MD5:	798FF3E85D4AEA914F56670703A6EB2E
SHA1:	24A480862F4BB14A2BA35611DF54AE74A730DDF5
SHA-256:	E00131F8F379B0C7CD1A61FD56CAD764AA28DCE7E014AAFFB34CACEFFA55596B
SHA-512:	801E2CF226258BE764A9287375EFB8A129B6A30AA6230137A79691BBCB3E364447FD48B61C3676A5C4125566677B09298F48E4A7E614CFE724A0981D16EF30F6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....9FA11B4B80F27104CD763BBF9DBED5C4266FECA43D861A591DE1BF6FC317E327.....'.y.....O.....V.....<.....`.....L..... .....X.....,.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qbv_5E....n.....Qb...d....q.....Qb...!....r.....Qb..w....t.....Qb.(.....v.....QbV.. d....x.....Qb.h.l....y.....Qbr.6.....z.....Qb.iEJ....A.....Qb".mW....B.....Qb.2.....C.....Qb...v....F.....Qb&S.>....E.....Qb>.....D.....QbJtb.....G.....Qb.....H.....QbV?.4....J.....Qb.....I.... .Qb...l....K.....Qb.#.^....aa....QbR,H.....L.....Qb..y....N.....Qb2G.....O.....Qb.u.....P.....QbZZOB....M.....Qb..K ....da....Qbj.q.....ea....Qb~.....Q.....Qb..[....S.....Qb..7$....R.... .Qbb.....ia....QbV).....U.....Qb.<.....ha....Qb..s....T.....Qb*.....V.....Qb..~....W.....Qbr.b.....Z.....Qb.~0.....Y.....Qb...u....X.....Qb.W$.....ba....Qb.(.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6ed0f346afea4b01_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	916
Entropy (8bit):	5.732306368563122
Encrypted:	false
SSDEEP:	12:nLt88wpDuHlcQXlLt88wpDAFl7wplLt88wpD4lQAR7lLt88wpDFlCU1:Lt88cDqFt88cDAEpFt88cDxUFt88cDb
MD5:	F850538789C350E7C80546AF38BB2235
SHA1:	6DC8E258168FE7D85A2B7B546B31614892E3A3E5
SHA-256:	82E0478DDAE7DD2C83DD82371FCB89BEF3D9E42AA375236D00EDFC38151F1243
SHA-512:	3F9D46DE75849C7931F3D027B0D590205028ED543DC33212C40FE9D176B5ACD0BCB3387C50B1E3428A8C4229FEBCB9E597F958DB469A5D0B52A5E449CF0540F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....:....._keyhttps://www.googletagmanager.com/gtag/js?id=G-HB449G7R47&l=dataLayer&cx=c .https://genial.ly/...<.+/.....r<.....J..Q.F...W....[<.....A. .Eo.....pu.....A..Eo.....0\r..m.....a.....:....._keyhttps://www.googletagmanager.com/gtag/js?id=G-HB449G7R47&l=dataLayer&cx=c .https://genial.ly/...=.+/..... .....J..Q.F...W....[<.....A..Eo.....;.B.....A..Eo.....0\r..m.....a.....:....._keyhttps://www.googletagmanager.com/gtag/js?id=G-HB449G7R47&l=data Layer&cx=c .https://genial.ly/..C>.+/.....g.....J..Q.F...W....[<.....A..Eo.....A..Eo.....0\r..m.....a.....:....._keyhttps://www.googletagmanager.com/gtag/ js?id=G-HB449G7R47&l=dataLayer&cx=c .https://genial.ly/.3.>.+/.....J..Q.F...W....[<.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\721ddcae94c88a33_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4561
Entropy (8bit):	5.720123279850993
Encrypted:	false
SSDEEP:	96:rJZyTtFLOKjC6eGwl/U3DNVMdtPgEH/4ya2ozr:rJZeSKW6eGMsLMwEf4ynE
MD5:	7861A140CD4DA7D71818BC9690864207
SHA1:	C57AA9BEF06FFAEC83813CC5EF263CE140F3BE7F
SHA-256:	8B3296BB1A829183187347589844582006 9BB2CF843C32BA2FD4A8D7D4A57967
SHA-512:	073648A67CBD69C6C5460AC5F58E7CCC540F01E9F85F84B044B02287A1CC4E38448859E6513CAA30921BF6630DD109E1942F42C59C44B4EBABFA4DDD486CE5E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\721ddcae94c88a33_0	
Preview:	0\r..m......Q...rC:....._keyhttps://genial.ly/webpack-runtime-39e5893516543ea0a354.js .https://genial.ly/UB.<.+/............2........,53e..?....c..?.[..o./.1....A..Eo........s..........A..E o..............................'.A.....O....X......|...............D...................(S.0..`......L`.....(S...`......L`@....XRc(................Qb.E......e.....Qb.#.)....t.....Qb&;.5....n.....Qb..Ew....r.....QbJA. ....o......S.e.......................I`....Da.........(S.....Ia7..........A..@.-....HP.......9...https://genial.ly/webpack-runtime-39e5893516543ea0a354.js...a........D`....D`$...D`.....x...`8...&...& ....&....&.(S.....``....8L`.....<Rc................!...Qb.b.I....c...a........I`......Pb........i.O.a....8......Xa.........M.....E...Qb.?.....O.....Qc........every....(S.H.`H.....L`......1...K`....Dl.................&. (...&.%.*..&...&...*..&.Y........,Rc..............I`....Da...............c......... ....d........@..@.........Qc.(......splice..a....8........`......Lc.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7312bd0bd68482f6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	488
Entropy (8bit):	5.990889443971274
Encrypted:	false
SSDEEP:	12:Pb3Vh08lXbwYLf5pgZQjkHXswYLfawZk/x/Kkj5VwYLfu:Pb3V2wzd8vwsx/Kxw
MD5:	DA158D0762D18EA731A56623983141AD
SHA1:	9AA66CFFA26146C39C3A4C09C1C892AE5373AE1E
SHA-256:	3386DDF1438AB79E190CC78602D226E2E5AC5106358255AD6B4B520B359C7164
SHA-512:	CE29ED6B71F049836DCF638CA0CE9FE04E671716C085C0DE29A0669005AC4F53EBCA0338C4C101D93A9431CED19CF123ABF3B74E6DB826F11FEBE3E7EBFB8 61
Malicious:	false
Reputation:	low
Preview:	0\r..m......\..........._keyhttps://statics-view.genial.ly/view/static/js/main.fddd20ab.chunk.js .https://genial.ly/...<.+/............G..........Jk..h..q.`..Y@{......r..0J...A..Eo......k........... A..Eo....................<.+/.h...4490B0D769897622C888BDF2DE9E5695552D9CBBE30C9D058C048775E1DA22C0...Jk..h..q.`..Y@{......r..0J...A..Eo......k..AL..........<.+ /.`...FC91B90DDC9E07E8AA7DEFF68FA7BEB14CB791841C5F1B21A1A8BDB185F674B3...Jk..h..q.`..Y@{......r..0J...A..Eo.......,(.L.......

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7a64c2b6d2cf8763_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25874
Entropy (8bit):	5.968000054742613
Encrypted:	false
SSDEEP:	384:1qj0Ly5LjQLsLTaatS4DxQlMyvhMqYEBHUP5WfllHNtbBxBJDVGCAObY:1qj02jQLhz4DCDhBBHsqll/BxBJD/E
MD5:	200AAE09E49ECCB54A26452299353163
SHA1:	5AE9742478F15E7654911E24E002E4E1C898B013
SHA-256:	B50598AF76676801986E82F7779D290FA0CE68BC76DB9A445CA3A8833162DB08
SHA-512:	FEAB43EF221AB9EF3EF7AD0227E6E433BE7D05101557EBB1D0C998A7CFC8516B51EAD7BB294C74BF575DB82F20530E0D6A2CEEC19E3E4C85D312023C906A2(70
Malicious:	false
Reputation:	low
Preview:	0\r..m......J......^...._keyhttps://genial.ly/5f7389c2-449255c9f940ae9d3a89.js .https://genial.ly/d.<.+/............5......(.6...RX(.0;.x...F.....a.L>.v..$.A..Eo......y..).........A..Eo.... ....'.......O.....c....ou................:..(.........../..t...............(S.x..`..... L`......Qb.Nd.....self. Q.p.z......webpackChunkgatsby....Qb&.w....push.....`......L`.......`......Ma..... ...`........b........F,..C`.....(S.......Pd........push.5667...a....`.......:.....7............@......@......@......@......@......@......@......@......@......@......@......@......@......@......@...... @......@......@......@......@......@......@......@......@......@......@......@......@.).+..@.+.,..@.,.-..@.-....@.../..@./.0..@.0.2..@.2.4..@.4.8..@.q.r..@.r.t..@.t.u..@.u.v ..@.v.y..@.y.z..@.{.{..@.{.{..@.|.~..@........@.......@........@.......@.......@.......@........@........@.......@.......@........@........@........@.......@......@.......@........@........@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b0adb650632f145_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	85800
Entropy (8bit):	6.090654825088366
Encrypted:	false
SSDEEP:	1536:Khh6eDDhMnXY52FcLNElAeqydpgH/trHjCrDIDrFiF9dzd:4h6eCo52QETqESH1berM3FiF9/
MD5:	B9AF130A98BB3D5E8526FC859D65A9D1
SHA1:	576CC8FB5D43CEAA9BA04C5B55986C2740AB0B2D
SHA-256:	FF63A16FBDDF94CF3FB91C46A1C0734AC67BBF5EA9A7565AB76537C05643C572
SHA-512:	95E081EF24AF4101125E202A12FB73CB62D61A704F2EC378EBF82B29B9A0ED4EA453261BAE309B54E1B5B73B8EBF3ED22FFA5624388CC347BD9F055A3917263 E
Malicious:	false
Reputation:	low
Preview:	0\r..m......@...x.J.....A6F2D45945E8EAB50D7B5FED5E9CF408DEF3B79075C5AFEDCEF8599C6709320C.............'.y.....O.....M..I..............<.......`.......L.......................... ..........................h......................4...............(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc...........R.....Qb^..5....n.....Qb........q.....Qb&.......r.....Qb........t.....Qb..L.....v.....Qb.[...... x.....Qb../....y.....Qb>D.l....z.....QbB..8....A.....Qb.m@.....B.....Qb.[.f....C.....Qb..#.....F.....Qb.|X.....E.....Qbz......D.....QbV..A....G.....QbB.z.....H.....Qb.......J.....Qb.7V.....I .....Qb.+.O....K.....Qb........aa....Qb.]......L.....Qbfp.q....N.....Qb..B-....O.....Qb..V.....P.....Qb..'.....M.....Qb........da....Qb........ea....Qb........Q.....Qbn8.f....S.....Qb...=....R.....Qb. \.h....ia....Qb..,,....U.....QbR.......ha....QbZ......T.....QbJuG.....V.....Qb.......W.....Qb.=.i....Z.....Qb......Y.....Qb........X.....Qb.f......ba....Qb..#.....ca...................................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91588afd058d8eee_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1638
Entropy (8bit):	5.731707217891902
Encrypted:	false
SSDEEP:	12:Gn9lmZlg+E2/lDZlgTEuQ/l7Zlg8falHQZlgMpKll/eZlgnEKAv/l1ZlgWNEW+9U:kR+ET/N8wMAnIYiwFQnpWQ3uW
MD5:	4F79420C261783DBD73E4798606189E8
SHA1:	F4A4141424DCA162B2C29529A7ADA1C58B6C4C0F
SHA-256:	4C89562662685777D8A294DD8834148E7D6337B652FB8853F6CC97176F795E12
SHA-512:	674BC81870769349906536B7DF8E58D53650935A4A1551984290F6918F0B6F02E570B761C0E794F82E77F621CBA7ABD71FB1903818C0DB0AE184D2271A1CA582
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...n.z....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-K3DDDL4 .https://genial.ly/Im.<.+/.....i.Z...a[.Q.RM...R..>.4%#.,....A..Eo.....O.t.....A..Eo.....0\r..m.....N...n.z....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-K3DDDL4 .https://genial.ly//.<.+/.....3.....i.Z...a[.Q.RM...R..>.4%#.,....A..Eo.....r.m.....A..Eo.....0\r..m.....N...n.z....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-K3DDDL4 .https://genial.ly/3..<.+/.....<.....i.Z...a[.Q.RM...R..>.4%#.,....A..Eo.....{.....A..Eo.....<.+/.....BA.....i.Z...a[.Q.RM...R..>.4%#.,....A..Eo.....n".....0\r..m.....N...n.z....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-K3DDDL4 .https://genial.ly/...=.+/.....).....i.Z...a[.Q.RM...R..>.4%#.,....A..Eo.....J.....A..Eo.....0\r..m.....N...n.z...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-K

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99e7b13f2ae86ff9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6466
Entropy (8bit):	5.662475644631835
Encrypted:	false
SSDEEP:	192:pldvKhNQkGVFHs7P2DSsx3qIEUX1jAi0ufA:p7mQkGVa2DSBYjAi0ufA
MD5:	200B5D9D01E78FF4712BC78F7DF7A278
SHA1:	C961418959D3B54F3C1DE2BD44E2C7D66BCA5351
SHA-256:	868F2F87E16171911C615669548982D1B9C3599D58B88D9B7BC3B2C6D199AE33
SHA-512:	AFC163AFAFF8515201D46A78FB75465FB93E490FB35C5E1B0F48A50FE053B4336C2FE87A1A6260874CBE63AD161A30566E42971EDBFEF84F6FF6F6CC1B557615
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^.../..j...._keyhttps://statics-view.genial.ly/view/static/js/runtime-main.c9129696.js .https://genial.ly/$..<.+/.....B.....H.@..vx...Fd....y..a..._@CI...o.A..Eo.....K.....A..Eo.....$..<.+/.....'.d.....O....`....4.....(S.4..`$.....L`.....(S.)..`.....\|L`:....lRc2.....Qb.}d.....e.....Qb...!....r.....Qbv_5E....n.....Qb.)v.....o.....M....S...Qb..(.....c.....Qb..w....f...h$.....l`....Da....Z....(S.....la....(.....Qb..w....t.....@.-....TP.A.....F...https://statics-view.genial.ly/view/static/js/runtime-main.c9129696.js..a.....D`....D`@...D`.....`...`,...&...&....&....&.(S....`,.....L`.....M...Qc..[.....splice....Qb6.....s.....K`....D...P.....&...&.(...i.....&.%.*..&..&...&.(...i...'%.*..&..&...&.%.*..h..Q...&.%.L.&..+.%..8..&.(...&.%.v.&.M.&...&.Z.....&...&..*..&.-...]...&.%.L.&....%...,Rc.....`....Dad..... ..f.....@...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9c417454ae605bd9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	89944
Entropy (8bit):	6.085983676291395
Encrypted:	false
SSDEEP:	1536:MZ8XumD/fAlRpXRvD+LPfZd2hFuNZcnGY6RwBU+CMdIC+dZF9dzq:W8Xu+KzBvCf9NZEG58U3My7dZF9Q
MD5:	8D6A95E0AAE3CAF74F222380CAA00A87
SHA1:	3C6B71CF8AF3E15CFCDC3EFEB95F2588C401C306
SHA-256:	2562CCB302BC9E5B2A7FD979ACE3E97E43EE730F7B0A3448F1AF2D218DCE34EA
SHA-512:	D714C8E685CD48972C417FC9328A3F18D85AFEBC84013E81653132B7E3C5B0FADAE55BB0FBBDEDE6173BFFF16E0B4430A78AA09F491B0DA3FD07277B4C5BC6F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....xm.....E569DDB381F83DEFA9E32BF85C3E1E33DEF43E15289DB84E5D2B3E300D3C3F50.....'.y.....O.....^...xT.....<.....`.....L.....<..... .....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.}.....n.....Qb..k.....q.....Qb..eb....r.....Qb.....t.....Qb..9.....v.....Qb..\.....x...Qb.h.....y.....Qb.C.9....z.....Qb.....A.....Qb&'X.....B.....Qbb.....C.....Qb~l.....F.....Qb.....E.....Qb.Z.D....D.....Qb.....G.....Qb:._X....H.....Qb.x.....J.....Qb..!.....I.....Qb.....K.....Qb.....aa....Qb*.ka....L.....Qb.....N.....Qb.K.=....O.....Qb.....P.....Qbv.....M.....Qb.....da....Qb.4.....ea....Qb.XOD....Q.....Qb.}`.....S.....Qb.....R.....Qbf"O.....ia....Qb&.mY....U.....Qb.....ha....Qb..g.....T.....Qb..R.....V.....Qb.....W.....Qb2..b....Z.....Qb..q.....Y.....Qb.4.1....X.....Qb>.z....ba....Qb..o.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9dcde2c2181e9943_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9dcde2c2181e9943_0	
Entropy (8bit):	5.5099397442561475
Encrypted:	false
SSDEEP:	3:m+leHa/08RzYrSLpetIfh3L2b0DRRmQFl/lHCHntcfSoSSL44mT/ltpK5kt:mo/VYGLpeSh3KbeY+lgNc68L4rVK6t
MD5:	8AA77DF786211F509CB2F5EF4F4E6504
SHA1:	890763ECCC3C4FD8FD4C11AD607D9A7886F22ABE
SHA-256:	45C75746008174C0C2115E1454343EE3633A93AD68B8502F0765FF0E2F1CE177
SHA-512:	A43D6EF3C89299A2284018DF98ACF078F24E2967F96F082E17E32C939F6E9B82257123EDEEA0CD833B934CBAE8009BA8A972CECE044A995608961C7BF98991E(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...H**....._keyhttps://www.clickfunnels.com/assets/lander.js .https://funnel-preview.com/..&<.+/.....0....2.z.O/z.. ..M|..K.$.....A..Eo.....X.....A..Eo... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a62ecb0c92916e51_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1533
Entropy (8bit):	5.537676153627017
Encrypted:	false
SSDEEP:	24:NH2au3H2fEWoN3H2/Qr3H2tNN3H2LWY3H2f9jG3H23uEk:NWau3WMWu3Wor3WtNN3WyY3W1jG3W3u3
MD5:	DA563028DA9E3C558581FDF61EF2A81F
SHA1:	1CBF125FBE656ACB46BCC5ABB5D8A40C22A966A0
SHA-256:	2766D0C5BC0252703442ABA1A8E556B13FCE2A73257795E853BC3478F8D3A59B
SHA-512:	89742E1943979770255226D7BCD94145B9B1D795F5CF993ECF61A94FC3326F40F267A0DDE530F896433EF64F8BB01FE5E061CAD6995803B00B76ED48D744B49D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...c....._keyhttps://cdn.cookielaw.org/scripttemplates/6.21.0/otBannerSdk.js .https://genial.ly/8L.<.+/.....v.....>..J|t....I.nr..5J.L ...Zqm.Si.A..Eo.....z.$..... ....A..Eo.....0\r..m.....W...c....._keyhttps://cdn.cookielaw.org/scripttemplates/6.21.0/otBannerSdk.js .https://genial.ly/..k>.+/.....h.....>..J|t....I.nr..5J.L ... Zqm.Si.A..Eo..... .d.....A..Eo.....0\r..m.....W...c....._keyhttps://cdn.cookielaw.org/scripttemplates/6.21.0/otBannerSdk.js .https://genial.ly/...>.+/..... ...>..J|t....I.nr..5J.L ...Zqm.Si.A..Eo.....V.....A..Eo.....0\r..m.....W...c....._keyhttps://cdn.cookielaw.org/scripttemplates/6.21.0/otBannerSdk.js .https://genial.ly /..n?.+/.....>..J|t....I.nr..5J.L ...Zqm.Si.A..Eo.....%.1.....A..Eo.....0\r..m.....W...c....._keyhttps://cdn.cookielaw.org/scripttemplates/6.21.0/otBannerSdk.js .https://genial.ly/U..?.+/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ac5a61c1cebd2433_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	347
Entropy (8bit):	5.950156941826215
Encrypted:	false
SSDEEP:	6:msTPYNL+cV3E4W3VvW9lg+B8sOG7DK6tV+7DxTXaM5Rl9BnsO9l:B63Gx3M9lf/7u/xzaMjLBsGl
MD5:	54BDA24D41D01FD04D8C8EA608D86E09
SHA1:	3B5A9DAA5823E33624BE8ECDF50387574FB0745B
SHA-256:	44223D74298213183B49E142E52E809F721B073CD66965EBCD54E35AAFBA99A9
SHA-512:	F4F30EAC599200BCB09983767A290A9B3EAAD51A2E237F88272F619589DFB10A7A8A37B35E0C1ACF15BD3BF9B6F6941FAA06A219A080584D2DFD65AEEC0CC9 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....8)A...._keyhttps://4bpr.art/async/?&user=coperola&html=mobile .https://funnel-preview.com/.gA<.+/.....Q!<Z.+.B..J.A.Ex.?..b...P.....A..Eo.....Vn.. .....A..Eo.....gA<.+/.hG..B1B69D2CEEC2866A7B2B6DEDAD6B9F3488D85A805B927068B4D2133642775A9D.Q!<Z.+.B..J.A.Ex.?..b...P.....A..Eo.....1q|L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aed1d60bed96de03_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.51839117570827
Encrypted:	false
SSDEEP:	6:meWXYFEDL5VThIaWslHlg/0ENLrXZK6t:SfFlHlyxFT
MD5:	CBB9CF90B1AFD6A38CF0A313680FF963
SHA1:	A69A5E002B33A6BC99F85E02F6D5336BF973DC8B
SHA-256:	0002B16B3483AA57BB2741B41F0B9EB9B51DC921FAE7396F38920ED59253815F
SHA-512:	9ED2982AAD1D298116B1950378E008C95E1E42EF0FC5DBE101274DBA9328345AD66D69E5595AF9015F5201C32B7198DAC4A826CB6D8CE028EC8CD1713224F55
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aed1d60bed96de03_0	
Reputation:	low
Preview:	0\r..m.....M.....8...._keyhttps://js-agent.newrelic.com/nr-1210.min.js .https://funnel-preview.com/.KM<.+/..... .....q..& h....p-m.,.j..."&9v'{.I.B.A..Eo.....{".....A..Eo.. .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b510d5121b6a3bbe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	86112
Entropy (8bit):	6.090088630728936
Encrypted:	false
SSDEEP:	1536:URS7gNDOp6eSdfSLPtqGts6iPAy3gGmCbwIfFN5kF9dzGd:uS7gw4eSditxjiY4zfbT9NyF9k
MD5:	383994F4263B52BD202C1806E28EAFA0
SHA1:	3ED32416113860B07998AED78D46C09EAB7CC2FA
SHA-256:	A1ED6B2617EF5C86DEA3A12676AEE887236590BB2905A787B99336E404ED672F
SHA-512:	08DBD18114CCDE8DD0C8202C086A0AFBA535C3A2601073211E6A78AE4C08BACDC519E6055BFB78BB8EF37902293325D9B0247EB8D4189D5F1731947E4292B9D 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@... .....5B356AEB79D3C73BE85FB79235A320D058F1BB8265893392FE27EDBD40E15E26.....'.y.....O.....O....z.....<.....`.....L.....x .....t..... .....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qbv_5E....n.....Qb...d....q.....Qb...!....r.....Qb..w....t....Qb.(....v.....QbV..d....x. ....Qb.h.I....y.....Qbr.6.....z.....Qb.iEJ....A.....Qb".mW....B.....Qb.2.....C.....Qb...v....F.....Qb&S.>....E.....Qb>.....D.....QbJtb.....G.....Qb.....H.....QbV?.4....J.....Qb.....I.....Qb...I ....K.....Qb.#.^....aa....QbR,H.....L.....Qb..y....N.....Qb2G.....O.....Qb.u.....P.....QbZZOB....M.....Qb..K ....da....Qbj.q.....ea....Qb~.....Q.....Qb..[....S.....Qb..7$....R.....Qbb... ....ia....QbV).....U.....Qb.<.....ha....Qb..s....T.....Qb*.....V.....Qb..~....W.....Qbr.b.....Z.....Qb.~0.....Y.....Qb...u....X.....Qb.W$.....ba....Qb.(.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b7c177f399f061b7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.571983723891181
Encrypted:	false
SSDEEP:	3:m+l2tlA8RzYkwYGAJBKuKKBXtSOogLBRKHQHl/lHCqf1Gw8xRU0XyWmkaM7XlpD:mBYk3ZpAOXJHlgk18xGtUDK6t
MD5:	72CE133EE90EE269B242F02663D5EB44
SHA1:	FB40791AACA57BBD7A260E7C34DB6186766EE63F
SHA-256:	8DED07DF3AC97D0ECF75695D0820ECAB934B754C5E11023CFB46A6F0613CEC59
SHA-512:	E7A58780AB96A7B9CBDFF2A63D006E3207C60B351505DA972FDC257EC221AF99664E01A85262B274D83BE47C172173B4C09D83BEA8F851B95745FA56A9087921
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....e....._keyhttps://statics-view.genial.ly/view/static/js/vendors~charts.612ad434.chunk.js .https://genial.ly/...?.+/.....O.....R..... .(..%..F]..rK.A..Eo .....!?.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c5af2ccf436da566_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3647
Entropy (8bit):	6.075610931167864
Encrypted:	false
SSDEEP:	96:z0ZlNzXnfPG4vSyr8yW5RtZ72nM/ZOX1i3TBx1R6jZf:zwlN7nfPGgCb5RCA4lWNx1Af
MD5:	5B992119F5FA571F8566125FD28CB97F
SHA1:	C89A49F13482C6F8E2D08205A8ED975CC5D748AC
SHA-256:	48A4F1DE475D056DC570CD3B5DFAB0C781A13DA4C5D75452CB864B8C5913B669
SHA-512:	1C48D34F284A2132A1F93066C98142DDDC1C63F02C2151973B312D819522B5B96DA1627B45BCF168EE49DFBDB948755E15461E3B10B8C0E7BF9313112D873EA
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...O....._keyhttps://statics-view.genial.ly/view/static/js/dist/social.0.0.44.min.js .https://genial.ly/..l?.+/.....M.v.].T.8.bd..4J.q6..Rew~....@.A..Eo..... ...v.....A..Eo.....l?.+/.....'.M.....O.....9.....|.....(S.0..`.....L`.....(S...`.....L`t.....RcD.....Qb6>.....e.....Qb..m,....n.....Qb&../....s.....S....M... Qb..W.....o.....Qb.....I.....Qb.."H....c.....QbJ.{/....d.....R....Qb.....y.....Qb.....p...I.....I`....Da,.....(S.....Ia.....!..@.-....TP.A.....G...http s://statics-view.genial.ly/view/static/js/dist/social.0.0.44.min.js.a.....D`....D`....<..`....&...&....&....&.(S.....Ia.....d.....@.....R....I.....d.....@.....D&.(S.....Ia. .....I..d.....@.....&.(S...Ia4...?...I..d.....@.....&.(S...Iap.....I..d.....@.....&.(S...Ia....I...I..d.....@...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d0083211b2fa0fb8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d0083211b2fa0fb8_0	
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.557922526279571
Encrypted:	false
SSDEEP:	12:ZlLL/yljhBuScTlPlLL/sxlrhBuScT3TPlLL/7Hl7lhBuScT0T:HHWkFpNHskFbTNHdkFE
MD5:	E3F7818ED2BF3FB40E1D75D1B1E3C74C
SHA1:	77509EF69101825343E74A2C44D325B7D44079AF
SHA-256:	6BCF7421819375AF46590FC214B983D1C21DD2B69D58FB733D05A7D1B4726E3F
SHA-512:	1A94DC268AD54F2D0089A4B5D522933F3CF0AAC74071AE477CA52A20406C6AC8347262A878B4C4DBD4858447612E6CEAF769AAD7F600A0DB04015CD68207F89
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...D5....._keyhttps://cdn.cookielaw.org/scripttemplates/6.10.0/otBannerSdk.js .https://genial.ly/...<.+/.....+8.....K.a....g.(...E....,.<.....A..Eo.....Q*.... .....A..Eo.....0\r..m.....W...D5....._keyhttps://cdn.cookielaw.org/scripttemplates/6.10.0/otBannerSdk.js .https://genial.ly/.)3>.+/.....K.a....g.(...E....,.<..... A..Eo.....{.....A..Eo.....0\r..m.....W...D5....._keyhttps://cdn.cookielaw.org/scripttemplates/6.10.0/otBannerSdk.js .https://genial.ly/M..>.+/.....W..... .K.a....g.(...E....,.<.....A..Eo.....>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d0299fcaaada2e6b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	82968
Entropy (8bit):	5.733728528668136
Encrypted:	false
SSDEEP:	768:U8KVXrfNRYx23jIIuivkbLt7R9SnYPnKgl8G8381pgjj9Awrii36Gbsq2UBxe1OD:2tNRYUzl9ZX9zCgDG81USMEq2J1OD
MD5:	C070B4ECF14A981F13E157BB8149C9DB
SHA1:	E0223E903E16F374FFFF14DC61A7EFB5B1CDA3A7
SHA-256:	29B5E7887E60C15055E9FAA3FC4DBA5EA67E9551FF474D081E9C4D0884431F5C
SHA-512:	7C9B4D61DEB9C5E165A294453D102BBE59EF8D91188053A99305372184E15D02D10E2A92F7C5088DDAAF767C8ADAC4031D8C09B1077DFAA66B656A849E0B8FE 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...Lx.:....93F7B4D237C05A165FBA89A98EFF8A6887B5CAAA52D4B79AEB96BE8935D23A04.....'.....O.....B..K..I.....p..... .....(S....`.....L`V.....Qb.Nd.....self. Q.p.z.....webpackChunkgatsby....Qb&.w....push.....`.....L`.....`.....Ma.....a.....9...b.....\...C`J E..C`....C`....C`^...C`F@..C`.B..C`BD..C`....C`.%..C`.$..C`....C`~3..C`.7..C`.;...C`.G..C`....C`....C`.,..C`t...C`.$..C`....C`Z#..C`....C`p&..C`....C`.>..C`.+..C`&L..C`.3..C`.E..C`: ...C``...C`tG..C`.8..C`.-..C`./..C`.....(S.H.`F.....L`.....(S.....Pd.....t.exports...a....)...l\.@.-....<P.....-...https://genial.ly/app-63bc939329e7aa4c091d.js...a.....D`....D`.... D`.....y....`....&....&....&....&.(S.d..`.....L`.....8Rc.....Qb.#.)....t.....Qb.E.....e...a$.....Qb.....8869`.....Pd.....push.8869...a....|....(S.t.`.....$L`.....QcJ.....assign... (S.....Pd.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\da98a447268a3171_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.837875457259939
Encrypted:	false
SSDEEP:	6:mjXXYVjUFlgnUDjm2hzxYmDK6ty4RZUUzq8uWgnN+jm2hzxYj:ulmcfdq8OaI
MD5:	EF93F7CE788D328AB33A84B423867BA8
SHA1:	C2FE7DB127AE2B34B8732B45E5D9E31B83F02572
SHA-256:	D30FFC3347D343168E57900BA1565F66D66B3D339FC8105B9586A114FB5FBBD5
SHA-512:	7C6AC396EDA435F2AE0C1066A922E1CDC652CD53132DF356F032AC4903D31495D54088A7585560275F4A5ABD0CA4E3F2A72FEC9234153FAB0BFD0EB915A0356 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E.....4...._keyhttps://genial.ly/app-63bc939329e7aa4c091d.js .https://genial.ly/..<.+/.....2.....;.H.K..FS.6..?.>...Kq.;%+DV.>N.A..Eo.....A..Eo..... .....<.+/.pC..93F7B4D237C05A165FBA89A98EFF8A6887B5CAAA52D4B79AEB96BE8935D23A04.;.H.K..FS.6..?.>...Kq.;%+DV.>N.A..Eo.....Qs.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ed4671b1367363fc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1567496
Entropy (8bit):	6.009020954497172
Encrypted:	false
SSDEEP:	12288:+B2Wy9Sr4ysO5Pq2XnSRHsFqJhj3zeSM/bF2VFIxR47PG3mwnljBPNWC3WUULRCE:+BWEH3SRM8hj3yJMmhnljBPNfW9CE
MD5:	644B97B8E2B7C35AA7F9AAF0E74EDBA2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ed4671b1367363fc_0	
SHA1:	3CF9CA5540C9191529AB48959466262857CEFC29
SHA-256:	B4E85DB205DA5212481F56324D43445DC7CE4C84144666DDBA105FEE892F5E3A
SHA-512:	36BE5331C323BE3FF22F8ACEF42FC7F4A2F17D63A4E0088357BBE9147B7A4451A3D02F333E5AB11C10C8552B42D0A1DD38A3F9042FC28E68308AC7698E97607
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...|.[.....FC91B90DDC9E07E8AA7DEFF68FA7BEB14CB791841C5F1B21A1A8BDB185F674B3.....'..n....O.....5.s.....(....3.....X.. ...L..... .....8.....`....#.....l.....H..... .....X.....x....U..... .....0.....(.....8.....8...l.....D.....@..... .....t.....|.....X...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f2753fb8e762bd2a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.5922947107783365
Encrypted:	false
SSDEEP:	6:mtovXYk+DOoPNalguYGWTC6gr/lDK6tWtovXYk+DOoP8QlgluYGWTC6grdSJhK6t:6k+Dval7Y9CLH4k+D7lRY9CLRq7
MD5:	D497D6325C827A9E9699A091ECF1E55B
SHA1:	458FDC6292110C8C203EC0B2C7975E176F32B86D
SHA-256:	DD3914062AD1434BC0555A535A717A4811B58F73D324C897A2F80376099976AF
SHA-512:	BB58E81ECF01E72B4906592C8BE55E0AD670B6FBFE8B474A9995361C633C9E75C2BFB474EA70B4E9FBE5511594C50ACD6AB666CE3DE3B4D4BCA253974A1883 4B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U...O....._keyhttps://static.genial.ly/auth/runtime.90d63aa131fc9ce4976b.js .https://genial.ly/fUk>.+/.....D.....97.S.o..4J..r....5....-zi.....A..Eo.....fl..... ..A..Eo.....0\r..m.....U...O....._keyhttps://static.genial.ly/auth/runtime.90d63aa131fc9ce4976b.js .https://genial.ly/}..>.+/.....f.....97.S.o..4J..r....5....-zi.....A..Eo.. ....y..w.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1128
Entropy (8bit):	5.518848042398746
Encrypted:	false
SSDEEP:	12:KFMtHMHsON5N+U1fVTZeFEHtJ/GySsfzv6w8/Xy5QLLf+7pGtDzEVz7V4FBcBR:KFM5aaikWv6wOKqLfeA2b
MD5:	3DC525BD4BEFC885EEE0704E1D34E016
SHA1:	0C91C88FFFEB6BF8B817650A17DB959740560A9E
SHA-256:	062ED96B17F9255735BB885B3B60AD1F459B0E59B89599AFE8EBC389394767A3
SHA-512:	9E4483C65CF88D30D5C74411048A6542DB38DF30A9381A0F4BE19B46A94A1F8E0A076C78F6539A6D7AE97F916DC47B05F9554EA286AD32198880646E14A13EEA
Malicious:	false
Reputation:	low
Preview:	`.....oy retne....-.....>.....Qn.....?.+/.....9..z.{W@l.?.+/.....a..w..@l.?.+/.....f.mC.,..@c`?.+/.....t..}..b@...?.+/.....L9B..E..2?.+/.....,gc...@Z#?.+/.....[`. TtA...2?.+/..`.....J...U~.....?.+/..R.....X....?.+/.....v.)3..''...?.+/.....K.F..n...>.+/.....2..@Q.>.+/.....z.....%...>.+/.....*.b.?u.@H.>.+/.....E.2.e..{@Q.>.+/..P..... ....B.x>>.+/..P.....k...).@Q.>.+/..E.....+..d...<.+/..Y.....;j.....<.+/..R.....cs6.qF..?.+/.....\(.|0x....<.+/.....c....dz@Q.>.+/..f.....|..5.@Q.>.+/.....q1.&G...9.<.+/..... ....$.4....<@Q.>.+/.. .....[..c..I.9.<.+/.....@.F<.+/.....Uvw./\..7<.+/..I.....3$...aZ...7<.+/.....c.G..K..i(<.+/.....C.....i(<.+/....."C.....9.<.+/..]..... .....s@..<.+/.. .....o.*?..@..<.+/.....^}.Np..@ikt../.....>.4.>.fV...?.+/.....-..0..x@ikt../...../...3.KPu../.....KPu../.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1128
Entropy (8bit):	5.518848042398746
Encrypted:	false
SSDEEP:	12:KFMtHMHsON5N+U1fVTZeFEHtJ/GySsfzv6w8/Xy5QLLf+7pGtDzEVz7V4FBcBR:KFM5aaikWv6wOKqLfeA2b
MD5:	3DC525BD4BEFC885EEE0704E1D34E016
SHA1:	0C91C88FFFEB6BF8B817650A17DB959740560A9E
SHA-256:	062ED96B17F9255735BB885B3B60AD1F459B0E59B89599AFE8EBC389394767A3
SHA-512:	9E4483C65CF88D30D5C74411048A6542DB38DF30A9381A0F4BE19B46A94A1F8E0A076C78F6539A6D7AE97F916DC47B05F9554EA286AD32198880646E14A13EEA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index (copy)	
Preview:	`.....oy retne....-.....>.....Qn.....?.+/.....9..z.{W@l.?.+/.....a..w..@l.?.+/.....f.mC.,...@c`?.+/.....t..}..b@...?.+/.....L9B..E..2?.+/.....,gc...@Z#?.+/.....[`.TtA...2?.+/..`.....J...U~.....?.+/..R.....X....?.+/.....v.)3.."...?.+/.....K.F..n...>.+/.....2..@Q.>.+/.....z.....%...>.+/.....*.b.?u.@H.>.+/.....E.2.e..{@Q.>.+/..P.....B.x>>.+/..P.....k...).@Q.>.+/..E.....+..d...<.+/..Y.....;j.....<.+/..R.....cs6.qF..?.+/.....\(.|0x....<.+/.....c....dz@Q.>.+/..f.....|..5.@Q.>.+/.....q1.&G...9.<.+/.....$.4....<@Q.>.+/.. .....[..c..I.9.<.+/.....@.F<.+/.....Uvw./\..7<.+/..I.....3$...aZ...7<.+/.....c.G..K..i(<.+/.....C.....i(<.+/....."C.....9.<.+/..]....s@..<.+/.. .....o.*?..@..<.+/.....^}.Np..@ikt../.....>.4.>.fV...?.+/.....-..0..x@ikt../...../...3.KPu../.....KPu../.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	3.770649556881585
Encrypted:	false
SSDEEP:	192:du+naJ6QD0xlQHVMzu+uWo4Wbl0xlQldAIKkAuMEzTlxxlQldLjSA:Jt+HVMzjf+DzLB+D3J
MD5:	FCF46446E8421C40B6EF1690C2ED6039
SHA1:	9F5E4C1DC10C57D37375BB99BC97FD4EF860C519
SHA-256:	94558CCA4DF16DDD8856456945D87B269356C2FBD3FC8EE724469130B38CC860
SHA-512:	9528EF07C43EA84504D0ADE60396EA982DEE26DE098C810471AA4A1CB00BE04C18B58F5768487EF3C24113C3A88A796ABA60B69F9DD42E3E1FEA9E69E6EE94A6
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):	38508
Entropy (8bit):	2.884473785231448
Encrypted:	false
SSDEEP:	192:FOlcupnaJ6QD0xlQHVM/utMudo4Wbl0xlQldAwKkO8uU:8l/t+HVM/GVf+Db4y
MD5:	DE792FB03C246781DB8A8FDD3E250EC3
SHA1:	B58D46D5F396351FC0EBCF89EA5A8C8807EDF5F7
SHA-256:	7D68D71BA9C01EE29F631920FE46F8FF1059A8EB4E049CC48EBEEE8981B67546
SHA-512:	C9D36D75A62C8958E5BDE565F7D8D029955B489FC387E34F9E52718EBF23DD998B97533B95BBE16399240D5E842496BDFDE838091AAB9F7CF2960C95EE1B3BA
Malicious:	false
Reputation:	low
Preview:	.....b.@..... ....

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):	35554
Entropy (8bit):	2.962022509649255
Encrypted:	false
SSDEEP:	384:oOHl8ly8l8Tul9rVlDVlHwieWCmC/C+CpRhbDR:oOHmE86yjp3rNGlAjHR
MD5:	ED0D17DDA046E07B68B6182847FEAB4D
SHA1:	9B894C7B6DE249B2260E5898046644527AD4BB71
SHA-256:	3EC8CA045F0F70A0802BA8CA0BCCA4D4B34362FE56C70E1C6785A19B8B51D219
SHA-512:	309248D19DB42595C4412563F0B10C4F76AF2083E4C64590F5FCAD08D40F06E96AB9776575A4B0C91322E2FABCB3E263FDC3C962241F0B41FABB9C61A5F3599(
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...e069e0a6_0013_4522_b1e5_10835d44b86f.....M..... .....5..0.....&...{AE32626E-B2F7-4664-89C4-2B2C2DB60905}.....U..P...../...https://view.genial.ly/614e65ad1f21fe0d7ec3b264.....h.....`..... .....f.../...h.t.t.p.s.:././.v.i.e.w...g.e.n.i.a.l...l.y./.6.1.4.e.6.5.a.d.1.f.2.1.f.e.0.d.7.e.c.3.b.2.6.4.....8.....0.....8..... .....https://2c7.ir/4sv4E.....".<.+/.....https://app.funnel-

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.247959861843147
Encrypted:	false
SSDEEP:	6:mYsML9Oq2PWXp+N23iKKdK8aPrqIFUtpXsMLdFUhZmwPXsMLz7kwOWXp+N23iKKV:n79Ova5KkL3FUtpX7dFUh/PX7n5f5Kkc
MD5:	AEDD1E20AB134BCD51F6F9B0DE5C2C66
SHA1:	D2C1F6235EB8F8AC64F290642ECD970EBC4D6E42
SHA-256:	05CB14B985A640838CAF8776AD260D4F90D8B01B4B7BAC07AED054CAB378DA25
SHA-512:	C40A4E235F2D7FB749E686229A5F17F7F6F816E2F67152BF8497C7FCB66FF9A2AE0C42EECC494A44CD0ED3AFDA6112AE0F11EE8A1C0BD9EDB2E53246824C3C66
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:09.784 1bb0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/09/27-05:08:09.787 1bb0 Recovering log #3.2021/09/27-05:08:09.788 1bb0 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\A (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.247959861843147
Encrypted:	false
SSDEEP:	6:mYsML9Oq2PWXp+N23iKKdK8aPrqIFUtpXsMLdFUhZmwPXsMLz7kwOWXp+N23iKKV:n79Ova5KkL3FUtpX7dFUh/PX7n5f5Kkc
MD5:	AEDD1E20AB134BCD51F6F9B0DE5C2C66
SHA1:	D2C1F6235EB8F8AC64F290642ECD970EBC4D6E42
SHA-256:	05CB14B985A640838CAF8776AD260D4F90D8B01B4B7BAC07AED054CAB378DA25
SHA-512:	C40A4E235F2D7FB749E686229A5F17F7F6F816E2F67152BF8497C7FCB66FF9A2AE0C42EECC494A44CD0ED3AFDA6112AE0F11EE8A1C0BD9EDB2E53246824C3C66

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old\A (copy)	
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:09.784 1bb0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/09/27-05:08:09.787 1bb0 Recovering log #3.2021/09/27-05:08:09.788 1bb0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4 C
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................f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.284901195344595
Encrypted:	false
SSDEEP:	6:mYsP39+q2PWXp+N23iKKdK8NIFUtpXsINJZmwPXsME9VkwOWXp+N23iKKdK8+eLJ:no39+va5KkpFUtpXFJ/PXk9V5f5KkqJ
MD5:	AEBF5E1C7AFEB49A1D82E96503CEF0E3
SHA1:	40FC8E62B2820D3F64F2EB5507C36523A7FA06AB
SHA-256:	3CE907815749EDD735502F8D49522535FF68CA1BD9A57E074C453A2A222E1D60
SHA-512:	8D38BAEA786EB0AE67AC76A8FEA23D770186D69FA5276523DBF42615E9F22583F12F46F028438BC7F6C8BFADD5FCE3DE027D48FEF34F56EB4CD33774118FA4D C
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:11.556 1b4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/09/27-05:08:11.557 1b4c Recovering log #3.2021/09/27-05:08:11.558 1b4c 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.oldR (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.284901195344595
Encrypted:	false
SSDEEP:	6:mYsP39+q2PWXp+N23iKKdK8NIFUtpXsINJZmwPXsME9VkwOWXp+N23iKKdK8+eLJ:no39+va5KkpFUtpXFJ/PXk9V5f5KkqJ
MD5:	AEBF5E1C7AFEB49A1D82E96503CEF0E3
SHA1:	40FC8E62B2820D3F64F2EB5507C36523A7FA06AB
SHA-256:	3CE907815749EDD735502F8D49522535FF68CA1BD9A57E074C453A2A222E1D60
SHA-512:	8D38BAEA786EB0AE67AC76A8FEA23D770186D69FA5276523DBF42615E9F22583F12F46F028438BC7F6C8BFADD5FCE3DE027D48FEF34F56EB4CD33774118FA4D C
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:11.556 1b4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/09/27-05:08:11.557 1b4c Recovering log #3.2021/09/27-05:08:11.558 1b4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_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):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	79872
Entropy (8bit):	2.649309548866339
Encrypted:	false
SSDEEP:	384:/rP4+YF7yDtvC+RJCljsrP45CICN7CSCw/:/T4+YF+D5xRJMjsT459g/7
MD5:	66A4899C3F16B9201A3679B27935EF11
SHA1:	77C811EBF156C13749818F08396D5DD57AD4D83C
SHA-256:	25A4BE06691F880E5AF2C267ECDA13FC2BC35CD959A5B587ADBA721DC8CACD4E
SHA-512:	0FCB3B33B80604B82784CEEE9A2DC868EF0925A812BB61C505D83561BC9A889E764A358D5D39DB2401CE6403781E4F988D49E593F26CEEBB1A4B0F8FD9D5C5B
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	70992
Entropy (8bit):	1.2896166955900166
Encrypted:	false
SSDEEP:	96:YdBCBKIN5wVF3QgqnnMnsBCfY/XqFRBC4b0u7CCTdC1lAG0HE2CTO2C1b:YLHVOMneLXcnpMCTdC1BgCThC1b
MD5:	21B4A94081BACE292E3C6FC4A6B1916B
SHA1:	2A2AC7E815E96D8534618BE4283EB8D4DDEE1CA7
SHA-256:	9DAFF523600A2047948978A6CF49AD5C4B6BF7983A896D9A41CAE1FD231FDBD9
SHA-512:	5E028831B14824853F6C794DA3147378A5A67FFFB781E90ACD2A2AD4D5740974357CA8977B473BD13AB3DC82F57AA54137E43564919C58EBCFF8E833154B3FBE
Malicious:	false
Reputation:	low
Preview:	.....!..K..... ....

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):	5.268770263050666
Encrypted:	false
SSDEEP:	6:mYsEp+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpXsjZZmwPXsqVkwOWXp+N23iKKdP:nB+va5KkTXfchI3FUtpXY/PXfV5f5KkI
MD5:	4D9AB9971E9B6F72E541FDDE48882B7D
SHA1:	DADF04073C7348788D196505EDDCA9EF41516B89
SHA-256:	6535B4909AE72775516101B84972D593F7A2934BF4B4B9DA4D7123D4D7C326E6
SHA-512:	D8CDFB6FE840FBDC594DDCD56871D0C08ADA546A63C4DC22B647FBE2B1D1CBE16659283C0CE6B2712CF790555C96F1761719E1A3EC976D5CDE0E9E0927F9343
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:17.128 1ddc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/09/27-05:08:17.130 1ddc Recovering log #3.2021/09/27-05:08:17.131 1ddc 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.oldVN (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.268770263050666
Encrypted:	false
SSDEEP:	6:mYsEp+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpXsjZZmwPXsqVkwOWXp+N23iKKdP:nB+va5KkTXfchI3FUtpXY/PXfV5f5KkI
MD5:	4D9AB9971E9B6F72E541FDDE48882B7D
SHA1:	DADF04073C7348788D196505EDDCA9EF41516B89
SHA-256:	6535B4909AE72775516101B84972D593F7A2934BF4B4B9DA4D7123D4D7C326E6
SHA-512:	D8CDFB6FE840FBDC594DDCD56871D0C08ADA546A63C4DC22B647FBE2B1D1CBE16659283C0CE6B2712CF790555C96F1761719E1A3EC976D5CDE0E9E0927F9343
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:17.128 1ddc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/09/27-05:08:17.130 1ddc Recovering log #3.2021/09/27-05:08:17.131 1ddc 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):	5.235780088206654
Encrypted:	false
SSDEEP:	6:mYsX3+q2PWXp+N23iKKdK25+XuoIFUtpXsIu2ZmwPXsIuyVkwOWXp+N23iKKdK28:ni3+va5KkTXYFUtpX62/PX6yV5f5KkTZ
MD5:	70E9A01A5ABC3A7B102B437811D26C99
SHA1:	306AD5AFEE4F12624196F8BF55A25B83E58078CC
SHA-256:	8B324263067A03BB642A1F50DC75F21A93B0FCDCD03420D04849C39C26760E17
SHA-512:	12D5D82ED4E6833DA496EA3B7FA5A4554462D1AF963816F5EA2C0B28B91C3E0F6ADC102D252815404D83A05945965E9FD35FDDFA4123339580852F0768F66A79
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:17.121 1ddc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/09/27-05:08:17.124 1ddc Recovering log #3.2021/09/27-05:08:17.124 1ddc 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):	5.235780088206654
Encrypted:	false
SSDEEP:	6:mYsX3+q2PWXp+N23iKKdK25+XuoIFUtpXsIu2ZmwPXsIuyVkwOWXp+N23iKKdK28:ni3+va5KkTXYFUtpX62/PX6yV5f5KkTZ
MD5:	70E9A01A5ABC3A7B102B437811D26C99

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
SHA1:	306AD5AFEE4F12624196F8BF55A25B83E58078CC
SHA-256:	8B324263067A03BB642A1F50DC75F21A93B0FCDCD03420D04849C39C26760E17
SHA-512:	12D5D82ED4E6833DA496EA3B7FA5A4554462D1AF963816F5EA2C0B28B91C3E0F6ADC102D252815404D83A05945965E9FD35FDDFA4123339580852F0768F66A79
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:17.121 1ddc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/09/27-05:08:17.124 1ddc Recovering log #3.2021/09/27-05:08:17.124 1ddc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.307198888918401
Encrypted:	false
SSDEEP:	6:mYsy+q2PWXp+N23iKKdKWT5g1IdqIFUtpXsYZmwPXsoVkwOWXp+N23iKKdKWT5gZ:n7+va5Kkg5gSRFUtpXh/PX1V5f5Kkg5i
MD5:	25ED491287C4FCB1D9D4CC50AA3A083F
SHA1:	EAAEADF606DDCEFCDC085FD42597FDDD417EB0FA
SHA-256:	F1DAD31533E69688A4D92CA7AFF5138609A133F6541181664ECCC875E19AA5AA
SHA-512:	B6F8A74BAA2466C4CE06008BA51920DB3E66104414D55184BBC040CEB5B1EB59443520E7D87ADA59AFD29CFEE3A038AA4881B6B4C5DB42040E4E227DB6FD09D0
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:16.394 1ddc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/09/27-05:08:16.396 1ddc Recovering log #3.2021/09/27-05:08:16.396 1ddc 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):	5.307198888918401
Encrypted:	false
SSDEEP:	6:mYsy+q2PWXp+N23iKKdKWT5g1IdqIFUtpXsYZmwPXsoVkwOWXp+N23iKKdKWT5gZ:n7+va5Kkg5gSRFUtpXh/PX1V5f5Kkg5i
MD5:	25ED491287C4FCB1D9D4CC50AA3A083F
SHA1:	EAAEADF606DDCEFCDC085FD42597FDDD417EB0FA
SHA-256:	F1DAD31533E69688A4D92CA7AFF5138609A133F6541181664ECCC875E19AA5AA
SHA-512:	B6F8A74BAA2466C4CE06008BA51920DB3E66104414D55184BBC040CEB5B1EB59443520E7D87ADA59AFD29CFEE3A038AA4881B6B4C5DB42040E4E227DB6FD09D0
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:16.394 1ddc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/09/27-05:08:16.396 1ddc Recovering log #3.2021/09/27-05:08:16.396 1ddc 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):	0.45488079341118026
Encrypted:	false
SSDEEP:	3:8EflwF:8N
MD5:	3F09117F3AA9FD6B468CC46EBA000872
SHA1:	B27A32B3E1CBA961269522B1A3345B1C8BC91F22
SHA-256:	158794AB782549C4FC24D31D700DBE92149E1DB78704A67E94C23AAC4ADED4A8
SHA-512:	0BFD9ECB45A6DCB805D76A147B85C27458CB718FA3FC72C7695C9015331A76DF60B5F7DF964710CFFB5715DE6274EBE10DC07B05D79D36E581CA4EAE56C5170
Malicious:	false
Reputation:	low
Preview:	.'..(.....=.+/.....

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):	155648
Entropy (8bit):	0.7645651105651531
Encrypted:	false
SSDEEP:	192:bA2rnlOHb22ReJlWMnCGHoN22usCYeJl2iMnCGHqiN22v5CYeJlpMnCGH/BN22B7:VC1CwHCX2CEC24CT
MD5:	52A0DA15F09EC11590DBAF20F5AB76CF
SHA1:	EEC9C4EF6C3427B2A9C280400D5A746D5BFD3AC8
SHA-256:	EF3F00A2F2171CC0A0DE5637AF46E62038BEF1450094BFC2A53CD5F64FC18E65
SHA-512:	18C7DE2691DB43CE07E61A7CC906C7B12D8AB3CD7886040C895EEBFB589CFE82AEE85E85FF7B60CE217D70DBD701CF90091CB2F96989140F52130AA5CE2173F
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):	2083
Entropy (8bit):	5.9023908644071925
Encrypted:	false
SSDEEP:	48:0XBvk76R1J5He2wiBKkNWXNLMdD+fsHh2MjSuNnEd:OBd5Hnw2KkN4WpB26SuhEd
MD5:	34520855B55327094949415EC624FEA4
SHA1:	CD425157FFC5BF1FC00A104DDA1DF904106BAC12
SHA-256:	4A56493A57D01F3BF62181BF7DD7DFDCEA63C3F0FC8D0CE39B172410E8E648D8
SHA-512:	9FF51DA9DEEBAC83F276505155A91AAA2F7279B3A9511AEBDE4FA7E044851EE2697A30732DCB4AA933830005D688594EB6D4C2C1BA74CB5DC7ADFEEB123C040
Malicious:	false
Reputation:	low
Preview:	....."..."..0."1c196eecda853ede786dcd07e65b9687v2..app..at..awesome..bulmapan0203..by..clickfunnels..com..domain..for..funnel..https..landing..my..optin 1632526772591..page..powered..preview..track..true..updated..2c7..4sv4e..en..genially..ir..panelfbs..por..yapoyix621..614e65ad1f21fe0d7ec3b264..genial..ly..view*..."....0...&."1c196eecda853ede786dcd07e65b9687v2.....2c7.....4sv4e.....614e65ad1f21fe0d7ec3b264.....app.....at.....awesome.....bulmapan0203.....by.....clickfunnels..... com.....domain.....en.....for.....funnel.....genial.....genially.....https.....ir.....landing.....ly. ....my.....optin1632526772591.....page.....panelfbs.....por.....powered.. ....preview.....track.....true.....updated.....view.!...yapoyix621..2...!.....0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....a.....b..... ...c.....d.....e.....!.....f.....g.....

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):	158572
Entropy (8bit):	0.5843081478114466
Encrypted:	false
SSDEEP:	192:m8ljmc2AeJl0Hr224CYeJlhMnCGH32N22dCYeJlHMnCGHl0iN22a:mLCsC1C6CjJ
MD5:	079F97669266FE398D4986FBCE6E7BEC
SHA1:	BF7A29E2EBF1768E8DC99E94819E320B1F5110EE
SHA-256:	3B3E98BF33FD47FEA83F3646DCF05C5C70294B01DC1313855897262 73E8CA591
SHA-512:	EC9CA24F61153C20E9197FAA42C1F6EA1EA2C1F2E102C8E735289647D853A42CB220697A4EEA821274F75262C1E9C91B54FA406C2448FC9B20A6F0A8EE5BD07
Malicious:	false
Reputation:	low
Preview:	.....- ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last SessionO (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	35554
Entropy (8bit):	2.962022509649255

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last SessionO (copy)	
Encrypted:	false
SSDEEP:	384:oOHl8ly8l8Tul9rVlDVlHwieWCmC/C+CpRhbDR:oOHmE86yjp3rNGlAjHR
MD5:	ED0D17DDA046E07B68B6182847FEAB4D
SHA1:	9B894C7B6DE249B2260E5898046644527AD4BB71
SHA-256:	3EC8CA045F0F70A0802BA8CA0BCCA4D4B34362FE56C70E1C6785A19B8B51D219
SHA-512:	309248D19DB42595C4412563F0B10C4F76AF2083E4C64590F5FCAD08D40F06E96AB9776575A4B0C91322E2FABCB3E263FDC3C962241F0B41FABB9C61A5F3599(
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...e069e0a6_0013_4522_b1e5_10835d44b86f.....M..... .....5..0.....&...{AE32626E-B2F7-4664-89C4-2B2C2DB60905}.....U..P...../...https://view.genial.ly/614e65ad1f21fe0d 7ec3b264.....h.....`..... .....f.../...h.t.t.p.s.:././.v.i.e.w...g.e.n.i.a.l...l.y./.6.1.4 .e.6.5.a.d.1.f.2.1.f.e.0.d.7.e.c.3.b.2.6.4.....8.....0.....8..... .....https://2c7.ir/ 4sv4E.....".<.+/.....https://app.funnel-

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last TabsOG (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):	3247
Entropy (8bit):	5.526503610905829
Encrypted:	false
SSDEEP:	96:XgtigOgTgna72gnMSgpdbag5iUyUaDbQ5fgG8rS0g/:XgtigOgTgny2gnZgpdeg5iUyUaDE5fgW
MD5:	6ACC16CA9FAD8562B0BF64A3906ACD47
SHA1:	64B4B486C447583A67A463BDEBA40D3E649F4A3A
SHA-256:	638835F1CFE3FAF5F9A4DD066D6A5E9779D899A491EB2C3DD6CAC6EDA49FEB1C
SHA-512:	E96CED5DE0B8289B682A2418941499AFE14D3D187D69790B47910B8ACA662E24A9D92C8CE90431D830DB7FE5F849BEB00C11F75CD60AC70AFFCF2AF53A5EAD 1E
Malicious:	false
Reputation:	low
Preview:	.....*.....#META:https://app.funnel-preview.com.....C.(_https://app.funnel-preview.com..preview..true.&_https://app.funnel-preview.com..track..0.+_https:// app.funnel-preview.com..updated_at#.1c196eecda853ede786dcd07e65b9687v2.2_https://app.funnel-preview.com..firebase:sentinels3..../.....8META:chrome-extens ion://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache": {"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..4137430 00.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-09-27 05:08:18.30][INFO][mr.Init] MR instance ID: 97cc769f-62c0-4482- a4ef-b32196eb8a26\n","[2021-09-27 05:08:18.30][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-09-27 05:08:18.30][INFO][mr.Init] Native Mirroring Service is e nabled.\n","[2021-09-27 05:08:18.30][IN

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.185121761999004
Encrypted:	false
SSDEEP:	6:mYsMLv4q2PWXp+N23iKKdK8a2jMGIFUtpXsMLcJZmwPXsMLIH/DkwOWXp+N23iKi:n7v4va5Kk8EFUtpX7cJ/PX7IfD5f5Kkw
MD5:	8EC10F0CA87CB6ABE2E1A71C68ABEEAA
SHA1:	2B98CC456C66AD768022DE40371A008ED5D7249F
SHA-256:	7F43B5C78259C9DE8C5BAE1314FCD425E2E1960D5B61B4D8982A6124B60AD330
SHA-512:	784EC81EC6642EEEBF0274070D2497528557887B5A4078ECE793C3FD42B59D005D9CFEF0182D7B15EFEB645F4FCB611F937E0EC31DB007EAC88028AA95B2DE C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:09.498 1b20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/09/27-05:08:09.499 1b20 Recovering log #3.2021/09/27-05:08:09.501 1b20 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.oldea (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.185121761999004
Encrypted:	false
SSDEEP:	6:mYsMLv4q2PWXp+N23iKKdK8a2jMGIFUtpXsMLcJZmwPXsMLIH/DkwOWXp+N23iKi:n7v4va5Kk8EFUtpX7cJ/PX7IfD5f5Kkw
MD5:	8EC10F0CA87CB6ABE2E1A71C68ABEEAA
SHA1:	2B98CC456C66AD768022DE40371A008ED5D7249F
SHA-256:	7F43B5C78259C9DE8C5BAE1314FCD425E2E1960D5B61B4D8982A6124B60AD330
SHA-512:	784EC81EC6642EEEBF0274070D2497528557887B5A4078ECE793C3FD42B59D005D9CFEF0182D7B15EFEB645F4FCB611F937E0EC31DB007EAC88028AA95B2DE3C
Malicious:	false
Reputation:	low
Preview:	2021/09/27-05:08:09.498 1b20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/09/27-05:08:09.499 1b20 Recovering log #3.2021/09/27-05:08:09.501 1b20 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
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):	147456
Entropy (8bit):	1.4165928256139961
Encrypted:	false
SSDEEP:	768:HS1yctGcEnmHIeFnTJcgYR0FnTJc16R0FnTPIuaRcB3:HS1ftDEnmHIehTKg80hTK1S0hTwuyQ
MD5:	2536301E8813B460E8F2684AC2307875
SHA1:	53B3C52FC59B8CB08A45A33FEAABA583BC1CF5A8
SHA-256:	F15C9D15D9396BE5BCF7C61D4B9EFB1B6648AEB77CFE71E7EA4144C946B5B6CF
SHA-512:	C9EC57A5A5579382446D610C84EA7D4A7F2ED18CD26958FC59E50585274179204102CBA146967DC6A228F9ADFCACFEBB904B4C317A1236B11C4F4D454D3D885
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	154032
Entropy (8bit):	1.3203409074345245
Encrypted:	false
SSDEEP:	768:xw8vcfhDimdcgeFnTJcfmR0FnTJcGvuR0FnTPTv:xw8EfhDim+gehTKf20hTKGvO0hTrv
MD5:	28EA4A235B6799FD2C253B2087A5F906
SHA1:	B6D63C82ABFE081E338E913B4A563DB221EE47AE
SHA-256:	63241E88C3CD9B4B6D31D1E4257A18973A57F8C68C6C593169E66015D6D8BD6E
SHA-512:	9FB8DF0AF05D82AB20C54381008DC49766EA6BF03494AD536ECF8382D0E6B04B8A2AC17478E767B49EC361657CA98FA0D8D3487F5F067AF6A9006B17F6526B2
Malicious:	false
Reputation:	low
Preview:	.....,V ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent Statea (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent Statea (copy)	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3930
Entropy (8bit):	4.908530147628736
Encrypted:	false
SSDEEP:	96:JTOXGDHzzB8lZlaGgb65TwGPkpKV/roGlFtGGpV/H:JTOXGDHzzB8lZlazb65TwakpO/cgtGiZ
MD5:	7571A2F70768251878B86190A59D719F
SHA1:	8394D00E6DACFC4C0C2C75673DD3199803A33CD5
SHA-256:	E7C3FBC09A324BDA69F5AFBAE40BA5FAE15147D140BF5505D3F34397A2F1737E
SHA-512:	A9F4FCA8343C97188398B39AFC91354551E0D57957EF1557B4C029FA341FE8275A7FBB5D77487E1E82BA75589888584DA75A3F0ADD77E36DB58DCB083AEC506
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.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":"13279810091712367","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13279810091716938","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13279810091827320","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expi

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent Stated (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},

Static File Info

No static file info

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6832 Parent PID: 580

General

Start time:	05:08:08
Start date:	27/09/2021
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://2c7.ir/4sv4E'
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 7036 Parent PID: 6832

General

Start time:	05:08:09
Start date:	27/09/2021
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=1560,16086817351805558034,16500979573986469014,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1684 /prefetch:8
Imagebase:	0x7ff68b0a0000
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

Analysis Process: chrome.exe PID: 5580 Parent PID: 6832

General

Start time:	05:08:13

Start date:	27/09/2021
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=audio.mojom.AudioService --field-trial-handle=1560,16086817351805558034,16500979573986469014,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=3108 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly